Privacy Impact Assessment
for the

Online Detainee Locator System

April 9, 2010

Contact Point
James Chaparro
Director, Office of Detention and Removal Operations
U.S. Immigration and Customs Enforcement
(202) 732-3100

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

Abstract

The Online Detainee Locator System (ODLS) is a publicly accessible, web-based system owned by U.S. Immigration and Customs Enforcement (ICE). ODLS allows the public to conduct online Internet-based queries to locate persons detained by ICE for civil violations of the Immigration and Nationality Act. ODLS is intended to allow members of the public, especially family members and legal representatives, to determine whether an individual is currently in ICE detention and, if so, at which facility the person is detained. ICE conducted this PIA because this system makes available to the public personally identifiable information (PII) about individuals detained by ICE.

Overview

ODLS is owned by the ICE Office of Detention and Removal Operations (DRO). DRO is responsible for promoting public safety and national security by arresting, detaining, and removing persons from the United States in accordance with the Immigration and Nationality Act. ICE developed ODLS as a service to the public, especially family members and legal representatives, to help locate individuals arrested for administrative immigration violations and who are in or have recently left ICE custody ("detainees"). Currently, members of the public must contact a DRO field office by phone to determine the location of a detainee. With the deployment of this automated system, the public will be able to locate detainees more quickly and efficiently through an online query. The system will ultimately be available in several languages to help users whose native language is not English.

ODLS is a web-based system that is accessible from an Internet browser and may be used by any member of the public. ODLS is scheduled to deploy in June 2010, and will be accessible by visiting ICE's public website (http://www.ice.gov/locator). Persons using ODLS do not need to set up an account or get special permission to use the system. ODLS provides two ways to search for a detainee: (1) perform a query using an Alien Registration Number (A-Number) and country of birth; or (2) perform a query using a full name and country of birth. After receiving the query entered by the user, ODLS searches for a match among current ICE detainees and detainees who have been booked out of ICE custody (regardless of the reason) within the last 60 days.[1] All records that match the user's query are returned to the user in a list of one or more search results.

ODLS only performs exact-match searches. This means that the search query entered by the user (specifically, the name or A-Number) must exactly match the information in a detention record in order for the record to be identified as a match and included in the ODLS search results. For example, a search for "Robert Smith" will not return a detention record for "Robert Smyth" or "Bob Smith." When conducting an A-Number search, ODLS users will see a maximum of one record in the results because A-Numbers are assigned to individuals uniquely. When conducting a name-based search, however, ODLS users may see multiple records in the results if several detainees share the same name and country of

[1] The data searched by ODLS is extracted from detention records maintained in ICE's Enforcement Integrated Database (EID) and stored in a separate ODLS database. *See* Enforcement Integrated Database PIA at http://www.dhs.gov/privacy. The ODLS extract is updated approximately every 20 minutes.

birth. Users may use the year of birth provided in the results to distinguish among detainees with the same name.

ODLS only contains information about individuals who are currently in ICE custody or were previously detained by ICE within the past 60 days.[2] If a search is performed for detainees who have never been in ICE custody or were released from ICE custody more than 60 days ago, ODLS will return a result of "no records found." If a matching detainee record is found, the ODLS results screen will display the detainee's custody status as either "in custody" or "not in custody." An "in custody" status means the individual is currently in ICE custody, and ODLS will display the detention facility where the person is being held, the contact information for the facility, a link to the facility's website, and the contact information for the DRO office responsible for the detainee's immigration case.[3] A status of "not in custody" means the individual was released from ICE custody within the last 60 days for any reason. The "not in custody" status will be displayed if the individual was removed from or voluntarily departed the United States, was released on bond or through an alternatives-to-detention program, was released into the United States due to the resolution of their immigration case (e.g., grant of an immigration benefit that permits them to remain in the country), or was transferred into the custody of another law enforcement or custodial agency. For individuals released from ICE custody within the last 60 days, ODLS displays contact information for the DRO office responsible for the detainee's immigration case.[4]

ODLS also provides resources to help users find or identify the detainee they are seeking. First, ODLS includes a frequently asked questions (FAQ) page to answer common questions about the system and to help troubleshoot problems. Second, for those who are unable to locate the detainee in ODLS, a link is provided to all DRO offices so the public can contact the office in the appropriate geographical area for assistance. Finally, for every detainee included in ODLS, the responsible DRO field office is identified and its contact information is provided so family members and attorneys can call to confirm the detainee's identity, arrange for bond, or ask for additional information.

Concurrently with the publication of this PIA, ICE is also amending the Department of Homeland Security/ICE – 011 Immigration and Enforcement Operational Records (ENFORCE) System of Records Notice (SORN) to propose a new routine use that will allow the public sharing of detainee information through the ODLS system as described in this PIA.

[2] ODLS does not provide information about all individuals in ICE custody. Juveniles (under 18 years old) are excluded.

[3] If ODLS is searched while a detainee is being transferred between detention facilities, ODLS will show that the detainee is in custody at the original facility until the detainee has arrived and been booked into the new facility, and the detainee record in EID is updated. Because it may take up to eight hours for the detainee record to be updated after a transfer, persons planning a visit should call the detention facility to confirm the detainee is still at that facility.

[4] Persons seeking additional information about a former detainee (e.g., release date, reason for release, their current location, immigration status) must contact DRO. DRO may disclose this information only with the consent of the former detainee, or if disclosure is otherwise authorized by the Privacy Act or the routine uses in the ENFORCE System of Records Notice (75 FR 9233, March 1, 2010).

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?

Generally, ODLS contains information on current ICE detainees and detainees who have been booked out of ICE custody (regardless of the reason) within the last 60 days (collectively, "detainees"). Specifically, ODLS contains each detainee's name; A-Number; country of birth; date of birth; custody status ("in custody" / "not in custody"); the name, location, contact information, and website of the detention facility where the detainee is being held (if applicable); and the DRO office responsible for the detainee's immigration case. Juveniles under the age of 18 are not included in ODLS.

As noted in the Overview, persons using ODLS may perform either an A-Number or name-based search in ODLS. To perform an A-Number search, the ODLS user must enter the detainee's A-Number and country of birth into the ODLS query screen. (Country of birth is selected from a drop-down menu.) ODLS then displays matching results, if any. The ODLS results screen displays the following information for the detainee that matches the query:

- A-Number
- First, middle, and last name
- Country of birth
- Detainee's custodial status ("in custody" or "not in custody")
- Name, address, phone number, and website of the detainee's current detention facility (if the detainee's status is "in custody")
- Contact information for the DRO office responsible for the detainee's immigration case

The name-based search requires the user to input the detainee's first and last name and country of birth into the ODLS query screen. The ODLS user may also provide the detainee's date of birth (if known) to narrow the search results. ODLS will display the matching results if any records are an exact match. The ODLS results screen displays the following information for the detainee(s) that match the query:

- First, middle, and last name
- Country of birth
- Year of birth
- Detainee's custody status ("in custody" or "not in custody")

- Name, address, phone number, and website of the detainee's current detention facility (if the detainee's status is "in custody")
- Contact information for the DRO office responsible for the detainee's immigration case

ODLS collects limited technical information for each visit to the ODLS website, including the visitor's Internet domain, Internet Protocol (IP) address, and the Internet address of the website from which the visitor linked directly to the ODLS website. This information is collected to allow ICE to troubleshoot issues with the system and to monitor and protect the system from cyber-attacks. This information is not used to identify people who use ODLS, to track what they search in the system, or to assist with immigration enforcement activities. Additionally, the ODLS website uses session cookies, which are small bits of text that do not collect any information about users but are used to track and help ODLS users while they navigate throughout the site. The cookies only last for the duration of an active browser session and once a user closes the browser or has been inactive on the website for 20 minutes, the cookie is deleted.

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

The ODLS detainee information, the information about the detention facilities, and the information about the DRO field offices is obtained from an ICE database known as EID. EID contains arrest, detention, and removal records for individuals ICE has arrested for violations of the Immigration and Nationality Act, among other types of data. A Privacy Act SORN has been published for the records maintained in EID. *See* DHS/ICE-011 ENFORCE SORN (75 FR 9233, March 1, 2010). EID has a significant amount of identifying and other information about detainees, which is described in the ENFORCE SORN and the EID PIA. However, only a small subset of that information is extracted from EID and included in the ODLS database.

The people using ODLS provide the queries that the system uses. The system itself generates the search results based on the queries entered by the ODLS users.

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

The information in ODLS is being made available to the public to facilitate the identification and location of individuals who are in or have recently left ICE custody. The system is intended to allow family members, legal representatives, and other interested parties to locate persons in ICE custody more quickly and efficiently, and to reduce the number of ad hoc telephone inquiries handled by DRO field offices. As mentioned above, limited technical information for each visit to the ODLS website is collected in order to allow ICE to troubleshoot issues with the system and to monitor and protect the system from cyber-attacks. The session cookies are used to track and assist ODLS users while they navigate through the application.

1.4 How is the information collected?

ICE personnel collect and enter information about detainees into EID when they are arrested and booked into a detention facility. For example, the detainee's name, date of birth, and country of birth will all be collected during ICE's initial processing of a detainee. This information may be obtained from the detainee, from the detainee's travel documents, or from pre-existing government records on the individual, such as previous detention records or the Alien File, or from a combination of these sources.[5]

An extract of very limited data is taken from EID and stored in a separate ODLS database. ODLS uses the query provided by a user, searches the extract, and returns results that match the user's query. The ODLS extract is updated every 20 minutes in order to provide the user with the most current information available in EID.

1.5 How will the information be checked for accuracy?

Detainee data available through ODLS originates from EID. Several steps are taken to check the accuracy of EID data generally, including collecting information directly from individuals and/or from their identity and travel documents; using data quality review processes to detect and fix data entry errors; and mandatory training for system users which emphasizes verifying data input into EID. For more information on data accuracy in EID, please see the EID PIA.

ICE policy requires all information pertaining to the release, removal, or transfer of detainees be entered into EID within eight hours of the action. In most cases, the information is promptly updated but there are situations when it may take up to eight hours to update the information in EID. This means that the information displayed in ODLS may not always be timely when a detainee is in the process of being removed, transferred, or released, or when one of those actions has been completed within the last eight hours. In such cases, ODLS could display information that is out-of-date for up to eight hours. For example, ODLS may show an "in custody" status when the detainee has just been released, or show that the detainee is at a particular detention facility, when in fact the detainee has just been transferred to another facility. To mitigate public concerns and inconvenience that may arise from this, the ODLS website notifies users of this issue and advises them to contact the detention facility or the relevant DRO office in circumstances where the most current location data is required (e.g., prior to a visit or when arranging bond).

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

DHS has been authorized to collect information under numerous authorities. These authorities include, but are not limited to, 5 U.S.C. § 301; 8 U.S.C. § 1103; 8 U.S.C. § 1225(d)(3); 8 U.S.C. § 1324(b)(3); 8 U.S.C. § 1357(a); and 8 U.S.C. § 1360(b). Additional authority is provided in 6 U.S.C. §§

[5] The Alien File is the DHS record that contains copies of information regarding all transactions involving an individual as he/she passes through the U.S. immigration and inspection process. *See* DHS/USCIS-001 Alien File (A-File) and Central Index System (CIS) SORN, January 16, 2007, 72 FR 1755. The A-Number is the numeric association to that individual's file.

202; 8 U.S.C. §§ 1158, 1201, 1365a, 1365b, 1379, and 1732; and the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (Pub.L. 104-208).

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: Because ODLS is accessible to the public, there is a risk of exposing too much personal information about detainees in the search results.

Mitigation: This risk has been mitigated by intentionally limiting the detainee information displayed in the search results to only that information which is necessary to allow the user to identify a specific detainee and determine their current custodial status and location. ICE maintains a great deal of information on detainees in EID, but ODLS uses and displays only a small subset of this information that is necessary to accomplish the purpose of the system. For example, if a user conducts a name-based search in ODLS (which requires a query containing at least the detainee's name and country of birth), ODLS will not disclose the detainee's A-Number in the results. If the user knows the A-Number, he can elect to do an A-Number search but a user cannot learn the A-Number of a detainee through ODLS.

Privacy Risk: There is a risk that unauthorized persons may attempt to extract significant amounts of detainee information from ODLS using sequential queries or malicious programs.

Mitigation: The queries for ODLS are intended to mitigate this risk by requiring that users know at least two separate identifiers about the detainee Users must query ODLS using a name and a correct country of birth, or an A-Number and a correct country of birth. A name or A-Number alone will not suffice. Additionally, a challenge-response mechanism is in place which requires the user to view a system-generated image and to type the characters displayed in the image. This helps to ensure that malicious computer programs and computer-generated queries cannot extract information from the system.

This risk has also been mitigated by a technical decision about the design of the ODLS. Early design discussions considered whether ODLS should query a customized extract of EID data, or should query the entire EID dataset. The decision to use an EID extract for ODLS was made because EID contains substantially more PII than ODLS would need to operate. By using only a subset of the larger EID database, ODLS limits the risk to a smaller number of records and a more limited set of PII. While robust security protections are in place in order to protect the data in the ODLS extract, limiting the PII that is potentially at risk enhances the overall privacy and security posture of this system.

Privacy Risk: There is a risk that the information in ODLS regarding a detainee's custodial status or location will not be current.

Mitigation: To mitigate public concerns and inconvenience that may arise from this risk, the ODLS website notifies users that the information may not always be current, and advises them to contact the detention facility or the relevant DRO office in circumstances where the most current location data is required (e.g., prior to a visit or when arranging bond). The contact information for the detention facilities and the appropriate DRO office is provided by ODLS.

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.

ODLS information is used to help members of the public locate detainees who are in or have recently left ICE custody. While ODLS is open to everyone, ICE anticipates that its primary users will be family members, legal representatives, or other persons who have an interest in the detainee.

Limited technical information for each visit to the ODLS website is collected in order to allow ICE to troubleshoot issues with the system and to monitor and protect the system from cyber-attacks. This information may be used to investigate or prosecute criminal violations of federal law regarding the misuse of federal information systems. This information will not be used to identify or track people using the website for legitimate purposes, or to enforce U.S. immigration laws. As noted above, session cookies are used to track and assist users while they navigate through the ODLS website.

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

This system performs an exact-match search to compare the information entered by the user on the ODLS search screen against the detainee information in ODLS. Only detainee records that exactly match the search query are displayed to the user on the ODLS results screen.

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

ODLS 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.

ICE has limited the amount of detainee data that is available to the public through ODLS. This limitation was necessary to ensure that the system cannot be used for reasons other than the intended purpose of helping to locate ICE detainees. Although anyone can submit a query in ODLS, the system is designed to ensure that only users who know something about the detainee can perform a successful search. For example, users must enter at least two discrete identifying pieces of information about the detainee to successfully submit a query. In addition, ODLS uses exact-match searching to help limit the search results returned, thereby avoiding over-exposing detainee data. Additionally, the challenge-

response mechanism helps to protect the ODLS dataset from automated attacks by malicious computer programs.

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?

ODLS uses an extract of EID data that contains limited information about current detainees and detainees that were released during the last 60 days. This data is retained in the system. Search queries entered by users are used by the system in order to process the queries and return results. Limited technical information for each visit to the ODLS website is maintained in server logs.

3.2 How long is information retained?

Detainee records in the ODLS extract are updated as the records in EID change. A detainee record that no longer meets the criteria for the ODLS extract because, for example, the detainee was released from ICE custody more than 60 days ago, will be deleted from the extract. Other records will be retained in the extract for as long as the record meets the extract criteria. Search queries entered by users are not retained once the query has been run by the system. The logs for the ODLS that capture the limited technical information are retained for seven (7) years.

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

A record retention schedule is currently in development and will be presented to NARA for approval.

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

Privacy Risk: There is a risk that the data in ODLS may be retained for longer than is necessary.

Mitigation: The data in ODLS is retained only as long as is necessary to allow the system to function as intended. No detainee data is retained in ODLS unless it pertains to a detainee who is eligible to be queried in ODLS (i.e., current detainee or one released within last 60 days). Query data is used only to perform searches and is not retained.

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?

Any member of the public, including DHS personnel, may use ODLS to locate ICE detainees. No special interfaces have been developed for DHS organizations or users.

4.2 How is the information transmitted or disclosed?

DHS personnel would access ODLS either through the ODLS website or through the ICE public website in the same manner as any other user.

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

There are no unique privacy risks posed by the use of ODLS by DHS personnel.

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?

Any member of the public may use ODLS to locate ICE detainees. There are no special interfaces that have been developed for certain organizations or users.

Limited technical information collected for IT security purposes may be shared with external law enforcement or prosecutorial agencies if it becomes relevant to the investigation or prosecution of criminal violations of federal law regarding the misuse of federal information systems.

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

Yes, sharing of detainee location information helps to facilitate the operation of the immigration enforcement process, which is the purpose for which this information was originally collected. ODLS information is part of the ENFORCE SORN, DHS/ICE-011 (75 FR 9233, March 1, 2010) which is being updated with the publication of this PIA to include a routine use that permits the sharing of detainee information through ODLS.

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

ODLS results contain information about detainees, and the results are displayed on the Internet browser used by the person performing the query. In order to better protect the information, ODLS encrypts the data as it travels between the user's Internet browser and ODLS.

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

Privacy Risk: There is a privacy risk that members of the public are able to collect a significant amount of detainee information using the system.

Mitigation: This risk is mitigated by the amount of information a user must enter to obtain information about a detainee, by having ODLS search against an extract from EID and not against EID itself, and by the security measures discussed elsewhere in this PIA, which prevent malicious computer programs from extracting large volumes of data. Also, the search results are tailored to provide the minimum amount of information about detainees necessary for users to identify and locate the detainee they are seeking.

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. Persons booked into a detention facility by ICE are provided notice in writing that limited information about them will be available to the public through ODLS. In addition, the publication of this PIA and the concurrent republication of the ENFORCE SORN provide general public notice on the existence of the ODLS system.

As mentioned above, the ODLS website collects limited technical information for each visit and uses session cookies to help support ODLS users while they are on the website. The ODLS website has a privacy policy which provides visitors with notice regarding the use of session cookies and regarding the collection and use of the limited technical information that is collected.

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

Because of the law enforcement context in which detainee information is gathered, individuals do not have the opportunity or right to decline to provide identifying information to ICE. Additionally, some information about the individual may be gathered from the individual's immigration benefit forms, travel documents, or border crossing/visa records.

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

At this time, ICE detainees do not have the option to opt-out of participation in ODLS due to the administrative burden that it would place on ICE. As discussed above, detainees under 18 years old are automatically excluded from ODLS based on their age.

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

Privacy Risk: There is a risk that individuals whose information is made available to the public through ODLS may be unaware of that fact.

Mitigation: The publication of this PIA and the concurrent republication of the ENFORCE SORN mitigate this risk by providing a detailed description of the system and how the data is used. In addition, ICE provides each person arrested on administrative immigration charges with written notice informing them that their information can be queried by the public in ODLS. The written notice will be available in several languages to help detainees whose native language is not English.

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?

Because ODLS is a publicly available website, individuals may query their own information in ODLS to obtain access. Individuals may also request access to ODLS records about them by following the procedures outlined in the ENFORCE SORN. Please see the ENFORCE SORN for more information. Additionally, individuals seeking notification of and access to any record contained in the ENFORCE system of records, or seeking to contest its content, may submit a request to the ICE FOIA Office. Please contact the ICE FOIA Office at (866) 633-1182 or see the ICE FOIA Office's website (http://www.ice.gov/foia) for additional information on how to submit a FOIA. If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0550, Washington, D.C. 20528.

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

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

In addition to the procedures above, individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the ICE FOIA Office. Please contact the ICE FOIA Office at (866) 633-1182 or see the ICE FOIA Office's website (http://www.ice.gov/foia) for additional information. 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 ENFORCE 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?

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.

There are no significant risks to privacy that relate to the access and amendment of records in ODLS.

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?

ODLS is designed to allow members of the public to locate detainees who are currently in or have recently left ICE custody; therefore there are no restrictions on who may use the system.

8.2 Will Department contractors have access to the system?

Yes. ICE contractors have access to ODLS just like any other member of the public.

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

Because the system is intended to be used by members of the public, there is no privacy training provided to the users.

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

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

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

ODLS uses a challenge-response mechanism to prevent the exploitation of the ODLS dataset by malicious computer programs and computer-generated queries. Specifically, ODLS requires the user to view a system-generated image and to type the characters displayed in the image. This security protection is designed to ensure that the query is being performed by a human being and not a computer. It is also designed to ensure that technology cannot be used to submit large numbers of random searches against the system and thus gather a large amount of detainee information. Additionally, ODLS encrypts the information that is exchanged between the user's Internet browser and ODLS in order to prevent it from being accessed inappropriately.

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

Privacy Risk: There is a privacy risk that technology will be able to be used against the system to submit large numbers of random search criteria and collect lists of detainee information.

Mitigation: The technical safeguard described above is used to ensure that only a human being can submit a query to ODLS, which mitigates the risk that malicious computer programs will be used to exploit and extract detainee data from ODLS.

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?

ODLS is a tool that allows members of the public to locate detainees in ICE custody.

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

ODLS is currently being developed. Deployment is scheduled for June 2010.

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 copy signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security