Privacy Impact Assessment
for the

Microfilm Digitization Application System (MiDAS)

September 15, 2008

Contact Point
Donald K. Hawkins
Privacy Officer
US Citizenship and Immigration Services
(202) 272-8000

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

Abstract

The Department of Homeland Security U.S. Citizenship and Immigration Services (USCIS) Records Division maintains the Microfilm Digitization Application System (MiDAS), which houses 85 million electronic immigration-related records previously stored on microfilm. USCIS is conducting this Privacy Impact Assessment (PIA) to analyze the privacy impacts associated with the new release of MiDAS that will enable USCIS to 1) electronically search and retrieve historical immigration-related records, 2) process web-based requests for these records submitted by Federal, state, and local Government and Public Genealogy Customers, 3) provide case tracking capabilities for USCIS Records Division staff, and 4) provide these records to the law enforcement and intelligence communities.

Overview

USCIS developed the MiDAS system to preserve and digitally index approximately 85 million historic immigration related records that were previously stored on microfilm. Historic immigration related records include index cards and immigration records. Index cards were created to reference over 20 different record series in use between 1893 and 1975. The records are microfilmed images or original copies of the actual immigration records, such as Alien Registration forms and Naturalization Certificates. MiDAS converts index cards and records from deteriorating microfilm into digital images to improve retrieval of these historical records. The objective of MiDAS is to enable USCIS personnel to search, retrieve, and deliver information about individuals ("Subjects") contained in USCIS records to respond to requests received from "Customers," such as Federal, state, and local Government agencies and the public. Government agencies will use information obtained from MiDAS to assist in the determination to grant or deny a Government benefit or to conduct a law enforcement investigation. Members of the public will use MiDAS to obtain historical immigration records for genealogical and other historical research. MiDAS is a standalone system which does not share information with other systems.

The demand for records by historical and genealogical researchers, as well as other members of the public, has grown dramatically over the past several years. USCIS processes requests for historical immigration related records under its program for responding to Freedom of Information Act (FOIA) requests. Historical immigration related records that are the Subject of a FOIA request are usually released in full because the Subjects of the records are deceased, and therefore, the Privacy Act does not apply. When responding to these requests, USCIS presumes that immigrants born more than 100 years ago are deceased.[1] Thus, when the Subject of a record request was born less than 100 years prior to the date of the request, primary or secondary documentary evidence of the Subject's death would be required. The Customer would bear the burden of establishing to the satisfaction of the Genealogy Program Office that the Subject is deceased. Acceptable documentary evidence includes, but is not limited to death records, published obituaries, published death notices or published eulogies, church or bible records, photographs of gravestones, and/or copies of official documents relating to payment of death benefits. No records would be released in the case of an immigrant born less than 100 years prior to the request date until evidence of the Subject's death is received. If it is determined that the Subject is still alive, the MiDAS request will be cancelled and the public Customer will be advised to submit a Freedom of Information Act (FOIA) request. MiDAS helps USCIS respond to this increased demand for agency records and assist USCIS personnel effectively and efficiently obtain these records.

USCIS will also use MiDAS to respond to requests for historical immigration related information

[1] Schrecker v. U.S. Dep't of Justice, 349 F.3d 657, 664-65 (D.C. Cir. 2003)

about Subjects who are still alive. Examples of those requestors are personnel from Federal, state, or local Government agencies who require the information to make a benefit determination or conduct a law enforcement investigation. Such requests are reviewed to ensure release and handling of information is consistent with an appropriate routine use in the Alien File (A-File) and Central Index System (CIS) system of records notice (DHS-USCIS-001, January 16, 2007, 72 FR 1755.)

MiDAS is made up of three components. The Request Page (RP) module allows Customers to submit a request for historical immigration related records via the Internet. The Case Management (CM) module is a tool used by USCIS personnel to receive, track, and manage Customer requests. The Digital Image Storage and Retrieval System (DISR) is the database that houses digital images of historical immigration related records in an electronically searchable format.

Requests from the Public

A typical transaction in MiDAS begins when a member of the public goes to the USCIS.gov website in search of historical immigration related records, usually for genealogical research. The public Customer is directed from the USCIS home page to the Genealogy home page. This page provides information about the historical records sets, the type of genealogical information found within USCIS records, and detailed instructions for submitting an Index Search or a Records Request (including fees associated with each type of request.) At the point the public Customer decides to submit a request, he or she will be directed to the MiDAS Request Page where the Customer will enter data needed for the search and data needed for USCIS personnel to respond to or contact the Customer for follow up. The Customer will have a choice to either pay by credit card and submit his or her request electronically or print out the electronic form and submit payment and request via postal mail. For online payment, the Customer is automatically directed to the Department of Treasury's secure Pay.Gov online payment site, which then processes the transaction and sends a "paid" or "not paid" confirmation back to the Case Management module in MiDAS, where each request becomes a case. Paid requests are then processed by USCIS according to the content of the request.

There are two types of requests that a public Customer can make: and Index Search or a Records Request. An Index Search is a search of whether USCIS has records pertaining to a Subject, and a Records Request is a request for copies of the actual records. If the Customer isn't sure whether USCIS has a historical record of the Subject, the Customer may request an Index Search. The Customer will submit required information about the Subject along with the Index Search fee. In response to an Index Search request from its public Customers, USCIS will search MiDAS to determine if USCIS has any records from the five historical record series relating to the Subject. USCIS will inform the Customer whether records were located and what the records are. The second type of request is a Records Request, which is for copies of the actual records and requires a separate request and payment. The Records Request appears in the CM which USCIS retrieves, reviews, and then pursues responsive information or records using the DISR or other USCIS systems. If the Subject of the Index Search or the Records Request was born fewer than one hundred years from the request date, the Customer will have to demonstrate to USCIS that the Subject of the record is deceased by providing a death certificate, obituary, or other proof of death (via mailing or scanning the documentation). Once the record is located and obtained, USCIS personnel process the request by providing copies of releasable records to the Customer on paper or in digital form (on CD) by postal mail.

Requests from Government Agencies

MiDAS also allows Government personnel, including state and local Government to submit requests for historical immigration related information pertaining to living Subjects if the government entity is responsible for providing benefits, investing or processing violations of civil or criminal laws, or protecting the national security. These requests require users to register with USCIS through their sponsoring agencies to access a secure portion of the Request Page module. These Government Customers are validated through

their sponsoring agency point of contact as identified in the agency's Memorandum of Understanding (MOU) with USCIS.

Upon registration, these Customers are not able to search MiDAS data directly, but are able to request that USCIS perform an Index Search or a Records Request. Requests made by other Federal, state, or local agencies will transpire in the same manner as requests from the public, with three main differences. First, because these Customers will be requesting information about Subjects whose information may not be publicly releasable, the request can only be made in a secure portion of the Request Module that requires user identification (user ID) and a password provided by USCIS to authorized users. The second difference is that Government Customers will not be required to pay a fee for the Index Search or Records Request. The final difference is that when USCIS releases information pertaining to a living individual to a Government Customer, a record of that disclosure is maintained in the Subject's file. USCIS keeps an accurate accounting of each disclosure to outside entities pursuant to the subsection (c) of the Privacy Act, (5 U.S.C. 552a.). Each disclosure is recorded on a Form G-658, *Record of Information Disclosure (Privacy Act)*, which is maintained in the Subject's A-File or maintained in such a way that it can be easily retrieved when requested. Once the Government agency user submits a request using this secure portion of the Request Page module, the request is processed by USCIS in the same manner as a request from the public. USCIS responds to requests from Government Customers by fax, email, postal or express mail.

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?

Information in the RP module

The RP module will collect information about the Customer making the request and the Subject of the request.

Information about the Customer includes his or her:

- Name,
- Mailing or email address,
- Telephone number,
- Reply from Pay.gov stating fees have/have not been paid (public Customers only[2]), and
- User ID, password, and agency (Government agency Customers only), or
- Security Question and Answer (for public Customers.)

Information about the Subject includes his or her:

- Name;
- Date of birth;
- Country of birth;
- Paper or electronic copy of death certificate, obituary, or other proof of death if the date of birth is fewer than 100 years prior to request.

[2] Credit card information is not collected by USCIS and thus is not maintained.

The Customer may also opt to provide the following additional information about the Subject to narrow the search results incase multiple Subjects have the same name, date of birth, and country of birth. These optional fields include:

- Place of residence (address)
- Parent's and/or children's names
- Certificates (e.g., birth, death, marriage, and naturalization)
- Legal documents or notes (e.g., divorce decree, or other)
- Identifying numbers issued by previous records holders such as the Immigration and Naturalization Service and its predecessors (e.g. Alien Number, Naturalization Certificate number, or other personal identifying file numbers.)

Upon submission of the request, the RP generates an identification number (Case ID number) and provides this number to the Customer.

Information in the CM module

The CM module contains all information (listed above) provided by the Customer request. USCIS may also input that information into the CM based on follow-up interaction with the Customer if the search results need to be further narrowed or the search needs to be augmented. In addition, the CM module maintains case status information indicating whether the case is pending or completed.

The CM also contains electronic images of any correspondence USCIS has with the Customer, such as USCIS response letters to the Customer, and electronic copies of records provided to the Customer.

Information in the DISR module

Information in the DISR includes digital images of paper and microfilmed historical immigration records collected and maintained by the former Immigration and Naturalization Service (INS) prior to the inception of USCIS. Prior to 1975, the former INS collected information from applicants and petitioners seeking immigration related benefits using paper forms. The INS stored copies of all applications/petitions for naturalization, derivative citizenship, arrival, expulsion, exclusion, and lawful entry on microfilm and also created an index card system to track these records. This filing system of microfilmed index cards is called the Master Index (MI), covered by DOJ/INS-001 Index System (58 FR 51847, October 5, 1993.) USCIS replaced MI in 1975 with the Central Index System (CIS), covered by DHS-USCIS-001, (72 FR 1755, January 16, 2007.) After this transition, unless further action was taken with respect to a Subject whose records were contained within the MI, the information remained in the MI and was not transferred to CIS.

The DISR module stores digitized images of the MI (microfilmed index cards,) which contain the following limited information about the Subjects of records:

- Name,
- Date of birth,
- Country of birth,
- Biometric identifiers (e.g., photograph, signature)
- Place of residence (address)
- Parents Names
- Identifying Numbers issued by legacy Immigration and Naturalization Service now the Department of Homeland Security (e.g. Alien Number, Naturalization Certificate number), and

The location of the Subjects' official files, including:

- Index to Naturalization and Citizenship files 1906 – 1956

- Index to Alien Registration files 1940 – 1975
- Index to Immigrant Visa files, 1924 – 1944
- Index to Registry/Lawful Entry files, 1929 – 1944
- Alien Registration Forms (AR-2) 1940 – 1944, and
- Index to other records created at the applicable agency's headquarters in Washington, DC between 1893 and 1975.

In addition to index cards, the following record series are schedule to be digitized, indexed and added to MiDAS during the next five years:

- Alien Registration Forms, 1940 – 1944
- Certificate Files (C-Files), 1906 – 1956
- Some Repatriation, Resumption of Citizenship and Replacement of Naturalization Certificate files, 1929 – 1956
- Immigrant Visa Files, 1924 – 1944
- Registry/Lawful Entry files, 1929 – 1944
- Other records created at the applicable agency's headquarters in Washington, DC between 1893 and 1975
- Naturalization Certificate files 1906 – 1956

DISR does not collect any new information directly from the individual to whom the record pertains.

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

Information in the RP is collected directly from the Customer. Upon submission of the request, that information is populated into the CM module. Additionally, the Department of Treasury's Pay.Gov service will provide the CM with a status indicating whether the required fee has been paid (if necessary), and the CM generates information on the status of the request to aid USCIS personnel in tracking and responding to the request.

DISR contains historical immigration related records collected from Subjects between 1892 - 1975, who sought an immigration benefit or naturalization and/or were in immigration enforcement proceedings from the former Immigration and Naturalization Service and its predecessor agencies. Those predecessor agencies are Department of Treasury (1891 – 1903), Department of Commerce and Labor (1903 – 1913), Department of Labor (1913 - 1940), Department of Justice (1940 until 2003). Some MiDAS data also contains information about Subjects collected from other Government agencies circa. 1950 – 1975 (e.g. the index card references the individual was under investigation by other agencies).

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

Data, images, and indices of Subject records in the DISR module are being converted from microfilm into digital images, which enables USCIS to more efficiently search for and retrieve information pertaining to a Subject.

The CM and RP modules use information collected from Customers to provide information responsive to Government requests that may be utilized by the Governmental entities with the adjudication of benefits applications, execution of law enforcement actions, verification of immigration status, and the

processing of Freedom of Information Act (FOIA) requests. This collection of information from the Customer is required to respond to the request for information and is in compliance with the purpose for maintaining the system.

When USCIS identifies a record requested by the public through MiDAS that may not be releasable in full to the requestor, the case will be referred from MiDAS to USCIS FOIA and Privacy Act request specialists for processing. For example, a record about a Subject who is deceased may contain personally identifiable information about the Subject's children, which may not be releasable to the public.

1.4 How is the information collected?

Information in the RP is collected electronically and automatically uploaded into the CM module. Alternatively, the Customer may opt to print a hard copy of the request form completed electronically in the RP and mail it to USCIS, in which case it is manually keyed into the CM.

Information, in the form of images, contained in DISR is derived from microfilmed historic USCIS records, which cannot be altered. The images of historic records are converted directly from un-modifiable microfilm.

Additionally, the data elements from the digitized images are keyed into the DISR module so that electronic searches may be performed using these elements:

- Name
- Date of birth
- Country of birth
- Identifying Numbers issued by legacy Immigration and Naturalization Service now the Department of Homeland Security (e.g. Alien Number, Naturalization Certificate number.)

1.5 How will the information be checked for accuracy?

As part of their standard operating procedures, USCIS administrative staff check the name and other identifying information provided to conduct a search for the Subject of the request and verifies the Subject is the same individual by comparing data in the Central Index System.

Customers enter their information directly into the RP to ensure its accuracy. Additionally, those Customers provide their contact information to USCIS so that USCIS may contact the Customer to correct any information that is found to be inaccurate.

1.6 What specific legal authorities/arrangements/ agreements define the collection of information?

The authority to collect information in the CM and RP modules is contained in *Aliens and Nationality*, 8 USC 1101, 1103, 1304 and 1360 et seq., and includes definitions, powers, and duties of the Secretary of Homeland Security.

Subject data stored in the DISR Module converted from historical records and their indices were collected under various legal authorities dating back to 1882.

USCIS published a proposed rule entitled "Establishment of a Genealogy Program" in the Federal Register (71 FR 20357, April 20, 2006), which provides additional authority for the collection of information. USCIS published a final rule entitled "Establishment of a Genealogy Program" in the Federal Register (73 FR 28026, May 15, 2008).

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

Privacy Risk: A single request brings back records on multiple people.

Mitigation: In order to fulfill a request, personally identifiable information about a Subject that is obtained from Customers must be entered into MiDAS to conduct a search. While MiDAS collects a minimum set of personally identifiable information to perform a search, USCIS contacts Customers (public and other Government agencies) when multiple records result from a search to obtain additional information to narrow the records results and provide the correct records to the Customer

Privacy Risk: Inadvertent access to and/or disclosure of personally identifiable information collected from Customers.

Mitigation: Limited personally identifiable information is collected from the Customer to enable USCIS to respond to the requests for genealogical records in an accurate and timely fashion. Only USCIS Records Division personnel with the appropriate security clearance, necessary training, and system access authorization will have access to MiDAS. No records would be released to the Public Customer in the case of an immigrant born less than 100 years prior to the request date until evidence of the Subject's death is received. If it is determined that the Subject is still alive, the MiDAS request will be cancelled and the public Customer will be advised to submit a Freedom of Information Act (FOIA) request. For more information as to how an individual can submit a FOIA request, please see www.uscis.gov.

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 information contained in MiDAS is used to receive, track, and respond to requests for historical immigration records from USCIS Customers, including members of the public and other Government agencies. Requests from the public are primarily genealogical research requests, which result in searches and/or findings of historical records relating to deceased individuals. Federal, State, or Local Governments may request information from MiDAS to collect law enforcement intelligence for criminal or civil law enforcement proceeding such as an investigation, prosecution, enforcement, or implementation of civil or criminal laws, regulations, or orders.

MiDAS is a standalone system that maintains historical immigration records that document the arrival and subsequent naturalization of millions of American immigrants but does not update or locate USCIS documents to support a separate application or petition for benefits from USCIS. For example, requests to replace a lost naturalization certificate would not qualify as a MiDAS research request.

In response to an Index Search request from its public Customers, the USCIS searches DISR to determine if USCIS has any records from the five historical record series relating to the Subject. Once a Customer has demonstrated to USCIS that the Subject of the record is deceased by providing a date of birth more than 100 years prior to the date of the request or a death certificate, obituary, or other proof of death (via mailing or scanning the documentation), routine record copies and information would be reviewed and mailed directly to the Customer. (The information is stored in the Case Management Tracking module for one year.)

Request Page Module

The Request Page (RP) is the web-enabled module for initiating a request for information from USCIS on individuals who entered the United States prior to 1975. The RP module consists of two different web-based Request pages.

Secure Request Page Module

The first Request Page module is used by internal Department of Homeland Security (DHS) Customers and external federal, state, and local Government agencies and requires a User ID and password to log in to the system.

Public Request Page Module

The second Request Page is used by all Customers to make requests and view the status of requests online. The primary users of this module are members of the public who are making genealogy requests. To create a request, the public Customer is prompted to select a security question and provide the answer prior to completing the initial request. When the request is submitted, the Customer receives a Case ID number. The public Customer can later use the Case ID number and security question and answer to access information about the status of their genealogy request.

The information from the Request Pages is downloaded into the CM after the Customer completes the electronic form. The form itself cannot be retrieved. When the request case appears in the CM, USCIS retrieves the request information, reviews it, and then pursues responsive information or records using the DISR or other USCIS systems.

The Department of the Treasury's Pay.gov Service

In addition to the DISR, CM, and RP modules owned by USCIS, The Department of Treasury's Pay.gov Collections Service[3] will be used to process fees electronically via the public Request Page for genealogy requests. The request information will be processed directly through the Pay.gov Website, a separate secure website used to facilitate electronic payments between the general public and Federal Government Agencies. MiDAS (Public RP module) will redirect (link) the Customer to the Pay.Gov's payment processing web-site. The Customer will enter the payment information through Pay.Gov's interface. When the payment is successful, Pay.gov will send a successful response to MiDAS, and redirect the Customer to MiDAS' payment success page. MiDAS will neither collect nor store personal financial information supplied by public Customers. USCIS personnel will not have access to personal financial information supplied by members of the public nor will they have the ability to view personal financial information. Credit card information collected by Pay.gov is not within the scope of this PIA.

Case Management Module

The Case Management (CM) module will be used by the USCIS Records personnel to track and manage Customer search requests. The CM module will enable a more timely response to requests. Reporting and case analysis activities will also be implemented as part of the CM module.

USCIS Records personnel are granted access to use the CM module based on their job function. The CM will enable USCIS Records personnel to attach electronic case artifacts as well as create and attach correspondence letters that will facilitate the fulfillment of requests.

Digital Image Storage and Retrieval Module

The Digital Image Storage and Retrieval (DISR) module contains the digitized image of microfilmed index cards and some records. The following index data from the digitized index cards are keyed into the DISR module so that electronic searches may be performed:

- Name
- Date of birth
- Country of birth

[3] For more information about Pay.Gov, see Department of Treasury's Financial Management Service Privacy Act System of Records Notice, 70 FR 34522, published June 14, 2005.

- Identifying Numbers issued by the agency that created or maintained the records, such as the Alien Number or Naturalization Certificate number.

To retrieve historical immigration related records in DISR, USCIS searches the index data and then views the results in the form of index data and pictures of cards. The cards hold additional information that tells USCIS where to go look for one of millions of different kinds of files in paper, microfilm, microfiche, or digital format, that may be stored in a variety of locations depending on the file type and age. Those still in USCIS custody may be stored at USCIS headquarters or in field offices. Some of the file series have been transferred and are stored at the National Archives, while others were destroyed long ago.

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

The CM contains software for analyzing data to generate aggregate reports of MiDAS activity and case workflow. The system cannot accommodate global or profile searches. Each search must contain the required fields above.

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

The MiDAS application 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: Unauthorized Use of Information

Mitigation: The information contained in MiDAS is used to respond to inquiries from authorized Government agencies and members of the general public who provide documentation showing the Subject is deceased.

Only USCIS Records personnel with the responsibility of responding to Government and public requests for information will be granted access to the MiDAS system. The system administrator will grant access to users as authorized by the responsible Records Division program areas. All USCIS employees using the MiDAS database will be properly trained to release information in accordance with genealogy rules and regulations.

Privacy Risk: Release of unauthorized information to the public.

Mitigation: The proposed regulation sets forth the process by which USCIS personnel will perform searches for requested records. The Genealogy Regulation establishes an Index Search to determine if USCIS has a file on an individual. Section 103.40(c) of the Genealogy Regulation identifies information required to perform an Index Search and Section 103.40(d) identifies information required to retrieve records. Section 103.40 also identifies information required for release of records.

Information that may be provided by the Customer about the Subject's spouse or children is only used to identify the correct Subject in the index. It is not used to update any official record, nor does it become part of any record other than the CM case. Any PII information relating to living relatives/individuals will be redacted in accordance with FOIA/PA.

In addition, when a public Customer requests record of an immigrant whose date of birth is less than 100 years ago, the public Customer will be asked to provide documentary evidence that the Subject is deceased. USCIS presumes that immigrants born more than 100 years ago are deceased.[4] Thus, when the Subject of a record request was born less than 100 years prior to the date of the request, primary or secondary documentary evidence of the Subject's death is required. The Customer will bear the burden of establishing to the satisfaction of USCIS that the Subject is deceased. Acceptable documentary evidence includes, but is not limited to death records, published obituaries, published death notices of published eulogies, church or bible records, photographs of gravestones, and/or copies of official documents relating to payment of death benefits. No records would be released in the case of an immigrant born less than 100 years prior to the request date until evidence of the Subject's death is received. If it is determined that the Subject is still alive, the MiDAS request will be cancelled and the public Customer will be advised to submit a Freedom of Information Act (FOIA) request. For more information as to how an individual can submit a FOIA request, please see www.uscis.gov.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 How long is information retained?

Information contained in the DISR module is retained and disposed of in accordance with the schedule approved by the National Archives and Records Administration ("NARA") the week of March 13, 2006 (N1-566-06). The original Master Index *microfilm* (photo images, no electronic data) is permanent. MiDAS contains digital images taken from the microfilm, as well as keyed electronic data unique to MiDAS. This unique electronic data is scheduled as permanent. The digital images are temporary because digital images do not yet meet NARA standards for permanent retention, and the same images are available on microfilm.

Data contained in the CM Module and information (data and electronic images) pertaining to correspondence with the Customer (RP information) is retained and disposed every six years in accordance with the National Archives and Records Administration's General Records Schedule 14 and in conformance with the desired Certification and Accreditation (C & A) audit capability. (The information from RP Module is downloaded to the CM module once the request is submitted by the Customer and the RP cannot be retrieved). A revised retention schedule covering the case management and Request Page modules is pending review by NARA.

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

The National Archives and Records Administration approved Disposition schedule, N1-566-06, on October 12, 2006.

[4] Schrecker v. U.S. Dep't of Justice, 349 F.3d 657, 664-65 (D.C. Cir. 2003).

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

Privacy Risk: Unauthorized access to, or disclosure of, information contained with the system.

Mitigation: Information in this system is safeguarded in accordance with applicable laws, rules and policies. All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards that include restricting access to authorized personnel who have a need-to-know. This adheres to requirements of the DHS Information Technology Security Programs Handbook to include the issuance and use of password protection identification features. All internal components are mandated by DHS to comply with DHS' Sensitive System Security guidelines.

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?

Only USCIS HQ Records personnel have access to the MiDAS system CM and DISR module. All other USCIS and DHS personnel (ICE and CBP) with proper authorization submit their request to USCIS HQ Records personnel through the RP module.

When USCIS identifies a record requested by the public through MiDAS that may not be releasable in full to the requestor, the case will be referred to USCIS FOIA and Privacy Act request specialists for processing. For example, a record about a Subject who is deceased my contain personally identifiable information about the Subject's children, which may not be releasable to the public.

4.2 How is the information transmitted or disclosed?

USCIS HQ Records personnel provide Subject information to requesting Customers via electronic mail, compact disk, fax, telephone, or regular mail based on the Customer's preference.

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: Access to MiDAS CM, RP, and DISR modules by unauthorized individuals

Mitigation: Only USCIS HQ Records personnel with appropriate security clearances who are authorized to perform information searches will be provided access to the CM and DISR modules. These personnel are mandated by DHS to comply with Sensitive System Security guidelines and to complete annual Computer Security Awareness training.

Although the RP module is a part of MiDAS, the Customer is not directly accessing MiDAS when making a request. Each public Customer, upon submitting the initial request, is issued a different unique identifier (Case ID) for each request submitted and must answer a challenge question they select. The Case ID and answer to the challenge question is used for later authentication. For a user to obtain access to their previously submitted request, the Customer will be asked to supply their Case ID and to answer, affirmatively, the challenge question derived from previously supplied information. Federal, State and local Government users are required to use a unique User ID and password to submit the initial request or inquire about the status of the request.

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 , and the private sector.

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

For records in MiDAS that only contain personally identifiable information on Subjects who are deceased, USCIS will share those records with members of the general public. This sharing is in compliance with the Freedom of Information Act (FOIA). When Public customers request historical immigration related records containing information about living people, the MiDAS request will be cancelled and the public Customer will be advised to submit a Freedom of Information Act (FOIA) request.

USCIS will share historical immigration related information via MiDAS that is not publicly releasable (i.e., pertaining to living Subjects) with Government personnel, including state and local Government responsible for providing benefits, investing or processing violations of civil or criminal laws, or protecting the national security.. MiDAS distinguishes those users by assigning the requestor a unique User ID and password to access the Request Page module on the Internet. The requestor receives acknowledgement of the request and a Case ID number. USCIS uses the following methods to validate that the requestor has a need for the information: Letter of Accreditation and Memorandum of Understanding between USCIS and the Federal, state, or local Government agency. The requestor does not have automated access to any Subject information through MiDAS; Information and/or copies of records will only be provided to the requestor through USCIS approved methods (i.e., U.S. Postal Service and courier service). Some of the external organizations MiDAS information is shared with are: Bureau of Prison, Central Intelligence Agency, U.S. Army, Social Security Administration, and various State and local Government agencies.

MiDAS information and/or copies of records are shared with the above Federal, State and Local Government agencies to provide the immigration status of an individual for employment, determining entitlement of an agency's benefits or law enforcement purposes. Every Government agency that USCIS releases historical immigration related information to has a current MOU or LOA with that allows USCIS to release this information based on a "need to know" to perform their job. In addition to the MOUs or LOAs in place, USCIS records the reason for each disclosure on the G-658 *Record of Information Disclosure (Privacy Act)*, which is maintained in the Subject's A-File or maintained in such a way that it can be easily retrieved when requested.

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 the MiDAS information is compatible with the original collection. USCIS has entered into a number of Letters of Accreditations ("LOAs") or Memorandum of Understandings ("MOUs") for the sharing of USCIS information with other Governmental entities. These agreements dictate the terms and conditions for the release of information, as well as the appropriate use and safeguarding of all personally identifiable information. The MiDAS system is subject to data sharing in conjunction with these existing MOUs and LOAs. The terms and conditions for the sharing of information with other Governmental agencies are also provided for in the Alien File (A-File) and Central Index System (CIS) system of records notice (SORN), DHS-USCIS-001, January 16, 2007, 72 FR 1755.

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

USCIS provides information regarding a Subject to requesting Customers via electronic mail, compact disk, fax, telephone, or regular mail based on the Customer's preference. Handling of information shared with other agencies is governed by the terms and conditions of the related MOUs. Information is safeguarded in conjunction with sensitive security guidelines as established by the Department of Homeland Security.

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

Privacy Risk: Distribution of information to unintended recipients for uses that are incompatible with the original collection of the information.

Mitigation: The terms and conditions of the MOUs require Government Customers to safeguard the information obtained and to ensure that it is not used for any other purpose other than as provided in the MOU.

In addition, USCIS protects information through the use a secure portion of the RP module that is only accessible to Customers with a user ID and password assigned by USCIS to users authorized by a data sharing agreement.

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?

The information contained in MiDAS pertaining to a Subject is described in the Alien File (A-File) and Central Index System (CIS) system of records notice (SORN), DHS-USCIS-001, January 16, 2007, 72 FR 1755. In most cases, Subjects submit information directly to USCIS on an immigration benefit form that includes a statement about how the information will be used.

MiDAS does not collect new information directly from the Subject. However, MiDAS does collect information directly from a member of the public who is requesting historical immigration related information. The collection of information pertaining to the public Customer is addressed in this PIA, and the Department of Homeland Security (DHS) Freedom of Information Act (FIOA) and Privacy Act (PA) Record System DHS/ALL 001, December 6, 2004, 69 FR 70460. Additional notice of the Genealogy program has been published in the proposed Genealogy Regulation published in the Federal Register, April 20, 2006 (71 FR 20357).

Notice is provided to the public on the OMB approved USCIS Historical Records Services Request forms G-1041(OMB 1615-0096) and G-1041A (OMB 1615-0096), which can be submitted by a public Customer. The USCIS Historical Records Services Request form provides in part the following notice:

> *USCIS will use the information and evidence provided on this form to ensure that basic information required to assess eligibility for the requested services is provided by the applicant to facilitate identification of a particular record desired under the Historical Records Services Program. The authority to collect this information is contained in 8 U.S.C. § 1101, 1103, 1304 and 1306 and 44 U.S.C. § 2116 (c). In accordance with 5 U.S.C. § 552a, the USCIS will not disclose any record to any person or another agency, without prior written consent, except under certain circumstances as prescribed by the Privacy Act.*

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

Subjects do not have the opportunity or right to decline to provide information for law enforcement or benefits determinations.

The public Customer may decline to provide information, but that would likely result in USCIS being unable to respond to the Customer's request. There are required fields for both electronic and paper submission of the Index Search and the Records Request. This is a fee for service program. The public Customer is required to submit payment in advance of the service provided. USCIS requires the name, date of birth, and country of birth of the Subject to perform the requested Index Search, and may require specific information about the records requested for a Records Request. USCIS also requires the public Customer's name and address to contact the Customer with search results.

Genealogical requests are identified as "third party" requests (requests from other than the Subject), and since the Subjects of the requests are deceased, the deceased Subjects themselves no longer have privacy interests in the records. This is established by OMB Guidelines, 40 FR 28948, 28951 (deceased persons do not enjoy Privacy Act protections); Department of Justice, Office of Information and Privacy, Freedom of Information Act Guide (May 2004) (noting "longstanding FOIA rule that death extinguishes one's privacy rights")

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

An applicant provides consent upon applying for a USCIS benefit. Many OMB approved application/petition requests for immigration related benefits contain statements asking the applicant to provide DHS with the written authority to release information provided by the applicant to assist in the determination of eligibility for the requested benefit:

Genealogical requests are identified as "third party" requests (requests from other than the Subject), and since the Subjects of the requests are deceased, the deceased Subjects themselves no longer have privacy interests in the records.

For A-Files created for purposes other than immigration and naturalization (e.g., enforcement, investigations), the individual does not consent to particular uses of the information.

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

Privacy Risk: Notice is not provided directly to the subject of the record in most instances.

Mitigation: The opportunity to provide notice depends on the purpose of a particular request. Notice is not provided to Subjects of requests from Federal, State and Local Government agencies because such notice could compromise the integrity of a law enforcement action. Subjects of requests for genealogical searches from public Customers are not notified because these Subjects are confirmed to be deceased.

Privacy Risk: Customers may not be aware of the information USCIS collects about them.

Mitigation: MiDAS Customers submit their information directly to USCIS, and at the time of submission, are provided with notice of how USCIS will use that information.

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?

MiDAS Customers can print a record of the information they submit to USCIS via a MiDAS request at the time of submission. Additionally, the public Customer is prompted to select a security question and provide the answer prior to completing the initial request. When the request is submitted, the Customer receives a Case ID number. The public Customer can later use the Case ID number and security question and answer to access information about the status of their genealogy request.

MiDAS Customers and record Subjects can gain access to their information by filing a Privacy Act request to the USCIS FOIA/Privacy Officer at:

National Records Center
FOIA/PA Office
P.O. Box 648010
Lee's Summit, MO 64064-8010

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

In non-paid cases, the case will await payment by mail. If payment is not received within 30 days, CM generates a reminder letter that is sent to the Customer. After another 30 days of non-payment, the case is closed.

Digital images in MiDAS are unchangeable and cannot be modified by USCIS MiDAS Program staff including employees and contractors.

Electronic data in MiDAS is derived from the digital images in MiDAS, and so will reflect any error in the original index card. There is no capability for updating or correcting MiDAS in this context. A living Customer obtains the correction/redress by following the FOIA/PA procedure and, as a result, having their correct official index information entered into the Central Index System (CIS).

Individuals should direct all requests to contest their information contained in MiDAS, with supporting documentation and other relevant identifying information, to the FOIA/PA Officer at the address listed above.

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

Subjects and Customers will be notified of the procedures to correct their information through the MiDAS SORN, which will be published in the Federal Register. In addition, this information will be provided on the website located at www.uscis.gov.

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

Formal redress is provided to individuals in accordance with Sections 7.1 through 7.3.

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: None. The redress process takes place entirely outside the MiDAS system.

Mitigation: None specific, individuals follow the FOIA/PIA process for redress.

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?

The following are user group types established to access MiDAS:

General User: This user type reviews and performs searches for requests received from Customers (external and internal)

System Administrator: This user type is responsible for creating user accounts for Administrators and General Users. They have the responsibility to view reports, update accounts, and unlock user accounts.

Public (Unsecured) User: This user type is for the general public to submit Genealogy request for information and to check the status (Pending or Closed) of their request. They access only the Request Page module for the purpose of entering request information. They cannot search or retrieve any other information other than the status of their request.

Government/LE (Secured) User: This user type is for other Government personnel (LE) to submit request using a User ID and password for search of or retrieval of historical data predating 1975.

All user types except the public require a User ID and Password. USCIS/ICE and CBP users are validated through the PICs (Password Issuance and Control System). All other Government users are validated through the POC identified in the interagency MOU. HQ Records managers are responsible for approving access as a General, System Administrator or Secured Users.

8.2 Will Department contractors have access to the system?

Yes, and contractor access is governed by the System Service Contract.

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

Each internal MiDAS user is required to successfully complete the annual DHS/USCIS Computer Security Awareness Training. New employees are expected to successfully complete the training within 30 days after starting work with USCIS. The Computer Security Awareness Training includes instruction on Federal laws and regulations concerning privacy and data integrity, the handling of data, and restrictions on data use and/or disclosure.

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

MiDAS received a full Certification and Accreditation on July 31, 2008. The MiDAS Authority to Operate (ATO) has been extended thru July 31, 2011.

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

The CM Module provides the capability to track and manage requests and activities at the application and user levels. Using this capability, the CM Module will track the actions taken by system users and create an audit trail of any changes made to a case.

MiDAS is maintained at a DHS Data Center, which has deployed a number of physical security measures and controlled access to safeguard against threats from external entities.

Intentional and unintentional electronic threats from authorized, internal and external, entities are controlled and managed by the Password Issuance Control System (PICS). PICS officers will assign management access to the application to ensure that the appropriate people are provided the correct access. All managers with authorized access are entrusted to only provide access to appropriate people.

The combination of awareness by the user community with the use of passwords and encryption technologies provide system-wide technical protection mechanisms.

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: Unauthorized access to information

Mitigation: Access to MiDAS is limited to USCIS authorized users. System users take computer security training and are granted system IDs and passwords based upon their roles and responsibilities. Administrative controls, such as periodic monitoring of logs and accounts help to prevent and discover

unauthorized access. Audit trails are maintained and monitored to track user access and unauthorized access attempts.

Privacy Risk: Non-authorized users may have indirect access to information

Mitigation: Only USCIS HQ Records personnel with appropriate security clearances who are authorized to perform information searches will be provided access to the CM and DISR modules. These personnel are mandated by DHS to comply with Sensitive System Security guidelines and to complete annual Computer Security Awareness training.

Privacy Risk: Misuse of information

Mitigation: Information obtained from MiDAS is limited and responsive only to information provided by the internal MiDAS user. Security controls are in place to protect the confidentiality, availability, and integrity of personal data, including role-based access controls that enforce a need to know 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?

MiDAS is an operational product, a software application that consists of the integration and configuration of several Commercial-off-the-Shelf (COTS) products.

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

MiDAS is in the Integration and Test phase and moving to the Implementation phase. The development of MiDAS and the continuing corrective and adaptive actions follow the DHS system development life cycle methodology.

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

No, MiDAS does not employ technology which may raise privacy concerns.

Approval Signature Page

Original signed and on file with the DHS Privacy Office.

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security