Privacy Impact Assessment
for the

Integrated Digitization Document Management Program (IDDMP)

January 5, 2007

Contact Point
Elizabeth Gaffin
Privacy Officer
U.S. Citizenship and Immigration Services (USCIS)
(202) 272-1400

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(571) 227-3813

Abstract

The United States Citizenship and Immigration Services (USCIS) has prepared a Privacy Impact Assessment (PIA) for a series of systems comprising the Integrated Digitization Document Management Program (IDDMP). Through the IDDMP, USCIS will digitize its paper-based Alien Files (A-Files) so that they may be shared more efficiently within the Department of Homeland Security (DHS) and information contained within the A-Files may be shared with outside agencies. This PIA covers the IDDMP, a new IT system that digitizes the paper-based A-Files into a new electronic format.

Introduction

DHS through USCIS implements United States (U.S.) immigration law and policy through the processing and adjudication of applications and petitions submitted for citizenship, asylum, and other immigration benefits. USCIS also supports national security by preventing individuals from fraudulently obtaining immigration benefits and by denying applications from individuals who pose national security or public safety threats to the U.S.

USCIS is embarking on an enterprise-wide "Transformation Program" that will transition the agency from a fragmented, form-centric, and paper-based operational environment to a centralized, person-centric, consolidated environment utilizing electronic adjudication. The new operational environment will employ the types of online customer accounts used in the private sector. This "person-centric" model will link information related to an individual in a single account in order to facilitate customer friendly transactions, track activities, and reduce identity fraud. IDDMP is a key building block of the USCIS Transformation Program.

Currently to support its operations, the USCIS assembles a paper-based file, known as an A-File, which contains official record documents pertaining to individuals. Information from the A-Files may be shared with other authorized Federal, state, tribal, local or foreign government agencies or organizations, or international organizations, responsible for providing benefits, investigating or prosecuting violations of civil or criminal laws, or protecting our national security. USCIS developed the IDDMP to provide electronic access to these A-Files thus permitting simultaneous access to more than one user at any given time. The IDDMP manages the scanning, storing, updating, and accessing of digital A-Files.

The A-File is the record that contains all transactions involving an individual as he/she passes through the U.S. immigration and inspection process, and chronicles interactions with the U.S. Government. Previously the legacy Immigration and Naturalization Service (INS) performed all of

these functions. Since the formation of DHS these functions have been divided amongst the following three components: 1) Customs and Border Protection (CBP) which performs the border enforcement and inspection processes; 2) USCIS which performs the immigration benefit adjudication process; and 3) Immigration and Customs Enforcement (ICE) which performs the investigatory, deportation, and immigration court functions. Although USCIS is the custodian of the A-File, all three components create and use A-Files in the course of performing their mission requirements.

A-File scanning is performed at a contractor-owned and operated physical location called the Records Digitization Facility (RDF). The digitized A-Files produced by the contractor are sent to government's Quality Assurance (QA) system. After QA is performed, they are stored centrally, and images within the A-File are accessed and updated using the Electronic Document Management System (EDMS). For the purpose of this document, the RDF, QA system, and EDMS will be collectively referred to as the IDDMP. Although the digitized images within the file cannot be modified, the IDDMP has a search capability that enables an authorized user to locate needed information within the file, make notes, and add additional images to the file. Access to information in the digitized A-Files is provided to authorized Federal, state, tribal, local or foreign government agencies or organizations, or international organizations, responsible for providing benefits, investigating or prosecuting violations of civil or criminal laws, or protecting our national security.

This PIA covers DHS' use of digitized A-Files and the information contained therein. All external Information sharing will be governed by appropriate agreements (e.g., Memorandums of Understanding (MOUs), Interagency Security Agreements, etc.) which will be developed with external agencies prior to being granted direct access to EDMS setting forth terms and conditions as to how information is to be safeguarded. This PIA will be updated as these sharing agreements are approved.

Section 1.0
Information Collected and Maintained

1.1 What information is to be collected?

The IDDMP is not a data collection system. The program is not collecting any new information. Existing hardcopy A-Files, which contain the individual's official record material, much of which has been obtained directly from individuals, are digitized at the RDF and made available to authorized users electronically via EDMS. The A-File includes information such as: applications and petitions for benefits in accordance with immigration and nationality laws; vital documents (e.g., birth certificates, passports, marriage certificates); biometric information (e.g., photographs, fingerprints); enforcement supporting documents (e.g., RAP sheet); and other documents (e.g.,

naturalization certificates; tax returns; labor certifications; correspondence; court dispositions; interview notes). A-Files sometimes contain non-scannable media such as videotapes, audiotapes, and CDs. The contents of non-scannable media will not be included in the digitized A-File, but the A-File will note its existence.

Metadata (also known as summary data) used for indexing and searching the digitized files is extracted from the A-File during the initial digitization process. Metadata saved with every digitized A-File includes:

- Primary A-Number
- First Name
- Last Name
- Date of Birth (DOB)
- Country of Birth (COB)

The system is also capable of capturing the data elements listed below as metadata and storing it in the digitized file. Metadata (also known as summary data) used for indexing and searching the digitized files is extracted from the A-File during the initial digitization process. It is likely that the following information will be added by USCIS after the file is digitized by the RDF:

- Receipt Number(s)
- Secondary A-Number(s)
- Middle Name
- Fingerprint Identification Number
- Country of Citizenship
- Alias(es)
- Sex
- Mother's First Name
- Father's First Name
- Social Security Number
- FBI Number
- Certificate Number
- Naturalization Date
- Naturalization Court Number
- Naturalization Location
- Date of Entry
- Port of Entry
- I-94 Admission Number
- Passport Number
- Access Control Flag
- Driver's License Number

1.2 From whom is information collected?

The IDDMP does not collect new data directly from individuals, rather IDDMP digitizes the hardcopy A-File data collected originally from or on individuals covered by provisions of the Immigration and Nationality Act of the United States. Much of this data is collected directly from the individual requesting the immigration benefit either filed with USCIS or with Department of State. In addition, A-Files are created for individuals who are under investigation, or who were investigated by the DHS in the past, or who are suspected of violating the criminal or civil provisions of treaties, statutes, Executive Orders, and Presidential proclamations administered by DHS, and individuals who are witnesses and informants having knowledge of such violations. Once an A-File is digitized, authorized users can make notes electronically and add additional images to the file.

1.3 Why is the information being collected?

The information is used by USCIS and other DHS agencies for immigration benefits processing, law enforcement, and protection of national security. Storing A-File information in one system and then allowing multiple users to view the data reduces processing times. During the course of their official duties, DHS employees may make additions to the digitized file.

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

The Immigration and Nationality Act, 8 U.S.C. Section 1101 et seq.

The paper A-Files are scanned at the RDF and turned into digitized files. After QA is performed, they are stored centrally, and images within the A-File are accessed and updated using the Electronic Document Management System (EDMS).

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

The primary risk is unauthorized access to or disclosure of information contained within digitized A-Files. To mitigate this risk, a number of business and system rules have been implemented. Access to A-Files via IDDMP is given only to users that need it to perform their official duties. All authorized users must authenticate using a userid and password. Users are restricted from copying text, images, or content from the file. Lastly, through policies and procedures, DHS limits the use and access of all data in IDDMP to the purposes for which it was collected.

IDDMP provides users with a new function - the ability to perform full text searches of A-Files. With this function, there is a risk that users will search for information on individuals and topics beyond the scope of their work. This risk is mitigated by IDDMP training and the enforcement of DHS policies that limits the use and access of all data in IDDMP to the purposes for which it was collected. An audit trail will be kept for system access and all transactions that request, create, update, or delete information from the system. The audit trail, which includes the date, time, and user for each transaction, will be secured from unauthorized modification, access, or destruction, and kept for at least 90 days.

Section 2.0
Uses of the system and the information

2.1 Describe all the uses of information.

The information is used for immigration benefits processing, law enforcement, and protection of national security.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern (Sometimes referred to as data mining)?

DHS does not conduct data mining within the IDDMP.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

No new information will be collected from the individual. All information in IDDMP will be derived from paper-based records. Quality reviews are performed at the RDF to check that the paper A-Files are scanned into legible digitized files and that metadata is entered accurately. The RDF contractor performs a quality review in accordance with a generally accepted standard for choosing samples of files to check. In addition, the Quality Assurance contractor, co-located at the RDF, will sample the digitized A-Files in accordance with the Government-approved Quality Assurance Surveillance Plan. Pages are checked to ensure that they are fully rendered; properly aligned and ordered; free of distortions; and named correctly. Metadata entered at the RDF undergoes a quality control check. Discrepancies are identified, reviewed, and corrected. Discrepancies and resulting actions are logged.

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above-described uses.

Digitized A-Files are used for the same purposes as paper A-Files. Policies and procedures within DHS are in place to ensure that data is used in accordance with authorized uses for information contained within the A-File. Any new uses of A-File data will be analyzed as part of the System of Records Notice (SORN) process or in the development of data sharing agreements, as applicable, to ensure that they support the DHS mission and are consistent with the purpose for which the A-file data was collected.

Access to digitized A-Files via IDDMP is given only to users that need it to perform their work. In addition, all users must be authenticated by user ids and passwords and user privileges are governed by role assignments (i.e., general user, records administrator, and system administrator).

DHS components are ultimately responsible for ensuring that the data is used appropriately. This is done by the establishment of standard operating procedures that stipulate proscribed and permitted activities and uses, auditing requirements, and integrity controls.

Section 3.0
Retention

3.1 What is the retention period for the data in the system?

Immigrant records are retained for 75 years from the date the file is retired to the National Archives and Records Administration (NARA) or date of last action (whichever is later) and then destroyed (see NARA Disposition Schedule NC1-85-80-5/1).

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

NARA approved the retention schedule for the paper A-Files. The digitized A-File has the same retention schedule as the paper A-File, and will replace the paper file as the legal record once digitized.

3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

The A-Files are retained to support adjudication decisions, law enforcement uses, and protection of national security. Additionally, via an approved disposition and retention schedule, NARA has directed that the information be retained for a specified period. The information is retained for the specified period because the relationship between USCIS and the individual may span and individual's lifetime.

Section 4.0
Internal sharing and disclosure

4.1 With which internal organizations is the information shared?

The A-File is the record that contains all transactions involving an individual as he/she passes through the U.S. immigration and inspection process, and chronicles interactions with the U.S. Government. Previously, legacy INS performed all of these functions. Since the formation of DHS, these functions have been divided among the following three components: 1) CBP which performs the border and inspection processes; 2) USCIS, which performs the immigration benefit adjudication process; and 3) ICE, which performs the investigatory, deportation, and immigration court functions. Although USCIS is the custodian of the A-File, all three components create and use A-Files.

Once the A-File is digitized, information is accessed by all three components so that they may perform their mission requirements. Information contained within the A-File may also be shared with other components within DHS responsible for law enforcement activities and protection of national security.

4.2 For each organization, what information is shared and for what purpose?

The IDDMP shares the information contained in the system within DHS for benefits processing, national security, law enforcement, and other DHS mission-related functions. Information is also shared in order to support associated management reporting, planning and analysis, or other administrative uses that require access to the information contained in the A-File.

4.3 How is the information transmitted or disclosed?

In all cases the digitized data is transmitted within IDDMP (from scanning to the repository to users of the information in the system) on the DHS core network, an unclassified, secured wide area network. Other types of transmission or disclosure may be required in some circumstances. For example, encrypted A-File data may be securely transferred on portable media (e.g., encrypted CDs and thumb drives) or via encrypted email to authorized DHS employees when there is no direct connection to IDDMP. This is process adds additional security safeguards to the process for shipping the paper A-File that exists today which provides for appropriate security of the information.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated. For example, if a decision was made to limit internal sharing to certain components because of privacy or other concerns, include such a discussion.

The primary risk is unauthorized access to or disclosure of digitized A-Files. The digitized format is easier to search and easier to transport. DHS mitigates this risk through strategies such as access controls and policies; auditing; and other physical, technical and administrative controls. DHS limits the use and access of all data to purposes for which it was collected. Only employees who need access to the A-File to perform their official duties are granted access to IDDMP. System users must complete mandatory Computer Security Awareness training and IDDMP training. All contractors must sign non-disclosure agreements. Data must always be securely transferred. For example, if IDDMP data is transferred on portable media or via email to authorized DHS employees, National Institute of Standards and Technology (NIST) approved encryption is used to ensure that data is not tampered with en route and to prevent unauthorized personnel from viewing it.

Section 5.0
External sharing and disclosure

5.1 With which external organizations is the information shared?

As provided in the A-File and Central Index System SORN, information in the A-Files may be shared with other Federal, state, tribal, local or foreign government agencies or organizations, or international organizations, responsible for providing benefits, investigating or prosecuting violations of civil or criminal laws, or protecting our national security. Most often information is

shared with the Federal Bureau of Investigations (FBI), the Department of Justice (DOJ), or the Department of State (DOS).

5.2 What information is shared and for what purpose?

Information contained in digitized A-Files may be shared with organizations for the purpose of providing benefits, law enforcement, or other uses consistent with the routine uses described by the Privacy Act notice for the type of record requested. Information contained within the A-Files may be shared with DOJ for law enforcement and prosecutions, DOS for benefit determinations, and FBI for investigations. Outside agencies will not have direct access to the IDDMP. They will follow the current practice for physical A-Files which is to appear in person at the local USCIS office. They are required per the USCIS Records Operations Handbook, to work with their local USCIS office to view A-File information. After showing proper credentials and demonstrating a need to know, the representative will work directly with USCIS records personnel to view the relevant portions of the A-File.

5.3 How is the information transmitted or disclosed?

In this phase, no direct access to A-Files within the IDDMP will be provided to users outside of DHS; however, information contained within the A-File may be transmitted or disclosed to external organizations in one of two ways:

- DHS personnel may provide information contained in the A-File to external organizations who are co-located with DHS personnel who have access to the system; and
- USCIS may securely transfer encrypted A-File data by email or other encrypted portable media (e.g., CD, thumb drive) when there is no direct access to IDDMP. USCIS transfers the encrypted data to an authorized DHS employee who then allows an authorized representative from an outside organization to view it. (See 5.4 and 5.5 for additional information.)

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

At this time USCIS does not have blanket sharing agreements or MOUs in place with external organizations to provide access to the IDDMP. USCIS will work with external organizations on a case-by-case basis. If an authorized representative from an external organization provides a valid mission requirement for viewing contents of the A-File record and can show proper credentials, USCIS may allow him/her to view it with an USCIS employee present.

5.5 How is the shared information secured by the recipient?

Representatives from external organizations may visit a USCIS office and view information from A-Files. They are shown only the portions of the files that they need. External representatives may not make copies but they may take notes. Each time a file is viewed by an outside organization, a non-disclosure form is completed and added to the electronic A-File. (See section 5.2 above for additional details.)

5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

Federal government employees and their agents must adhere to the OMB guidance provided in OMB Memoranda, M-06-15, "Safeguarding Personally Identifiable Information", dated May 22, 2006 and M-06-16 "Protection of Sensitive Agency Information," dated June 23, 2006 setting forth the standards for the handling and safeguarding of personally identifying information. Contractors must also sign non-disclosure agreements.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated. For example, if a decision was made to limit external sharing, include such a discussion.

The primary risk is unauthorized access to or disclosure of information contained in digitized A-Files. The digitized format is easier to search and easier to transport. To mitigate this risk, the process for data sharing is strictly controlled by Office of Records personnel. As noted in 5.4 and 5.5 above, a representative must be authorized to see the information and only relevant portions of the A-File are provided. Lastly, representatives viewing the data must sign a non-disclosure which outlines the limits and restrictions regarding use of the data. Information provided to external entities may not be further shared outside of those entities without the prior written consent of DHS.

Section 6.0
Notice

6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice. If notice was not provided, why not?

The information contained within IDDMP is from existing paper A-Files. A System of Records Notice (SORN) for the A-File and Central Index System was published in the Federal Register on September 7, 2001 (66 FR 46813 Justice/INS 001A). The A-File and Central Index System SORN is being updated to address the IDDMP. It will provide notice as to the conditions of disclosure and routine uses for the information collected in the repository. The A-File and Central Index System SORN provides that any dissemination of information maintained within the repository be compatible with the purpose for which the information was originally collected. In addition, each form or application on which USCIS collects information contains the required Privacy Act notice regarding use and dissemination of the information.

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

Information scanned at the RDF is taken from an existing A-File that is a direct result of applications submitted by an individual (or on an individual's behalf) or enforcement actions undertaken by DHS. The A-File is necessary for the benefits adjudication process. If the applicant does not wish to provide the information that is stored in the A-File, his/her or request for immigration benefits may be denied. For A-Files created for other purposes (e.g., enforcement, investigations), the individual does not have an opportunity to decline.

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

An applicant provides consent by virtue of applying for a USCIS benefit. For A-Files created for other purposes (e.g., enforcement, investigations), the individual does not consent to particular uses of the information.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

The extent of notice and the opportunity to provide informed consent varies based on the particular purpose associated with the original collection of the information. In most cases notice is provided when the applicant fills out the form or application for benefits. In the law enforcement or national security contexts, notice or the opportunity to consent would compromise the ability of the agencies to perform their mission. In these cases, notice and consent may not be available.

Section 7.0
Individual Access, Redress and Correction

7.1 What are the procedures which allow individuals to gain access to their own information?

The process for gaining access to one's information in an A-File is the same regardless of how it is stored (digital or paper). All requests for access must be made in writing and addressed to the Freedom of Information Act/Privacy Act (FOIA/PA) officer at USCIS. Individuals who are seeking information pertaining to themselves are directed to clearly mark the envelope and letter "Privacy Act Request." Within the text of the request, provide the A-File number and/or the full name, date and place of birth, and notarized signature of the individual who is the subject of the record, and any other information which may assist in identifying and locating the record, and a return address. For convenience, Form G-639, FOIA/PA Request, may be obtained from the nearest DHS office and used to submit a request for access. The procedures for making a request for access to one's records can also be found on the USCIS web site, located at www.uscis.gov.

An individual who would like to file a FOIA/PA request to view their USCIS record may do so by sending the request to the following address:

U.S. Citizenship and Immigration Services
National Records Center
FOIA/PA Office
P.O. Box 648010
Lee's Summit, MO 64064-8010

7.2 What are the procedures for correcting erroneous information?

The correction procedures for digitized A-Files are the same as paper A-Files. Individuals may have an opportunity to correct their data during interviews, otherwise they may submit a redress request as described by each program collecting the data or directly to the USCIS Privacy Officer who refers the redress request to the appropriate program office. When a redress is made, the change is added to the original information in the file. USCIS then goes the through process of making corrections in its systems, including auxiliary ones.

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

Information contained in the system is a digitized version of what is contained in the paper A-File. As such, individuals are not notified about procedures for the correction of errors contained within IDDMP. Redress procedures are established and operated by the program through which the data was originally collected.

7.4 If no redress is provided, are alternatives available?

Redress is provided (see 7.2 above). Redress procedures are established and operated by the program through which the data was originally collected.

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, what procedural rights are provided and, if access, correction and redress rights are not provided please explain why not.

The redress requests that might arise with respect to the various data collections stored in IDDMP shall be addressed by the program through which the data was collected.

Section 8.0
Technical Access and Security

8.1 Which user group(s) will have access to the system? (For example, program managers, IT specialists, and analysts will have general access to the system and registered users from the public will have limited access.)

Government personnel and contractors have access to the IDDMP. An individual is assigned one of three access roles: general user (assigned for example to an adjudicator or an ICE investigator), records administrator, or system administrator. General users can search, view, and add notations to A-Files. Records administrators can search and view files; edit metadata; and update security parameters (i.e., display the record on search lists, but not allow general users to access it). System administrators can search and view files; set access control permissions for users; delete files; update metadata; and set the access control flag (i.e., suppress an A-File and metadata from all search lists). If and when regular access is granted outside of DHS with external government agencies this PIA will be updated and an MOU will be executed. Public access will not be granted to the IDDMP.

8.2 Will contractors to DHS have access to the system? If so, please submit a copy of the contract describing their role to the Privacy Office with this PIA.

Some contractors have access to the digitized A-Files. The extent of access varies based on the need to fulfill the requirements of the contract under appropriate non-disclosure and use limitations. Three contracts are currently in place to support the IDDMP:

- Contract for converting the A-Files from paper to digital;
- Contract for quality assurance of the scanning process; and
- Contract for providing and maintaining the EDMS

The scope of the RDF scanning contract covers all activities related to the scanning operation at the Contractor-owned and operated facility, including needs assessment and analysis services, records management, document shipping and receiving, scanning and digitization, records control, facilities operations, and provision of a temporary file storage solution. The Quality Assurance contract covers the sampling of the digitized A-Files for a quality assurance review to check that images are: fully rendered; properly aligned and ordered; free of distortions; and named correctly. The scope of the contract for the EDMS includes design, development, testing, and deployment activities for the system that houses the digitized A-Files and provides user access to them.

All contractors are required to pass background checks. All IT contracts must have Privacy Act compliance language present before being awarded according to DHS contracting guidelines based on the Federal Acquisition Regulation and other Executive Orders, public law, and national policy. All access to IDDMP follows the logical access controls set up for access to USCIS computer systems. Access controls are applied to contractors and to federal employees equally.

8.3 Does the system use "roles" to assign privileges to users of the system?

Access to IDDMP is assigned based on the specific role of the user. Roles are created for each level of access required for individuals to perform their official duties. These roles include general user, records administrator, and system administrator. Supervisors assign these roles and their associated access based upon a user's need to know and level of security clearance.

8.4 What procedures are in place to determine which users may access the system and are they documented?

Both contractors and government personnel have access to the IDDMP. Security procedures are in place in accordance with the system security plan and the USCIS systems lifecycle methodology. This plan is the primary reference that documents system security responsibilities, policies, controls, and procedures. Access to IDDMP is controlled via the Active Directory which stores user roles. (Active Directory is an agency-wide software tool that manages userids and role assignments. It will ultimately be used to provide the agency and its components with single sign-on.) IDDMP uses the userid and password to retrieve the role (e.g., general user, records administrator, systems administrator) from Active Directory. IDDMP then assigns the appropriate permissions based on the role stored in Active Directory. DHS supervisors assign roles so that users have appropriate access to perform their particular job functions.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

Roles are assigned by a DHS supervisor and are reviewed regularly to ensure that users have appropriate access to IDDMP. Roles are stored in Active Directory and are used by IDDMP to assign the appropriate permissions (see 8.4 above). Access is audited and the audit logs are reviewed on a regular basis. Individuals who no longer require access are removed from the access list.

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

The IDDMP has developed a system security plan that is in accordance with the USCIS systems lifecycle methodology. This plan is the primary reference that documents systems security responsibilities, policies, controls, and procedures.

Access to records is controlled through the use of security parameters. Based on the sensitivity of information in the file, a Records Administrator evaluates the level at which the security parameter category should be set. The three security parameter categories are: "Open", "Controlled", or "Private." The Records Administrator can set the parameter to "Open" or "Controlled", while the System Administrator can set it to "Open", "Controlled", or "Private." Open files are A-Files that may be searched for, discovered, and viewed by all IDDMP users. Controlled files show up in search results, but a Records Administrator must make the file available for viewing if appropriate. Private files do not appear in search results and cannot be viewed.

If IDDMP data is transferred on portable media or via email to authorized DHS employees, NIST-approved encryption will be used to ensure that data is not tampered with en route and to prevent unauthorized personnel from viewing it.

The system shall comply with policy detailed in DHS MD 4300, Information Technology Systems Security, and the associated DHS 4300A, Sensitive Systems Handbook for auditing transactions. An audit trail will be kept for system access and all transactions that request, create, update, or delete information from the system. The audit trail, which includes the date, time, and user for each transaction, will be secured from unauthorized modification, access or destruction, and kept for at least 90 days. QA personnel at the RDF will regularly review the audit log to verify that the A-Files have been properly digitized and the EDMS systems administrator will review the audit log for all other system access activities.

Misuse of data in the IDDMP is prevented or mitigated by requiring that users conform to appropriate security and privacy policies, follow established rules of behavior, and are adequately trained regarding the security of their systems.

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

All DHS system users complete mandatory annual computer security awareness training which addresses some privacy issues. Users will also complete IDDMP training.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

The system is built according to FISMA requirements. The Certification and Accreditation (C&A) process, as identified in the USCIS systems lifecycle methodology, is being conducting while the system is in development. The C&A process will be completed prior to the system being operational.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

Unauthorized data access is the primary risk factor as the digitized format is easier to search and transport. DHS has a robust security program that employs physical, technical and administrative controls. These controls are validated through a C&A process on a regular basis. Access to IDDMP data is closely controlled by applying discrete user roles for three levels of access (i.e., general user, records administrator and system administrator). Roles are assigned based on the users' job function and are enforced via Active Directory after users are authenticated to the system (see section 8.4 above). These security requirements form the basis for a system security plan that is developed in accordance with the USCIS systems lifecycle methodology.

Section 9.0 Technology

9.1 Was the system built from the ground up or purchased and installed?

Significant sections of this system are contractor owned and operated; However, it is primarily made up of configured Commercial off the Shelf (COTS) applications that have been purchased for use by the IDDMP. Elements of the solution are constructed as custom software components to meet the unique needs of DHS.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

System designers and operational users of the system are working closely with privacy professionals to ensure compliance with the Privacy Act and the requirements of FISMA. The team is working within a comprehensive Computer and Telecommunications Security (C&TS) Program to address the integrity, confidentiality, and availability of sensitive but unclassified (SBU) information during collection, storage, transmission, and disposal. In addition, the team follows

the USCIS systems lifecycle methodology process, which is supplemented with information from DHS and USCIS security policies and procedures as well as the National Institute of Standards Special Procedures related to computer security and FISMA compliance.

9.3 What design choices were made to enhance privacy?

To protect against unauthorized disclosure, the system is designed to support discreet user roles and provide three levels of access to digitized A-Files – general user, records administrator, and system administrator. Access control rules are based on the user role, i.e., need to know of the person accessing the files. These security requirements form the basis for the system security plan that is developed in accordance with the USCIS systems lifecycle methodology. The system records and prepares an audit trail for all transactions that create, update, request, or delete information from the system. The audit trail, which includes the date, time, and user for the each transaction, will be reviewed regularly.

Conclusion

The IDDMP provides a valuable service to USCIS, DHS, and its external data sharing partners by providing electronic access to A-Files which were previously only available in hardcopy. While there are privacy risks associated with digitizing and providing electronic access to A-Files, these risks are mitigated by technical safeguards and supporting policies and procedures. These mechanisms include: system design and controls; DHS policies and security programs; training; and clearly articulated data sharing guidelines and operating procedures.

Responsible Officials

Elizabeth Gaffin
USCIS, Privacy Officer
Department of Homeland Security

Approval Signature Page

_____

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security