Privacy Impact Assessment
for the

OPLA Case Management System

DHS/ICE/PIA-036

June 26, 2013

Contact Point
Peter S. Vincent
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-5000

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
202-343-1717

Abstract

The U.S. Immigration and Customs Enforcement (ICE) Office of the Principal Legal Advisor (OPLA) is establishing a new information system called the OPLA Case Management System (OCMS), which is a case and document management system supporting the general legal work and specialized immigration court litigation performed by OPLA personnel. OCMS is replacing OPLA's existing case management system, the General Counsel Electronic Management System (GEMS). Because OCMS collects and processes personally identifiable information (PII) about federal employees, aliens, and members of the public, ICE is conducting this PIA to assess the privacy issues associated with the collection, maintenance, and use of this information.

Overview

Background

OPLA employs attorneys and support staff at ICE headquarters and at various field offices, which are referred to as Offices of Chief Counsel. OPLA personnel in these locations have various responsibilities including providing legal advice to the ICE Director and ICE program offices, operating the agency's ethics program, responding to Congressional requests, responding to taskings from both offices within ICE and from agencies outside of ICE, such as agencies within the Department of Homeland Security (DHS) and the U.S. Department of Justice (DOJ), and handling all federal court and administrative litigation against the agency such as tort claims, Freedom of Information Act (FOIA) claims, contract claims, Privacy Act claims, and employment claims. OPLA personnel are also responsible for representing the agency in removal proceedings before immigration judges in U.S. immigration courts and for advising the ICE offices of Enforcement and Removal Operations (ERO) and Homeland Security Investigations (HSI) regarding legal issues that arise during the course of their law enforcement and investigative work. Currently, GEMS serves as the case management system for OPLA, storing information related to immigration cases and certain limited non-immigration-related cases and projects on which OPLA personnel are working.[1] GEMS is being retired and replaced by OCMS to enable OPLA personnel to more easily track their cases and projects and maintain information relevant to them.[2] It will also help OPLA managers to more efficiently manage and assess the workload of their staff.

OCMS

[1] *See* DHS/ICE/PIA-002, General Counsel Electronic Management System (GEMS) PIA and PIA update, at http://www.dhs.gov/privacy-documents-ice.
[2] It should be noted that not all of the capabilities discussed in this PIA will be available when OCMS first deploys. Some capabilities will be available when the system initially deploys while others will be deployed in future releases.

OCMS is a web-based case and document management system used by OPLA personnel to manage their work. All records previously stored in GEMS will be migrated to OCMS prior to the OCMS deployment. The benefits of the system include:

- For U.S. immigration court cases and appeals, it reduces OPLA's reliance on and use of the paper alien file (A-File)[3] because OCMS is able to electronically store documents and information typically found in the A-File;
- It makes information about a case or project available to ICE OPLA, HSI, and ERO personnel who have a need to know to perform their official duties;
- It enhances data accuracy and consistency across cases and projects by using field-level validation and system-to-system connections to obtain relevant data from other systems (Note: there is more information below and in the appendix about the system-to-system connections);
- It provides a robust reporting capability for both routine and ad hoc reports; and
- It serves as a knowledge management resource enabling users to reference or build upon previous legal work or research performed by other users.

OCMS is comprised of four main components, which are described below: (1) Case Management; (2) Project Management; (3) Document Management; and (4) System Administration.

Case Management: The case management component is used for storing information about all of the various types of cases that OPLA personnel work on before administrative courts (including U.S. immigration courts) and those in federal courts (e.g., U.S. District Courts, U.S. Courts of Appeal). The system stores a variety of types of information, such as pre-trial notes, trial notes, and post-trial notes; legal memoranda, such as those stating positions for litigation, in draft or final form; notes to investigators; hardcopy and online research; information about individuals involved in cases including attorneys, aliens, judges, witnesses, legal representatives, and other individuals; records or information from agency recordkeeping systems, including electronic systems and A-Files, depending on the litigation needs of the ICE attorney; reports of investigations, statements, and arrest reports; correspondence; court filings; and logistical information regarding hearings including the hearing date, time, and location; and due dates for pleadings and motions. Much of the information stored in the case management component of OCMS is attorney-client privileged or attorney work-product information.

Project Management: The project management component is used to track projects and tasks, other than the administrative and federal court cases described above, that are performed by OPLA attorneys and support staff. There are no restrictions on the types of projects that users can create. Projects may involve any number of activities including providing legal advice to the ICE Director or program offices, reviewing or creating policies, working on budgets, and responding to taskings and congressional inquiries. The

[3] For more information on the A-File, see DHS/USCIS/PIA-003, Integrated Digitization Document Management Program (IDDMP) PIA (January 5, 2007), at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscis_iddmp.pdf and DHS/USCIS-001 - Alien File, Index, and National File Tracking System of Records SORN, 76 FR 34233 (June 13, 2011) at http://www.gpo.gov/fdsys/pkg/FR-2011-06-13/html/2011-14489.htm.

project management component stores, organizes, and tracks information about each project including related events, assignments, and individuals involved with the project.

Document Management: The document management component is used as a repository for documents and other files (including but not limited to Word documents, Excel spreadsheets, PowerPoint slides, Portable Document Format (PDF) documents, video files, and audio files) that pertain to cases and projects within the system. Users upload files associated with a case or a project and the system allows users to assign metadata elements to them such as case number, alien registration number (A-Number), or project name; author's name; office location; title of the document; and type of document. The metadata are used to permit easy file retrieval and searching. The document management component also supports the editing of draft documents until they are complete by tracking the version history of files and allowing users to access previous versions.

System Administration: The system administration component is used by system administrators to maintain the system and to troubleshoot issues that arise. System administrators' duties include creating, modifying, and deleting user accounts; customizing menus, business rules, and reports in the system; and monitoring the system's audit trail to ensure that the system is being used properly.

Information related to cases and projects is either manually entered into OCMS by OPLA users or is obtained via connections that OCMS has with other systems. OPLA personnel collect information related to cases and projects from a variety of sources including claimants, court pleadings, public records, other federal government systems, subscription-based information services, publicly available websites, and state and local criminal justice systems. The appendix to this PIA lists the federal government systems that are a source of information for projects and cases in OCMS and the type of information that each provides. This appendix will be updated as systems are added or removed as sources of information, as there are changes in the information that the systems provide, or when there are changes in the method by which information is shared with OCMS.

User Roles and System Access

Users are only able to input and view information in the system as authorized by their assigned user role. Immigration-related cases and projects are able to be viewed and edited by all OPLA attorneys and support staff at headquarters and in the various field offices. Because cases often transfer from jurisdiction to jurisdiction very quickly, OPLA requires that personnel in multiple offices have access to these cases in OCMS. OPLA headquarters personnel require this access to support the field offices by coordinating cases and advising on legal matters whenever the need arises.

Non-immigration-related cases and projects, however, are not accessible by all users. They are only accessible by personnel in the OPLA division assigned to that particular case or project. Access to non-immigration-related cases and projects is granted by the case or project's creator to other OPLA users who have an official need to know. In addition, OCMS allows for field level security, meaning that some fields in a case or project will not be available for every user to access or edit depending on the OPLA division

or user role that they are assigned. For example, only National Security Law Section division members are allowed to edit and enter national security-related information in immigration-related court cases.

In addition to OPLA personnel using the system, designated personnel in the ICE offices of ERO and HSI use the system. These personnel have been designated and approved for access by their supervisor, and are granted read-only access to all immigration-related cases in OCMS. They are not able to access any non-immigration-related cases or any projects in the system. ERO and HSI personnel need access to the immigration-related cases because they are simultaneously working on the same cases from a law enforcement perspective and at any point in time may need to see the status of a case pending before the immigration court to use that information to inform their next steps on their enforcement case. As described above, the immigration-related cases are extremely mobile as the cases often transfer from jurisdiction to jurisdiction very quickly, necessitating multiple jurisdictions of ERO and HSI users all needing to have access to a case.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

As noted above, in addition to handling both immigration-related and non-immigration-related cases, OPLA personnel provide legal advice, operate the agency's ethics program, respond to Congressional requests, and respond to taskings. Given the array of work that OPLA personnel perform and the numerous laws that ICE is responsible for enforcing, the legal authorities listed below are a representation of the main authorities relevant to the execution of ICE's duties and responsibilities: the Homeland Security Act of 2002; Immigration And Nationality Act of 1952, as amended; Illegal Immigration Reform and Immigrant Responsibility Act of 1996; the Illegal Immigration Reform and Immigrant Responsibility Act of 1996; the Immigration and Naturalization Service Data Management Improvement Act of 2000; Visa Waiver Permanent Program Act of 2000; the USA Patriot Act; the Enhanced Border Security and Visa Entry Reform Act; the Tariff Act of 1930, as amended; the Brady Handgun Violence Protection Act of 1993; FY 2008 Consolidated Appropriates Act; the Justice for All Act of 2004; the Consolidated Security, Disaster Assistance, and Continuing Appropriations Act of 2009; DNA Fingerprint Act of 2005; Adam Walsh Child Protection and Safety Act of 2006; the Freedom of Information Act, as amended; the Privacy Act of 1974; the Federal Records Act; the Ethics in Government Act of 1978; the Bank Secrecy Act; the Trade Secrets Act; the Federal Tort Claims Act; E.O. 9397; E.O. 12674 (as modified by E.O. 12731); E.O. 12958; 2 U.S.C. 1220, 5 U.S.C. §§ 301, 1204, 7301, 7351, 7353; 6 U.S.C. §§ 121, 201-203; 8 U.S.C. §§ 1103, 1105, 1153-1155, 1183, 1201-1204, 1221, 1222, 1225, 1226, 1229, 1231, 1281, 1302-1306, 1324, 1357, 1360, 1363, and 1365; 18 U.S.C. §§ 371, 544, 545, 554, 1905, 1956, and Chapter 27; 19 U.S.C. §§ 1, 8, 66, Chapter 4, 2701 and 2702; 28 U.S.C. §§ 2671-2680; 29 U.S.C. §§ 209, 211, 216, 217, 625; 31 U.S.C. §§ 1353, 5311-5330; 40 U.S.C. § 1315; 50 U.S.C. §§ 1701-1706 and 2410; 19 CFR Parts 171 and 172; 22 CFR 41.22; 28 CFR Part 28; 31 CFR Part 103.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

OPLA personnel handle a wide variety of cases and projects. The following SORNs apply to the various types of information maintained in OCMS:

- EEOC/GOVT-1 - Equal Employment Opportunity in the Federal Government Complaint and Appeal Records SORN, 67 FR 49338 (July 30, 2002);
- MSPB/GOVT-1 - Appeals and Case Records SORN, 67 FR 70254 (November 21, 2002);
- OGE/GOVT-1 - Executive Branch Personnel Public Financial Disclosure Reports and Other Name-Retrieved Ethics Program Records SORN, 68 FR 3097 (January 22, 2003) (correction published 68 FR 24722 (May 8, 2003));
- OGE/GOVT-2 - Executive Branch Confidential Financial Disclosure Reports SORN, 68 FR 3097 (January 22, 2003) (correction published 68 FR 24722 (May 8, 2003));
- DHS/ALL-001 - Department of Homeland Security (DHS) Freedom of Information Act (FOIA) and Privacy Act (PA) Record System SORN, 75 FR 50846 (August 18, 2010);
- DHS/ALL-013 - Department of Homeland Security Claims Records SORN, 73 FR 63987 (October 28, 2008);
- DHS/ALL-016 - Department of Homeland Security Correspondence Records SORN, 73 FR 66657 (November 10, 2008);
- DHS/ALL-017 - Department of Homeland Security General Legal Records SORN, 76 FR 72428 (November 23, 2011);
- DHS/ALL-018 - Department of Homeland Security Grievances, Appeals, and Disciplinary Action Records System of Records SORN, 73 FR 61882 (October 17, 2008);
- DHS/ALL-020 - Department of Homeland Security Internal Affairs, 73 FR 67529 (November 18, 2008);
- DHS/ICE-003 General Counsel Electronic Management System (GEMS) SORN, 74 FR 41914 (August 19, 2009).

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes. The environment in which OCMS will operate has already undergone a Security Authorization. It received its Authority to Operate on May 15, 2012.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Because GEMS is being retired, ICE will update the GEMS record retention schedule (N1-567-09-007) to rename it to OCMS and make minor updates as needed. The retention period for the immigration-

related cases that GEMS retains and OCMS will retain is not being modified. The remainder of the records in OCMS (non-immigration related case and project records) will be covered by the forthcoming Department of Homeland Security Legal Records retention schedule discussed in more detail in Section 5.1.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Although ICE does not use any forms to collect information about individuals for direct entry into OCMS, the system does contain some information collected pursuant to the Paperwork Reduction Act, to include OGE Form 278, Executive Branch Personnel Public Financial Disclosure Report (OMB No. 3209-0001); OGE Form 450, Confidential Financial Disclosure Report, Executive Branch (OMB No. 3209-0006); SF 95, Claim for Damage, Injury, or Death (OMB No. 1105-0008); and the DHS Form N-400, Application for Naturalization (OMB No. 1615-0052). The information from these forms, and in some cases the forms themselves, may be uploaded to OCMS because they directly relate to cases that OCMS users are working on.

Section 2.0 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.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

OCMS collects and maintains various types of information related to cases and projects. All cases and projects will be assigned a unique system-generated identification number.

For all types of cases, OCMS maintains information related to the case including pre-trial notes, trial notes, and post-trial notes; legal memoranda, such as those stating positions for litigation, in draft or final form; notes to investigators; records or information from agency recordkeeping systems, including electronic systems and A-Files, depending on the litigation needs of the ICE attorney; reports of investigations, statements, arrest reports, and charging documents; evidence; pleadings; briefs; correspondence; and court filings. The system also contains logistical information regarding hearings including the hearing date, time, and location; type of hearing; and due dates for pleadings and motions.

For immigration-related cases, OCMS also maintains biographic information about aliens including name, A-Number, address, telephone number, date of birth, age, nationality, language, known alias(es), and last known address; as well as information about individuals involved in cases including attorneys (including federal government attorneys and defense attorneys), aliens, judges, family members,

individuals who employ or sponsor the alien for an immigration benefit, witnesses, legal representatives, and other individuals who provide representation and assist respondents in removal proceedings. The information maintained for these individuals includes business contact information including title, place of employment, address, phone number, fax number, and email address. OCMS contains case history, including actions taken and the disposition of a case at the initial and appeal levels, information on A-File locations, the transfer of A-Files, and the transfer history of A-Files. OCMS also contains information on immigration applications, such as naturalization applications, which includes information about the alien, the dates the application was received and filed, and work authorization grants. Finally, information is captured regarding visa applications and visas that were issued, including the visa applications themselves, the visa's issue date, and the visa's expiration date.

For non-immigration-related cases, OCMS maintains information about the litigants, attorneys, witnesses, victims, and other persons involved directly or tangentially in the case. This could include any information that is disclosed or revealed during pre-trial negotiations, pleadings filed in court, discovery, and at trial. The categories of information collected or maintained for any particular litigation matter will vary tremendously depending on the type of litigation and the nature of the case. For example, a litigation matter that arises as a result of a tort claim filed by an individual injured in a car accident with an on-duty agency employee may result in OCMS maintaining information about the individual, including his or her name, address, and contact information; information about the car accident; details about the individual's driver's license status and car ownership; and medical information related to injuries associated with the accident.

For projects, OCMS maintains information about the particular subject matter of the project including the project type, time spent working on the project, the ICE program office being supported by the project (i.e., the "client" office), project history including actions taken by the attorney or support staff on the project, and documents associated with the project. This information may include PII. Because projects vary widely – from administrative matters to requests for legal advice by an agency employee or program office – the nature of the information collected and maintained in OCMS for projects is varied and dependent on the specific project. For example, a request for legal advice on a personnel matter may result in the PII of the employee and supervisor involved in the matter being maintained in OCMS. Another example is requests for legal reviews of agency responses to constituent inquiries from members of Congress may result in the constituent's PII being collected and maintained in OCMS.

OCMS is able to generate various reports. Standard reports, which may provide statistics and metrics regarding projects and cases, are used by OPLA and ICE management to report such things as the average life cycle of a case or to help management measure the level of effort on a project or case so that appropriate resources can be allocated to it. Users are also able to run ad hoc reports as well. All reports may include PII about individuals involved in the case or project if this information is included as part of the information to be in the report.

2.2 What are the sources of the information and how is the information collected for the project?

The information stored in OCMS is derived from various sources. OPLA may receive requests for legal advice or assistance from any part of ICE or DHS and, if the request relates to an ICE matter, any DHS employee or contractor or any ICE record or file, including A-Files, may be a source of the information in OCMS. OCMS also receives information from other federal government systems. The appendix to this PIA lists the specific federal government systems that are a source of information for projects and cases in OCMS. OCMS may also contain information that users input or upload from subscription-based information services that provide online legal research services and commercial services such as people finders. OCMS may also contain information that users input or upload from the DOJ's federal court electronic filing system, Public Access to Court Electronic Records (PACER) System, or from publicly available records (including websites) and academic databases such as Cornell Law School. OCMS users may also manually input or upload data from state and local criminal justice records, whether paper or electronic documents. Finally, information can be gathered from events that happen at hearings or trials, and from interviews conducted with individuals.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

As noted above, OCMS users may use information collected from publicly available commercial sources or publically available data including subscription-based information services that provide online legal research services and commercial services such as people finders, state and local criminal justice systems, and academic databases. This information is queried in relation to a case or project and entered manually into OCMS by the user if it is relevant to the case or project. For example, if an immigration case involves a state or local crime, the OCMS user may query a state or local criminal justice system to gather information about the crime including future hearing dates or to see if there has been a resolution to the criminal case. The user then enters relevant information into OCMS.

2.4 Discuss how accuracy of the data is ensured.

Procedures are in place for checking the accuracy of data as it is entered into the system for both cases and projects. For some fields in OCMS, data validation and formatting checks help ensure that valid information is entered and that the information is entered in a specific format, thus eliminating the possibility of multiple variations of a single data item. For example, when users enter a date in a date field in OCMS, they are forced to enter only numbers in a particular format. This ensures that dates are uniformly recorded in the system. Additionally, the case number field for the immigration-related cases will only allow numbers to be entered. Text cannot be entered in the field. Business rules also help with data accuracy by customizing drop-down fields that users can select based on information that has previously been entered in the record.

Protections are also built into the system to help prevent duplication in the creation of cases and projects. For example, before creating a new immigration-related case in OCMS, the attorney searches the individual's A-Number to see if a case already exists for the individual. If no case is found, OCMS searches other systems with which it has a system-to-system connection and uploads any information it finds to create a case in OCMS, such as alien biographic information, hearing information, or judge and attorney information. If none of the systems have any information for the given A-Number, the OCMS user creates the case manually. Once a case is created in OCMS, OCMS periodically searches systems with which it has a system-to-system connection to get any updated information that they may have for the given A-Number thus helping to mitigate the risk of outdated information in OCMS. This process also helps to ensure that inconsistencies in individuals' data among these systems are identified and addressed.

In order to ensure that OCMS receives the most accurate and up-to-date information from the systems with which it has system-to-system connections, various protections have been put in place. Prior to developing the system, OPLA looked at the various data elements provided to OCMS via system-to-system connections. Some data elements are contained in several systems, and in order to address the possibility that OCMS might receive conflicting information from these systems, OPLA identified the external system which it considered the "authoritative source" for that data element given OPLA's intended use of that data. Thus, if OCMS received conflicting information for a particular data element, OCMS would know which value to retain for the given data element in OCMS. For example, the custody status field in OCMS is only updated by the Enforcement Integrated Database (EID)[4] because EID is the system that ICE uses to maintain arrest, booking, case initiation, detention, and removal data on aliens arrested by ICE for immigration violations and placed into proceedings in immigration court. The authoritative source for the A-Number field is the Department of Justice (DOJ), Executive Office of Immigration Review's (EOIR) Immigration Review Information Exchange System (IRIES)[5] because EOIR maintains the official record of proceeding and uses the A-Number as the "case number" for the proceeding.

Additionally, if OCMS's connection with another system provides a new name for an individual, the original name in the OCMS record is not overwritten. The new name is added to the "Also Known As" list thereby adding the updated information but not destroying the original information. Furthermore, OCMS allows users to view the data ingested by OCMS from any external system for which there is a system-to-system connection (known as the "live fetch page"). This allows OCMS users to validate that the information shown in OCMS system is the most up-to-date and accurate and the same data as contained in the external system. Additionally, updates to cases are captured in the system's audit trail. Each case has

[4] *See* DHS/ICE/PIA-015, Enforcement Integrated Database (EID) PIA and PIA update, at http://www.dhs.gov/privacy-documents-ice.

[5] The primary mission of the Executive Office for Immigration Review (EOIR) is to adjudicate immigration cases. Under delegated authority from the Attorney General, EOIR conducts immigration court proceedings, appellate reviews, and administrative hearings. The Case Access System for EOIR (CASE) is EOIR's case and court scheduling system, and IRIES is used as a mechanism to retrieve and share the information from CASE with other systems including OCMS. For more information on CASE, see the CASE PIA located at http://www.justice.gov/opcl/eoir_pia.pdf. Additionally, DOJ does not consider IRIES a system. DOJ views IRIES as a "pass through" mechanism for passing data from CASE to other systems and thus there is no PIA or SORN for IRIES.

its own audit history that shows: (1) when the updates occurred; (2) the previous value for any data element that was updated; (3) whether the update occurred manually or via a system-to-system connection; and (4) the individual who made the update. Audit histories can be examined by system administrators and system security personnel in the event of a question or problem. Finally, in the future, OCMS will display to the user the system from which each ingested data element was received, allowing users to know with specificity the source of each data element.

Information from an authoritative source system cannot be modified by OCMS users. It can be corrected either by an OCMS system administrator who manually corrects the error in OCMS, or by an OCMS user who contacts the agency that provided the information and alerts them about the error. Once the information from the authoritative source system has been updated, OCMS retrieves the information via the system-to-system connection it has with the system.

As noted above, HSI and ERO users are given read-only access to the system and cannot edit, create, or delete records. This helps to ensure data accuracy and integrity as it prevents non-OPLA employees from inappropriately or erroneously modifying the information in an OCMS case.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that there could be an over-collection of information in OCMS.

Mitigation: As noted above, OPLA personnel gather information related to their cases and projects from various sources including other federal government systems, online legal research services, publicly available records (including websites), and academic databases but they only access systems that they need in order to perform their job. Only information relevant to cases and projects is added to OCMS and part of the training that OCMS users receive addresses the requirement to only collect relevant information in the system. The training also covers the procedure for removing non-relevant information from the system. The collection of relevant information and removal of non-relevant information is also addressed in the OCMS standard operating procedures and user manual.

Privacy Risk: There is a risk of poor data quality and integrity because data is often manually entered into OCMS.

Mitigation: This risk is reduced in several ways. First, OCMS often ingests information via connections with other systems, such as biographic information about aliens in removal proceedings in immigration court. As noted above, ICE looked at the various data elements provided to OCMS via system-to-system connections and determined what the authoritative source for each would be. Additionally, the information that is considered authoritative from its source cannot be changed by OCMS users. This electronic sharing removes the need for certain key data to be manually entered in the system and thus helps reduces the chance for inaccurate data in the system. Additionally, not all users can enter data into the system. Only OPLA personnel who have access to the system and who are trained to use the system can

enter information. Finally, protections such as data validation, formatting checks, and customized drop down fields help ensure that the correct data is collected and accurately entered in the system.

Privacy Risk: There is a risk to the quality and integrity of the data in OCMS due to reliance on external systems.

Mitigation: As noted above, prior to developing OCMS, ICE looked at the various data elements being provided to OCMS via system-to-system connections and determined what the authoritative source system for each would be. Additionally, OCMS users cannot change information that is considered authoritative. If an OCMS user discovers an error with authoritative information, the user contacts the agency that provided the information and alerts them about the error and once the information from the authoritative source system has been updated, OCMS retrieves the updated information. Identifying authoritative source systems, using system-to-system connections to provide information to OCMS, and preventing users from changing authoritative information help reduce risks to date quality and integrity.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

OPLA uses the information in OCMS in various ways. OPLA attorneys and support staff use it to manage their cases and to manage various projects including providing legal advice or representation outside the context of immigration and removal proceedings, reviewing or creating policies, working on budgets, and responding to taskings and congressional inquiries. OPLA personnel also use OCMS as a resource to identify previous research performed, advice provided, and cases or claims adjudicated. OPLA management uses OCMS to compile information and statistics to assess workloads, the efficiency of work performed, and to allocate resources in headquarters offices and in field offices in order to better carry out the agency's mission.

A-Numbers are used as the case identification number in OCMS for immigration-related cases.[6] OCMS also generates a unique identifying number for each OCMS case or project created.

ICE ERO and ICE HSI personnel use OCMS information to obtain information about the status of specific alien removal cases. ERO and HSI personnel need this information because they are simultaneously working on the same cases from a law enforcement perspective and, at any point in time, they may need to access a case to view the case status in immigration court as well as to use that information to inform their next steps on a case. ERO personnel in particular need this access to coordinate removal activities, such as

[6] If the alien does not yet have an A-Number, the system will not permit the user to create an immigration-related case matter. Instead, the OCMS user will create a project in OCMS to temporarily track the immigration-related case until an A-Number is assigned. Once an A-Number is assigned, the project can be linked to the case that is created for that A-Number so no information is lost regarding that case.

arranging transportation and obtaining travel documents from an alien's home country, and to carry out the removal, once they learn that a removal case has ended and the alien is now removable.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No, OCMS does not use any technology to conduct electronic searches, queries, or analyses in order to discover predictive patterns or anomalies in the information in the system.

3.3 Are there other components with assigned roles and responsibilities within the system?

No, only ICE personnel are able to access or use the system. Personnel from other DHS components are not able to access the system.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk of unauthorized disclosure of information in the system by users.

Mitigation: In the standard operating procedures for OCMS and in the training provided to system users, individuals are instructed how to properly use and protect the information in the system. In addition, all ICE personnel must take annual computer security and privacy training and sign the DHS rules of behavior before they are permitted access to the DHS network. The rules of behavior clearly explain what users can and cannot do within DHS systems and with the information they contain. Additionally, attorneys are deterred from making unauthorized disclosures of information because they are aware that making unauthorized disclosures could result in the loss of their license to practice law.

Privacy Risk: There is a risk of misuse by authorized users.

Mitigation: This risk is mitigated in several ways. Only individuals that have a need-to-know the information in the performance of their official duties have access to the system. Each user receives an account and the individual's user account controls what information he or she can access in the system. Additionally, users take annual security and privacy training and all users receive training on how to properly use the system. Finally, technical controls and robust auditing capabilities have been implemented to ensure appropriate use and access of the information.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Information in OCMS is typically collected from other systems or is relayed to OPLA by other offices in ICE that request OPLA's legal services. When appropriate, notice is provided to individuals at the time of collection by the underlying source systems. OPLA typically does not collect information maintained in OCMS directly from the individuals themselves, and therefore generally is not in a position to provide notice. There are some exceptions, however. In the case of the agency's ethics program, which falls under OPLA, individuals who complete the annual government employee financial disclosure forms are provided a written notice on those forms that complies with the notice requirements of the Privacy Act of 1974. Similarly, for individuals who file a federal tort claim against ICE, the claim form contains a Privacy Act notice that provides individuals notice and an opportunity to consent to the uses of their information by deciding to complete and submit the claim form to OPLA.

In immigration proceedings, OPLA may collect information from the alien during proceedings, either directly or through his or her counsel, or from witnesses or other entities that may have information relevant to the proceeding. There is no formal notice provided to these individuals at the time of collection of this information, although aliens who are arrested by ICE and given a notice to appear in immigration court are provided various forms of written notice about the immigration process, the information ICE collects about them, and how it may be used and disseminated.

Much of the information in OCMS is collected in order to help ICE manage its cases. There is a potential risk that the general public is not aware of the existence of OCMS, and the publication of this PIA, the DHS/ICE-003 GEMS SORN, and the other SORNs listed in question 1.2 mitigate this risk by describing the types of individuals whose information is contained in the system, the types of data it contains, and how the data is used.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Depending on the particular matter, individuals may not have the option to consent to particular uses of their information in OCMS. Because members of the public whose information is captured in OCMS may be involved in a law enforcement matter, or in litigation with the agency, such individuals are not afforded an opportunity to consent as to how their data is used within OCMS or to opt out. Additionally, since OCMS is a system used in litigation and for law enforcement purposes, allowing individuals to

consent to the agency's use of the data could seriously compromise underlying law enforcement matters or litigation for which the record was created.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals may not be aware of the existence of OCMS and the data it collects and maintains.

Mitigation: The risk is mitigated primarily by the public notice provided through this PIA, the DHS/ICE-003 GEMS SORN, and the other SORNs listed in question 1.2. One of the main purposes of OCMS is case management; therefore, it is not possible to provide notice to the individuals about whom ICE is working on cases because providing such notice could compromise the underlying litigation and law enforcement purposes of the system and may put other ICE work at risk.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

OCMS's predecessor system, GEMS, has an existing records schedule that is being updated to reflect the retirement of GEMS and the launch of OCMS. The retention period will remain the same, with records for cases and projects associated with immigration-related cases being retained for seventy-five (75) years after the last administrative action has been taken on the case. This retention period helps to ensure that information is available for historical purposes and for necessary case file research since some case files contain decades of information. This retention period is also necessary because cases may be active for decades or more (or be reactivated) as the subjects of the cases may have repeat encounters with immigration enforcement and/or cases pending before the immigration courts. For example, subjects of the cases may file motions to reopen cases that were previously adjudicated and closed in the years after the original case was decided. In these circumstances, the records in the original litigation case file are pertinent to the new matter as the same issues and questions may be able to be revisited if such a motion is granted. The records found in OCMS may also be unique and the information there may not be stored in other recordkeeping systems, including the A-File. Thus, these records would be necessary in future cases against the same subject. For example, a subject's case may have been closed for many years with a final order of removal, but it could be reopened by the EOIR after many years thus making the records in OCMS very relevant to the current proceedings.

As noted above, the other records in OCMS will be covered by the forthcoming Department of Homeland Security Legal Records retention schedule. This forthcoming retention schedule proposes retention periods for the other types of records in OCMS. Records for cases and projects associated with non-immigration-related cases will be kept for different periods of time depending on the type of case. Litigation case records that are non-immigration-related, such as tort cases, FOIA/Privacy Act cases,

contract cases, and employment cases, will be kept ten (10) years after a judgment is made or all appeals have been exhausted, whichever is later. Administrative case records that are non-immigration-related, such as Equal Employment Opportunity cases or some contract cases, will be kept for ten (10) years after a final order or decision has been made. Projects not associated with a litigation or administrative case will be kept for various periods of time depending on the content of the project. Projects involving informal legal opinions, advice, or analysis or those not pertaining to significant policy-making or major activities will be retained for three (3) years. Projects involving draft legislation or testimony regarding proposed legislation before Congress will be retained for fifteen (15) years. Projects involving claims or documents that may be relevant to potential liability of the government will be retained for three (3) years if no claim is filed. Projects involving regulatory actions, such as drafts of rulemaking documents, public comments received, and deliberative correspondence will be retained for twenty (20) years. Projects involving formal legal opinions pertaining to significant policy-making or major activities will be transferred to the National Archives and Records Administration (NARA) after twenty (20) years. Projects and documents related to legal advice provided regarding international law issues will be retained for fifteen (15) years. Reference materials will be destroyed when no longer needed. Projects related to congressional requests will be destroyed when no longer needed.

These retention periods ensure that the information is available for historical, auditing, and reporting purposes, and for necessary case research.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that information will be retained for longer than is needed to accomplish the purpose for which the information was originally collected.

Mitigation: ICE is proposing to retain the information in OCMS for the time frames outlined in question 5.1 in order to allow OPLA to properly carry out its work. The retention periods vary depending on the type of record. The immigration-related cases and projects are retained for seventy-five (75) years to ensure that the information is available for historical purposes, for necessary case file research, if a case is reopened after many years, or for use in future cases against the same subject. The draft Department of Homeland Security Legal Records retention schedule proposes the retention period for records related to non-immigration-related cases and projects and for projects that OPLA works on that are not related to any of its casework. Conforming with these retention periods helps ensure that the information is not retained for longer than is necessary.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

OCMS information is not routinely shared outside of DHS. There is routine sharing with DOJ for litigation purposes, for consultation on cases, or so DOJ can represent ICE on suits filed against the agency. Additionally, information in OCMS may be routinely shared with courts for the purposes of litigating issues that the agency is directly involved in such as immigration cases or litigation filed against or by the agency in any other courts. For the ethics program, ICE only shares information about individuals or cases when audited by the U.S. Office of Government Ethics (OGE). Reports sent to OGE consist only of aggregate data.

Any additional external sharing that occurs is in response to a formal request for the disclosure of such information. Any external sharing of information from OCMS is reviewed and approved by OPLA and/or the ICE Privacy Office prior to it being shared.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

As noted above, information from OCMS is not routinely shared outside of DHS except with DOJ. However, any information maintained in OCMS may be disclosed outside of DHS pursuant to 5 U.S.C. § 552a(b)(3).

6.3 Does the project place limitations on re-dissemination?

When information in OCMS is shared outside of ICE, generally the recipient agency may not further disseminate the information from OCMS unless it first obtains permission from ICE. Additionally, if the information is subject to any statutory protections, the recipient agency is made aware of those statutory protections.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

If disclosures of information outside of DHS are approved, users are instructed to account for the disclosure of the information. Accountings for disclosures are typically noted in the case or project record within OCMS and include what information was shared, to whom it was given, the recipient's contact information, and information about when it was given including the date and time. If the disclosure request was received in a letter or via e-mail, a copy of the letter or e-mail is stored in OCMS.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that data will be shared with external parties lacking a need to know, and that external sharing will not be properly recorded as required by the Privacy Act.

Mitigation: These risks are mitigated by the fact that information maintained in OCMS is shared in a manner consistent with the routine uses in the SORNs identified in question 1.2 and by any additional requirements required by law. Additionally, as noted above, if users disclose information outside of DHS, they are instructed to account for the disclosure. Typically, disclosures are accounted for in the relevant case or project record within OCMS.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

Individuals seeking notification of and access to any record contained in OCMS, or seeking to contest its content, may submit a request in writing to the ICE FOIA Officer:

U.S. Immigration and Customs Enforcement
Freedom of Information Act Office
500 12th Street SW, Stop 5009
Washington, D.C. 20536-5009
(202) 732-0660
http://www.ice.gov/foia/

All or some of the requested information may be exempt from access pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests. Providing an individual access to records contained in OCMS could inform the individual of an actual or potential criminal, civil, or regulatory violation investigation or reveal an investigative interest on the part of DHS or another agency. Access to the records could also permit the individual who is the subject of a record to impede an investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. In addition, access may be exempt in accordance with subsection (d)(5) of the Privacy Act (5 U.S.C. § 552a(d)(5)). Please see 6 C.F.R. part 5, subpart C, app. C for the exemptions related to the various DHS SORNs listed in question 1.2.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

The correction procedures are identical to those described in question 7.1 above. All or some of the requested information may be exempt from amendment pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests. Providing an individual access to records contained in OCMS could inform the subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal an investigative interest on the part of DHS or another agency. Access to the records could also permit the individual who is the subject of a record to impede an investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Please see 6 C.F.R. part 5, subpart C, app. C for the exemptions related to the various DHS SORNs listed in question 1.2.

7.3 How does the project notify individuals about the procedures for correcting their information?

The procedure for submitting a request to correct information is outlined in this PIA in questions 7.1 and 7.2.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals will be unable to meaningfully participate in the use of their data as maintained in this system or determine whether the system maintains records about them.

Mitigation: Because this system has a law enforcement purpose and contains information that is privileged, individuals' rights to be notified of the existence of data about them, to review the data to ensure it is correct, and to direct how that data may be used by ICE, may be limited depending on the nature of the case or matter that pertains to them. Notification to affected individuals could compromise the existence of ongoing law enforcement activities or cases and alert individuals to previously unknown investigations of criminal or otherwise illegal activity. This could cause individuals to alter their behavior in such a way that certain investigative tools will no longer be useful. Permitting individuals to direct the agency's use of their information could similarly interfere with the intended law enforcement use of the system.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

The auditing capability in OCMS captures all logon attempts, including those of ERO and HSI users, and any user activity information associated with viewing, creating, updating, or deleting records, including the specific user who performed the activity. The system's auditing provides information adequately detailed to facilitate reconstruction of events if compromise or misuse of the system occurs. The audit trail is protected from actions such as unauthorized access, modification, and destruction that would negate its forensic value.

The system's audit logs are reviewed by the system administrators and the system's Information System Security Officer (ISSO) on a weekly basis and whenever there is indication of system misuse. The ICE audit log management tool allows the ISSO to provide near real-time support in the analysis of the OCMS logs in order to identify unauthorized uses of the system. Logs are also examined randomly to ensure users and system administrators are accessing records and using the system in accordance with their job function and responsibilities.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All ICE personnel complete annual mandatory privacy and security training. Additionally, in the standard operating procedures for OCMS and in the mandatory training provided to system users prior to their accessing the system, individuals are instructed how to properly protect information in the system from inappropriate disclosure to third parties.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Each user account is assigned one or more user roles within the system depending on the user's job responsibilities. Assigning users to established user roles with certain capabilities helps to ensure that users are only able to access the information they need and helps to ensure system integrity. As noted above, select personnel in ERO and HSI have access to OCMS. These individuals are designated and approved by their supervisor as needing access. Prior to receiving access, the ERO and HSI personnel must complete the OCMS user training and submit a written request for system access to the authorized point of contact in their program office.

The OCMS user roles are described below:

OPLA attorneys and support staff: OPLA attorneys and support staff (those working at both ICE headquarters and at the Offices of Chief Counsel in the field) are granted access to create, view, and edit cases and projects in the system. Cases and projects that are immigration-related are accessible by all OPLA attorneys and support staff. Projects and cases that are non-immigration-related are only accessible by personnel assigned to the particular OPLA division working on that case or project. As mentioned above,

field level security has been set on some fields in cases and projects thus restricting which users can access or edit the fields depending on their division or user role. For example, only the National Security Law Section division members are allowed to edit and enter national security-related information in the immigration-related cases. OPLA attorneys and support staff are also able to run the OCMS standard and ad hoc reports.

External OPLA users (ICE users outside of OPLA): These users have read-only access to immigration-related case information. As noted above, for personnel in ERO and HSI to get access to OCMS, they must be designated and approved by their supervisor as needing access and they must complete the OCMS user training and submit a request for system access to the authorized point of contact in their program office.

System Administrators: System administrators create, edit, and delete user accounts; grant privileges to user accounts and user groups; activate and deactivate user accounts; reset passwords; customize menus and business rules in OCMS; customize and run reports in the system; monitor the system's audit trail to ensure that the system is being used properly; and perform other administrative functions. System administrators are typically OPLA employees.

ICE HelpDesk User: ICE HelpDesk users create user accounts, reset passwords, and assist OCMS users who contact the ICE Service Desk requesting assistance troubleshooting issues with the system.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

ICE does not have any information sharing agreements concerning the information in OCMS, nor does it envision the expansion of the systems' users or the intended uses of the information in such a way that any information sharing agreements would be required. In the event that such changes are considered, OPLA would engage with the ICE Privacy Office to discuss the intended expanded users and/or uses of this information to ensure that any privacy and legal risks are appropriately vetted. In addition, formal written agreements between ICE and other agencies to share data or provide access to OCMS would be reviewed by the ICE Privacy Office and OPLA as a matter of routine.

Responsible Officials

Amber Smith
Privacy Officer
U.S. Immigration and Customs Enforcement
U.S. Department of Homeland Security

Approval Signature

Original signed coy on file with the DHS Privacy Office

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security

APPENDIX

This appendix lists the federal government systems that are a source of information for projects and cases in OCMS and the type of information that each provides. This appendix will be updated as systems are added or removed as sources of information, as there are changes in the information that the systems provide, or when there are changes in the method by which information is shared with OCMS.

1) Enforcement Integrated Database (EID): DHS/ICE/PIA-015 - Enforcement Integrated Database (EID); DHS/ICE-011 - Immigration Enforcement Operational Records System (ENFORCE) SORN[7]

   OCMS ingests information about immigration-related cases from EID, an ICE system that is used to maintain arrest, booking, case initiation, detention, and removal data on aliens arrested by ICE for immigration violations and placed into proceedings in immigration court. The information ingested includes biographic information about the alien who is the subject of the case including name, A-Number, date of birth, and country of citizenship, as well as information regarding the investigation, arrest, booking, detention, and removal of the alien. It may also include limited biographic information including name, date of birth, and country of citizenship for individuals related to or associated with the alien. OCMS users can also select the alien on whom there is a case and ingest the information from EID into OCMS. OCMS obtains information from EID using a system-to-system connection, but OCMS users may also manually search EID and manually enter information from EID into OCMS. The information collected from this system is used to support immigration-related cases and projects.

2) TECS: DHS/CBP/PIA-009 – TECS System: CBP Primary and Secondary Processing; DHS/CBP-011 - U.S. Customs and Border Protection TECS SORN[8]

   CBP's TECS system is a source of information in OCMS including, but not limited to, arrival and departure records, Reports of Investigation (ROI) from ICE HSI, biographic information regarding aliens, previous encounters of aliens at the borders, and fingerprint history on aliens including any criminal history or hits on their fingerprints. Currently, OCMS users manually search this system and manually input any relevant data into OCMS, but eventually these systems may be directly connected to share data. The information collected from this system is used to support immigration-related cases and projects.

[7] The PIA for DHS/ICE/PIA-015 Enforcement Integrated Database (EID) and the subsequent PIA updates are located at http://www.dhs.gov/privacy-documents-ice. The DHS/ICE-011 - Immigration Enforcement Operational Records System (ENFORCE) SORN was last published on May 3, 2010 (75 FR 23274).
[8] The PIA for DHS/CBP/PIA-009 – TECS System: CBP Primary and Secondary Processing and the subsequent PIA updates are located at http://www.dhs.gov/privacy-documents-us-customs-and-border-protection. The DHS/CBP-011 - U.S. Customs and Border Protection TECS SORN was last published on December 19, 2008 (73 FR 77778).

3) Refugee, Asylum, and Parole System (RAPS): DHS/USCIS/PIA-027 - Refugees, Asylum, and Parole System (RAPS) and the Asylum Pre-Screening System (APSS); DHS/USCIS-010 - Asylum Information and Pre-Screening SORN[9]

   USCIS's RAPS provides OCMS with information obtained from an asylum applicant during the applicant's interview with U.S. Citizenship and Immigration Services (USCIS) and from the applicant's asylum application. The information includes biographic information about the applicant, information provided during the interview and on the asylum application, the status of the application, the reason the asylum application was denied, and information related to the referral of the applicant's asylum application to the immigration court. ICE periodically receives data from RAPS on cases that are being referred to the immigration court for litigation. Data received from RAPS is e-mailed in an encrypted text file from USCIS to OCMS. An automated process converts the contents of the text file into raw data that is uploaded into OCMS. The information collected from this system is used to support immigration-related cases and projects.

4) National File Tracking System (NFTS): DHS/USCIS/PIA-032 - National File Tracking System (NFTS); DHS/USCIS-001 - Alien File, Index, and National File Tracking System of Records SORN[10]

   USCIS's NFTS tracks the location of paper A-Files at DHS. Currently, OCMS users manually search NFTS to determine the location of A-Files and enter the location information in OCMS, but eventually these systems may be directly connected to share data. The information collected from this system is used to support immigration-related cases and projects.

5) Benefits Processing of Applicants Other Than Petitions for Naturalization, Refugee Status, and Asylum (CLAIMS 3): DHS/USCIS/PIA-016 - USCIS Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum (CLAIMS 3); DHS-USCIS-007 - Benefits Information System SORN[11]

   USCIS's CLAIMS 3 is the source of information provided by an alien on his or her application for an immigration benefit. The information varies depending on the benefit but generally includes the alien's name, date of birth, country of citizenship, and the alien's length of residence in the U.S. Additionally, CLAIMS 3 indicates which steps of the benefits adjudication process have been completed, including setting up of an appointment for the alien to submit biometrics for a background check, checking to see what other pending benefits the alien has, and investigating whether the applicant is suspected of fraudulent activity. Currently, OCMS users manually search CLAIMS 3 and manually input any relevant data into OCMS, but eventually these systems may be

[9] The PIA for DHS/USCIS/PIA-027 Refugees, Asylum, and Parole System (RAPS) and the Asylum Pre-Screening System (APSS) and the subsequent PIA updates are located at http://www.dhs.gov/uscis-pias-and-sorns. The DHS/USCIS-010 - Asylum Information and Pre-Screening SORN was last published on January 5, 2010 (75 FR 409).

[10] The PIA for DHS/USCIS/PIA-032 National File Tracking System (NFTS) is located at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscis_nfts.pdfPIA. The DHS/USCIS-001 - Alien File, Index, and National File Tracking System of Records SORN was last published on June 13, 2011 (76 FR 34233).

[11] The PIA for DHS/USCIS/PIA-016 - USCIS Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum (CLAIMS 3) is located at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cis_claims3.pdf. The DHS-USCIS-007 - Benefits Information System SORN was last published on September 29, 2008 (73 FR 56596).

directly connected to share data. The information collected from this system is used to support immigration-related cases and projects.

6) Computer Linked Application Management System (CLAIMS 4): DHS/USCIS/PIA-015 - Computer Linked Application Information Management System (CLAIMS 4); DHS-USCIS-007 - Benefits Information System SORN[12]

   USCIS's CLAIMS 4 provides information from the Form N-400, *Application for Naturalization,* as well as information generated by DHS or the FBI that may come up during a background check such as arrest and conviction information during the naturalization process. Additionally, CLAIMS 4 contains information obtained from applicants during interviews, basic information regarding the FBI's background check of the person's name (i.e., "Pending" because the search is ongoing, "No Record," or a "Positive Response"), or fingerprint check results and the date of the response. Currently, CLAIMS 4 is manually searched by OCMS users, but may eventually provide information to OCMS via a system-to-system connection. The information collected from this system is used to support immigration-related cases and projects.

7) Central Index System: DHS/USCIS/PIA-009 - Central Index System (CIS); DHS/USCIS-001 - Alien File, Index, and National File Tracking System of Records SORN[13]

   USCIS's Central Index System provides immigration case-related information on applicants seeking immigration benefits including lawful permanent residents, naturalized citizens, U.S. border crossers, aliens who illegally entered the U.S., aliens who have been issued employment authorization documents, individuals who petitioned for benefits on behalf of family members, and other individuals subject to the provisions of the Immigration and Nationality Act (INA). The information provided by CIS includes, but is not limited to, biographic information about the alien and historical information including the alien's past entries into and exits out of the U.S. and past applications that the individual filed. CIS also serves as a DHS-wide index of other DHS systems including CLAIMS 3 and CLAIMS 4 that maintain immigrant and non-immigrant status information on aliens. All of the information provided by these systems can be accessed through the CIS portal. Information on other individuals subject to the provisions of the INA and tracking information regarding the location of paper A-Files in local file control offices is also available through this system. Currently, OCMS users manually search this system and manually input any relevant data into OCMS, but eventually these systems may be directly connected to share data. The information collected from this system is used to support immigration-related cases and projects.

---

[12] The PIA for DHS/USCIS/PIA-015 - Computer Linked Application Information Management System (CLAIMS 4) and the subsequent PIA updates are located at http://www.dhs.gov/uscis-pias-and-sorns. The DHS-USCIS-007 - Benefits Information System SORN was last published on September 29, 2008 (73 FR 56596).

[13] The PIA for DHS/USCIS/PIA-009 - Central Index System (CIS) is located at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscis_cis.pdf. The DHS/USCIS-001 - Alien File, Index, and National File Tracking System of Records SORN was last published on June 13, 2011 (76 FR 34233).

8) Integrated Digitization Document Management Program (IDDMP) and Electronic Document Management System (EDMS): DHS/USCIS/PIA-003 - Integrated Digitization Document Management Program; DHS/USCIS-001 - Alien File, Index, and National File Tracking System of Records SORN[14]

   USCIS's EDMS is the repository for digitized A-Files. The A-File includes biographic information; applications and petitions for benefits; vital documents (e.g., birth certificates, passports, marriage certificates); biometric information (e.g., photographs and fingerprints); enforcement supporting documents such as the person's rap sheet; and other documents such as naturalization certificates, tax returns, labor certifications, correspondence, court dispositions, and interview notes. Currently, OCMS users manually search this system and manually input any relevant data into OCMS, but eventually these systems may be directly connected to share data. The information collected from this system is used to support immigration-related cases and projects.

9) Case Access System for EOIR (CASE) and Immigration Review Information Exchange System (IRIES): Case Access System for EOIR (CASE) PIA; JUSTICE/EOIR - 001 Records and Management Information System SORN[15]

   CASE is the Department of Justice, Executive Office of Immigration Review's (EOIR) case and court scheduling system. IRIES is used as a mechanism to retrieve information from CASE and to share the information from CASE with other systems including OCMS. IRIES retrieves information from CASE about immigration cases pending before the immigration courts and OCMS ingests this information from IRIES. The information includes biographic information about aliens including name, address, telephone number, date of birth, age, nationality, language, known aliases, and last known address; other individuals involved in cases including attorneys (including federal government attorneys and defense attorneys), aliens, judges, witnesses, legal representatives, and other individuals that provide representation and assist respondents in removal proceedings; contact information for these other individuals including title, place of employment, address, phone number, fax number, and email address; and case history information including actions taken in a case and the disposition of a case as issued by the immigration judge or the Board of Immigration Appeals (BIA). OCMS has a system-to-system connection with IRIES and receives data from IRIES in two ways. First, using a date range search, OCMS obtains immigration court hearing information for all cases occurring within the provided date range. OCMS can also retrieve hearing information for a particular hearing by querying a given A-Number. The information collected from this system is used to support immigration-related cases and projects.

10) Consular Consolidated Database (CCD): Consular Consolidated Database PIA; STATE-39 - Visa Records SORN[16]

---

[14] The PIA for DHS/USCIS/PIA-003 - Integrated Digitization Document Management Program is located at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscis_iddmp.pdf. The DHS/USCIS-001 - Alien File, Index, and National File Tracking System of Records SORN was last published on June 13, 2011 (76 FR 34233).

[15] The PIA for the Case Access System for EOIR (CASE) is located at http://www.justice.gov/opcl/eoir_pia.pdf. The JUSTICE/EOIR- 001 - Records and Management Information System SORN was last published on May 11, 2004 (69 FR 26179).

[16] The PIA for the State Department's Consular Consolidated Database (CCD) is located at

CCD is a Department of State system that provides information about foreign nationals who have applied for a visa including immigrant visa applicants and non-immigrant visa applicants. The information includes, but is not limited to, biographic information including name, address, date of birth, and country of origin; biometric data (fingerprints and facial images); and identification numbers (e.g., Social Security Numbers and A-Numbers). Currently, OCMS users manually search this system and manually input any relevant data into OCMS, but eventually these systems may be directly connected to share data. The information collected from this system is used to support immigration-related cases and projects.

11) ICE eService:

ICE eService is a system which allows the Office of the Principal Legal Adviser (OPLA) to securely send and receive documents that contain Sensitive Personally Identifiable Information (SPII), related to matters before the Department of Justice's (DOJ) Executive Office for Immigration Review (EOIR), including the Board of Immigration Appeals. ICE eService uses a third party cloud subscription service and serves as a trusted internet connection (TIC) between the OPLA Case Management System (OCMS) and external parties (e.g., trial attorneys, private immigration counsel, certified alien representatives, and unrepresented aliens) and supports the immediate service of documents upon and by the 26 ICE Offices of Chief Counsels (OCCs). The use of ICE eService by external parties is voluntary and is a substitute for service through regular mail. External users access ICE eService through an external facing website and use two factor authentication in order to access their own ICE eService workspace. Documents that may be submitted via the ICE eService portal include motions, briefs, applications, notices of appearance, notice of appeals, and any associated documentation. Once the documents are uploaded, they are transmitted to the ICE eService module. OCCs review the submissions and ensure that the documents received are complete and conform to relevant requirements and regulations. If the OCC accepts the submission by performing a manual review of the received documents, ICE eService will transmit documents electronically to the relevant case file in OCMS. The information collected from this system is used to support immigration-related cases and projects.

---

http://www.state.gov/documents/organization/93772.pdf. The STATE-39 SORN was last published on October 25, 2012 (77 FR 65245).