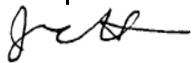


<b>EXECUTIVE OFFICE FOR IMMIGRATION REVIEW PRIVACY IMPACT ASSESSMENT</b>	
System Name	Case Access System for EOIR (CASE)
Component System Sponsor	EOIR/OCIO
Point of Contact Name	Jeffrey Secor
Job Title	
Address	5107 Leesburg Pike, Suite 2300, Falls Church, VA 22041
Phone Number	703-605-1328
Fax Number	703-305-0911
Email Address	<a href="mailto:jeff.secor@usdoj.gov">jeff.secor@usdoj.gov</a>
PIA Required	Yes
Component Approving Authority	Brian McGrath, Chief Information Officer
Date Received/Date Approved	
DOJ Administrative Review Intake	
Date Received/Date Approved	
Technical Review Officer	Brian McGrath, Chief Information Officer
Date Received/Date Approved	
Legal Review Officer	Gus Villageliu, Senior Associate General Counsel
Date Received/Date Approved	
DOJ Privacy Officer	Jane Horvath, Chief Privacy and Civil Liberties Officer 
Date Received/Date Approved	9/14/06 / 9/26/06
Publication	
Type/Method/Citation/Date	

## **Executive Office for Immigration Review**

The Executive Office for Immigration Review (EOIR) is responsible for adjudicating immigration cases. Under delegated authority from the Attorney General, EOIR interprets and administers federal immigration laws by conducting immigration court proceedings, appellate reviews, and administrative hearings.

EOIR consists of three components: the Office of the Chief Immigration Judge, which is responsible for managing the numerous immigration courts located throughout the United States where immigration judges adjudicate individual cases; the Board of Immigration Appeals (BIA), which primarily conducts appellate reviews of immigration judge decisions; and the Office of the Chief Administrative Hearing Officer, which adjudicates immigration-related employment cases. Detailed information about EOIR is electronically available at <http://www.usdoj.gov/eoir>. Section 208 of the E-Government Act of 2002 (44 U.S.C. 3501 note) requires EOIR to conduct the following privacy impact assessment of this information collection:

### **Privacy Impact Assessment for Case Access System for EOIR (CASE)**

#### **Introduction**

EOIR is updating and integrating its Immigration Court and BIA databases as a first step toward designing an electronic case access and filing system which will comply with the Government Paperwork Elimination Act (GPEA), achieve the Department of Justice's (DOJ) vision for improved immigration adjudication processing, and meet the public expectations for electronic government. The GPEA provides that the Office of Management and Budget (OMB) must ensure that executive agencies provide for the option of electronic submission of information, when practicable, as a substitute for paper. The new system, Case Access System for EOIR (CASE), will replace the Automated Nationwide System for Immigration Review (ANSIR) and will add data elements, allowing EOIR to provide more information about its processes to Congress and the public.

#### **General Description of System**

CASE will integrate the stove-piped legacy databases for the Immigration Courts and the Board of Immigration Appeals. This is the foundation of the larger eWorld project and database integration is nearing completion. User Acceptance Testing has been conducted and pilots are occurring during fiscal years 2005 and 2006. All staff will have immediate access to information about all phases of a case. The new CASE system will replace ANSIR, as noted above.

CASE will contain a docket listing the documents filed in each case; this docket will ultimately serve as the index to electronic documents in eWorld, but in earlier phases it may also reduce redundant data entry by Department of Homeland Security (DHS) staff into its new electronic case management (GEMS) system. Attorneys and other EOIR practitioners will eventually register, be assigned unique user IDs, and choose passwords via a web-based practitioner registration application linked to CASE. The CASE database will include only one record per attorney, regardless of the number of courts in which he or she practices or the

number of cases in which he or she is involved, reducing redundancy in notices and communications, and depending primarily on less costly electronic notifications rather than mailed notifications.

### **What Information Is Collected**

The information collected in CASE will be virtually the same as that currently collected in ANSIR. It will be biographic and demographic data of individuals in immigration proceedings before EOIR's courts or the BIA. There are a variety of sources of the information in the database, including the following.

- Department of Homeland Security (DHS) charging document
- Applications submitted by the alien, or a representative appearing on the alien's behalf
- Documents submitted by the alien or his representative
- Documents submitted by DHS
- Testimony provided by the alien or his representative when appearing in Court

### **Why Information Is Collected**

EOIR collects information in CASE to track an alien's immigration court and appeal proceedings.

### **Intended Use of Information**

The information collected may be used to determine eligibility for relief from removal or for some other government benefit. It also may be used to alert an individual of the status of a case before EOIR. It also may be used by DHS to coordinate the trial attorneys' calendars.

### **With Whom Information Will Be Shared**

The information collected in CASE may be shared with DHS staff (attorneys involved in the immigration proceeding, enforcement officers, or benefits officers) as well as with staff from the Office of Refugee Resettlement, in the case of individuals granted asylum. CASE information may also be shared with attorneys or respondents in individual cases.

### **Individuals' Opportunities to Decline or Consent**

Individuals in immigration proceedings do not have the opportunity to decline to provide information. If they do so, it may have an adverse effect on the outcome of their cases. An individual must grant consent for an attorney or other qualified individual to represent him, in which case that representative will have access to information about that individual. The basic case information that will be available is the same as that which can currently be accessed via a 1-800 number.

### **How Information Will Be Secured**

As of a result of the Department's plan to include the Justice Consolidated Office Network (JCON-II) as a Departmental asset, security is provided and funded through both the EOIR and the DOJ general support system/network. Any system-related security practice or application includes all of EOIR planned or operational systems. The JCON-IIA office automation system is based upon the DOJ enterprise architecture and standards, which comply with the Government Information Security Act, OMB policy, and NIST guidance. The new CASE system, for which EOIR has been adhering to all security procedures, is the first step in the eWorld transition from its two legacy stove-piped systems to a consolidated system to eventually implement electronic filing and provide public access. Therefore, current security certifications have been granted under the umbrella of JCON-IIA/CASE.

EOIR established the Information Resource Management (IRM) System Security and Integrity Staff in January 2000 to ensure that EOIR's information technology system security program meets the high standards for security protection mandated by the Department and the specific nature of EOIR cases. Therefore, the System Security and Integrity staff have been monitoring the development of CASE to ensure that the JCON security requirements are included.

The EOIR security staff has specific training and expertise in preventing, identifying, and resolving potential security breaches. The EOIR staff's training and expertise include: establishing, implementing, and maintaining system security policy, standards, and procedures; ensuring compliance with computer security awareness training; creating user accounts; auditing user accounts and system activities; conducting risk assessments; establishing security and contingency plans; conducting annual IT assessments; monitoring DOJCERT - Alerts, firewalls, and VPNs (CheckPoint); planning and testing disaster recovery and intrusion detection systems; providing training and access to Justice Secure Remote Access (JSRA) users; gathering information on public key infrastructure (encryption); ensuring telecommunications security; creating a security architecture; providing password management; disseminating virus protection; and conducting penetration testing.

Finally, the Inter-Agency Agreement (IAA) that governs data exchange with DHS stipulates how recipients can use data that is housed in CASE. IAAs will be updated as necessary to ensure the safeguarding and appropriate use of data.

### **System of Records Under Privacy Act**

No new system of records is presently being created in conjunction with the implementation of the Case Access System for EOIR because the use, collection and dissemination of this information is already included as a routine use in the System of Records for EOIR last published in the Federal Register in 2004 at 69 FR 26179-01, 2004 WL 1047096. Therefore, these initiatives comport with applicable Privacy Act standards and Section 208 of the E-Government Act of 2002. Also, system security practices for government users have been developed and restricted in accordance with the Government Information Security Reform Act, OMB Policy, and NIST Guidance.

### **Analysis**

The implementation of CASE does not involve additional privacy issues than those that prevailed under the legacy system. However, EOIR recognizes that CASE is simply the first step in the larger eWorld project. As such, a Privacy and Access working group was formed to define what information, both data and documents, will be available in eWorld, to whom, and under what circumstances. This work group consisted of representatives from each of EOIR's components, members of the Office of the General Counsel, and experts from the IRM System Security and Integrity Staff, and were guided by e-filing consultants with expertise in privacy and access issues in courts using electronic filing.

In preparation for the eWorld project the working group developed a set of five matrices for specific case types. Within each matrix the Privacy and Access working group compared each interested party against each data type. In doing this they considered and applied relevant policies to each comparison and made a determination of the appropriate access levels. These completed matrices are, and will continue to be, used as a reference for the planning, application development, and implementation of the eWorld project. In addition, the matrices form the basis of the Privacy Impact Assessment. Because of their size these matrices have not been attached to this document; however, they are available for review upon request.

Other responsibilities of the Privacy and Access working group included: (1) The monitoring of the development of guidance by the President or the Director of OMB interpreting the E-Government Act of 2002. (2) The definition of what information should be available to the public at large (including the press) over the Internet (i.e., whether the information currently available through the 800 number should be made available through the Internet and whether additional information in CASE and electronic documents should be added). (3) Review of current EOIR statutes, regulations, and operating policies and procedures memoranda (OPPM). Review of current EOIR regulations and OPPMs to determine whether additional procedures were needed for case by case determinations to grant or deny public and press access to specific documents and data that would otherwise be public or restricted from public access. (4) The drafting of a proposed policy and materials to implement a policy on notifying litigants and the public of the public or private nature of documents filed in EOIR cases. (5) Preparation for a privacy impact assessment for the eWorld project based on the requirements of Section 208 (b)(2)(B) of Title II of the E-Government Act of 2002.

Again, this Privacy Impact Assessment only concerns the implementation of CASE and sharing CASE data with DHS. EOIR intends to complete further Privacy Impact Assessments for future phases of eWorld, when deemed appropriate by the Chief Information Officer of EOIR and DOJ.