Privacy Impact Assessment

for the

Immigration and Customs Enforcement (ICE) General Counsel Electronic Management System (GEMS)

April 25, 2006

Contact Point

William C. Birkett
Chief, Knowledge Management Division
Office of the Principal Legal Advisor
Immigration and Customs Enforcement
Washington, D.C. 20536

Reviewing Official

Maureen Cooney
Acting Chief Privacy Officer
Department of Homeland Security
(571) 227-3813

Introduction

The Office of the Principal Legal Advisor (OPLA) within the Bureau of Immigration and Customs Enforcement (ICE) provides the full range of legal support, including core responsibilities for representing ICE before the Immigration Courts and the Board of Immigration Appeals. Legislation enacted by Congress over the past 15 years has significantly expanded ICE enforcement activities, resulting in increased arrests, criminal alien removal programs, Institutional Removal Programs, anti-smuggling efforts, conveyance seizures, expedited removal proceedings, and mandatory detention and removal of illegal/criminal aliens. These expanded activities have increased the need for OPLA legal services and, concomitantly, increased the need for an electronic management system to support the information needs of OPLA attorneys and other Department of Homeland Security (DHS) or Department of Justice (DOJ) attorneys or Department of State (DOS) who have a need for access to ICE records for the performance of their law enforcement duties.

The General Counsel Electronic Management System (GEMS) has been designed as a tightly integrated, automated knowledge management tool for use by staff in OPLA and other federal litigation components as needed. The primary goals of the proposed GEMS project were as follows:

- Reduce and eventually eliminate OPLA reliance on the paper alien file (A-File)
- Make key information about a case or project available online in a single user interface
- Make information about a case or project simultaneously available to all persons who have a need to know such information
- Institute OPLA-wide standards for certain automated capabilities
- Provide ICE management with summary and/or detailed information concerning office, case, or project status
- Provide knowledge management capabilities across the entire OPLA repository of information
- Provide US Attorneys and Office of Immigration Litigation Attorneys access to case information as needed for the prosecution of their civil/criminal alien matters and defense of alien federal appeals.

To comply with these pressing business requirements and Congressional mandates, ICE has created GEMS. In order to assess the privacy issues associated with the collection, maintenance and use of personally identifiable information that will be maintained in GEMS, which includes necessary sharing with other agencies, the DHS Chief Privacy Officer directed that a Privacy Impact Assessment (PIA) be performed in accordance with the guidance issued by Office of Management and Budget (OMB) on September 26, 2003, and that the PIA be periodically updated as necessary to reflect future changes.

Section 1 Scope of the Information Collected

1.1 What is GEMS?

GEMS is a web enabled knowledge management system built from customized off-the-shelf software. GEMS provides federal attorneys and attorney managers with real-time information on cases being litigated in immigration court and the federal courts. GEMS is comprised of three principal integrated component subsystems with specific purposes: Case/Project Management, Object Management,

and Knowledge Management. OPLA staff use these GEMS components to manage their immigration caseload.

1.2 What information is being collected

GEMS consists of all materials relating to the litigation of a particular case concerning an alien that is pending before an immigration court or a federal court. The records that are collected and maintained in GEMS therefore consist of the following: pre-trial notes, trial notes, post-trial notes, memoranda stating positions for litigation in draft or final form, notes to investigators, information from hardcopy and online research and other attorney work product;

A-File number, date, and place of birth, date and port of entry, as well as the location of each official hardcopy paper file known as the "A- file;" and subsets or complete sets of information, based on the litigation needs of the ICE attorney, that is also contained in the hard copy A-file, which may include the alien's official record material, such as naturalization certificates; various forms (and attachments such as photographs), applications and petitions for benefits under the immigration and nationality laws, reports of investigations; statements; arrest reports; correspondence; and memoranda on each individual for whom ICE has created a record under the Immigration and Nationality Act.

1.3 Why the information is being collected

GEMS is for the benefit of ICE attorneys and attorney management to be used for the tracking, processing, and reporting on the preparation and presentation of cases for a federal court or immigration court before which the ICE or the DHS is authorized to appear. As a result, the system will enable ICE to carry out its assigned national security, law enforcement, immigration control, and other mission related functions and to provide associated management reporting, planning and analysis in a uniform and efficient manner.

1.4 What is the intended use of the information

The system will be used primarily by ICE OPLA and other federal attorneys for the tracking, processing, and reporting on the preparation and presentation of cases for a court or adjudicative body before which the ICE, or DHS, or the Department of Justice (DOJ) is authorized to appear.

1.5 Can aliens whose information is contained within GEMS decline to provide that information, or consent to only particular uses of that information

No. The information pertaining to a particular alien that is contained within GEMS is derived from either the arrest processing of the alien, from court proceedings, or from attorney work product.

Section 2.0 Information Security, Sharing and Access

GEMS data will be shared with other DHS employees on a "need to know" basis to enable those employees to carry out their official duties, and with student volunteers whose services are accepted pursuant to 5 U.S.C. Section 3111 or students enrolled in a college work-study program pursuant to 42 U.S.C. Section 2751 et seq. GEMS information will also be shared with contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency

function related GEMS. GEMS information may be shared with a former employee of the DHS for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable DHS regulations. In addition, GEMS information may be disclosed for the purpose of facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where DHS requires the information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

GEMS information may be shared with other law enforcement agencies, both within and outside the United States, during the course of law enforcement investigations, where disclosure is necessary to elicit information required by ICE to carry out its official functions or statutory mandates. In addition, GEMS information may be shared with federal, state, tribal, local or foreign government agencies or organization, or international organizations, that are lawfully engaged in collecting law enforcement intelligence information, whether civil or criminal, or charged with investigating, prosecuting, enforcing or implementing civil or criminal laws, to enable these entities to carry out their law enforcement responsibilities, including the collection of law enforcement intelligence. GEMS information may also be shared with other federal agencies for the purpose of conducting national intelligence and security investigations. Where a GEMS record indicates, either on its face or in conjunction with other information, a violation or potential violation of criminal or civil law, the relevant records may be referred to the appropriate Federal, state, territorial, tribal, local, international, or foreign agency law enforcement authority or other appropriate agency charged with investigating or prosecuting such a violation or enforcing or implementing such law.

GEMS information may also be shared with DOJ, DOS or other federal agencies engaged in litigation when any of the following are parties to the litigation: DHS or DOS; any employee of DHS or DHS who is being sued in his or her official capacity; any employee of DHS or DHS who is being sued in his or her individual capacity where DOJ, or DHS has agreed to represent the employee; or the United States or any agency thereof.

GEMS information may also be shared with the Office of Management and Budget (OMB) in connection with the review of private relief legislation as set forth in OMB Circular No. A-19 at any stage of the legislative coordination and clearance process as set forth in the Circular. It may also be shared with and the National Archives and Records Administration (NARA) in records management inspections conducted under the authority of 44 U.S.C. Sections 2904 and 2906.

2.1 Who will have access to the data

The following government agencies have direct access to GEMS data for law enforcement purposes:

- Certain components of DHS - ICE, U.S. Citizenship and Immigration Services (USCIS), and Customs and Border Protection (CBP)
- Department of State (DOS) - Office of Exchange Coordination and Designation, Office of Consular Affairs
- Department of Justice (DOJ) –Federal Bureau of Investigation (FBI)

No non-governmental entities will have access to GEMS data except through normal Freedom of Information Act processes.

2.2 How will data quality be maintained

Information is checked for accuracy at multiple stages throughout the life cycle of the data. Error traps are in place for checking the accuracy of data as it is entered into the system. Comparative checking of related data to other systems will take place at the time records are created.

Documents that have been filed before a tribunal will be "locked" from editing.

Specific data that has been identified as erroneous can be corrected by a process of notification to the database administrator on a form called "GEMS Data Correction," which must be signed by the principal supervisor in the office where the request originates.

2.3 How will System/data security be maintained

DHS appreciates the sensitivity of the personal data supplied by individuals, regardless of their nonimmigrant status, and applies safeguards to this information to protect it from unauthorized access. The GEMS system is considered "sensitive but unclassified" because it stores and processes information about individuals.

Physical Security: GEMS is physically housed in a Government-secured facility and at a contingency site. Web and application servers for the DHS Web Services reside in the Justice Online Information Network at JDC-W. Access to the Web Services infrastructure is from the public Internet through equipment maintained by DHS, and from the ICE Intranet, through servers, routers, switches, and firewalls, some maintained by DOJ and some maintained by DHS network staff.

Data Security: GEMS operates under one environment—the ICE Web Farm Services must be accessed for all connectivity. Users access GEMS via the DHS Intranet or via SecurID token access to the DHS Intranet.

GEMS has been granted an Interim Authority to Operate under the Federal Information Security Management Act (FISMA). Under FISMA all systems are required to undergo system security certification and accreditation (C&A); GEMS currently has been granted an Interim Authority to Operate until December 2005, based on the last approved C&A in June 2005. GEMS is currently in the process of pursuing a full C&A based on GEMS Web Version Release 1.1, which was released in July 2005. The full C&A provides that GEMS is meeting those DHS current system security requirements that are within the scope of GEMS. Additionally, the system undergoes constant review by the Computer and Telecommunications Security group within DHS. This group participates in regularly scheduled release meetings in order to stay abreast of upcoming changes related to system security. Any time a change involving system security is made to the system, the effects are noted in relevant security documents. This process includes a risk assessment, as well as a security test and evaluation process. The findings of each are provided in a security report document.

Secure Identification/Password Access and Monitoring: Password Issuance Control System (PICS) provides GEMS user identifications (IDs) for all approved users. Once approved, users are prompted to create their own unique password in order to obtain access. User IDs & passwords are recorded and monitored by PICS. A GEMS user has to go through an authentication process using his or her specific ID and password, before accessing data in the system. ID and password inactivity for a period of 30 days or more will automatically lock a user out of the system and require a reset of the password by PICS, before access can be regained. Additionally, three unsuccessful attempts to access the system with an incorrect combination of ID and password will also lock a user out of the System.

GEMS records and maintains information on session activity (user ID, log on time, duration of session, log off time, etc.) each time a user accesses the system. Additionally, GEMS maintains a record of all changes that a user makes to the data in the system. These features provide an audit trail of all user actions, which can be utilized to monitor and analyze user activity for compliance. GEMS is monitored by the Knowledge Management Division of the Office of Principal Legal Advisor for case activity on a weekly basis. This would enable the agency to identify improper access to information contained in the system. These features also provide a measure of quality assurance for data integrity. The Knowledge Management Division of the Office of the Principal Legal Advisor audits GEMS access to assure that user's access to the system is according to their system "roles." System "roles" determine what level of system access users have, what data they can see, and what data they can change.

Risk Mitigation: DHS recognizes the privacy risks associated the collection of data about individuals. However, GEMS was specifically designed to access in an electronic environment only information that attorneys in the federal government are already allowed to access. The security measures and processes put in place to access GEMS assure that only authorized users will access the system. GEMS users will be trained on the requirements of the Privacy Act to minimize any privacy risks associated with this system of records.

Section 3.0 Information Retention and Destruction

In accordance with the provisions of 44 U.S.C. § 3303a, GEMS records will be retained and disposed of according to a disposition schedule approved by the Archivist of the United States.

Outputs (data sets pulled from the database for specific uses) will be destroyed when no longer needed for agency business.

For historical purposes, and because specific immigration law enforcement or benefit case file research can span decades, DHS/ICE will maintain GEMS data files in accordance with the 75-year retention period that is currently followed for the physical A-File until DHS/ICE in working with NARA establishes a more appropriate retention schedule for digital information.

Section 4.0 Redress

Because information in GEMS is attorney work product containing agency attorney's analysis of specific cases in contemplation of litigation, there is no mechanism for redress by individuals whose information appears in the system. Access to information contained in GEMS is through normal Freedom of Information Act application.

Section 5.0 Applicable System of Records Notice (GEMS)

Because GEMS maintains and uses information about aliens that is specific to the business practices of attorneys litigating cases about those aliens, GEMS has created its own system of records. This decision reflects the DHS policy to apply robust privacy protections to all individuals and is consistent with guidance issued by OMB encouraging agencies that maintain record systems containing commingled information about citizens and aliens "to treat such systems as if they were, in their entirety, subject to the Act." OMB, Privacy Act Implementation: Guidance and Responsibilities, 40 Fed. Reg. 28948, 28951 (July 9, 1975). A Privacy Act notice for this system is being published contemporaneously with this PIA.

Summary and Conclusions

GEMS collects litigation-specific information on aliens who are in removal proceedings before immigration courts or federal courts. In operating this system, GEMS program managers are mindful of the privacy concerns surrounding the information that is collected and have taken steps to ensure that any privacy risks are mitigated to the extent possible by including training for all personnel, appropriate access and security controls, and auditing capability.

Contact Information

- By mail: Immigration & Customs Enforcement, OPLA Knowledge Management Division, 425 I Street, NW, Room 6100, Washington, D.C. 20536
- By email: GEMS@DHS.gov
- By phone: 202-514-2895
- By fax: 202-514-5491

Appendix A: List of References

1.1 Statutory Authorities for Protection of Information and of Information Systems

5 U.S.C. § 552, Freedom of Information Act (FOIA) of 1966, As Amended

5 U.S.C. § 552a, Privacy Act of 1974, As Amended

Public Law 100-503, Computer Matching and Privacy Act of 1988

Public Law 107-347, E-Government Act of 2002, Section 208, Privacy Provisions, and Title III, Information Security (Federal Information Systems Management Act (FISMA))

1.2 Statutory Authorities for GEMS

Immigration And Nationality Act of 1952, as amended.

1.3 Other Supporting Documentation and Guidance

DHS/ICE Baseline Security Requirements for Automated Information Systems, July 18, 2003.

ICE Security Requirements, printed October 30, 2003.

IT Security Program Handbook, Version 1.3, Sensitive Systems, Department of Homeland Security, ID-4300A, June 20, 2003.

Federal Trade Commission, Privacy Online: A Report to Congress, June, 1998.

OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, Memorandum M-03-22, September 26, 2003.

Risk Management Guide for Information Technology Systems, NIST Special Publication 800-30, January 2002.

Appendix B: List of Acronyms

CBP	Customs and Border Protection
DHS	Department of Homeland Security
DOJ	Department of Justice
DOS	Department of State
FBI	Federal Bureau of Investigation
GEMS	General Counsel Electronic Management System
HQ	Headquarters
ICE	Immigration and Customs Enforcement
INA	Immigration and Nationality Act
JDC-W	Justice Data Center Washington
OMB	Office of Management and Budget
PA	Privacy Act
PICS	Password Issuance Control System
PIA	Privacy Impact Assessment
SBU	Sensitive But Unclassified
SEVP	Student and Exchange Visitor Program
SORN	System of Records Notice
USCIS	Citizenship and Immigration Services
U.S.	United States

Responsible Official

William C. Birkett
Chief, Knowledge Management Division
Office of the Principal Legal Advisor
Immigration and Customs Enforcement
Washington, D.C. 20536

Approval Signature Page

_____

Maureen Cooney
Acting Chief Privacy Officer
Department of Homeland Security