Privacy Impact Assessment

for the

Case Management Applications

Certifications:

I certify that this Privacy Impact Assessment conforms to the principles of OMB Memorandum M-03-22, and that the assessed system is in compliance with Section 208 of the E-Government Act of 2002 (Pub. L. 107-347).

/signed/ 5/31/2006

Joe Welsh Date
Program Manager, Case Management Applications
Executive Office for United States Attorneys
U.S. Department of Justice

/signed/ 5/31/2006

Siobhan Sperin Date
System Owner, Case Management Applications
Assistant Director, Case Management Staff
Executive Office for United States Attorneys
U.S. Department of Justice

/signed/ 5/31/2006

William G. Stewart, II Date
Acting Assistant Director, Freedom of Information & Privacy Staff
Executive Office for United States Attorneys
U.S. Department of Justice

/signed/ 6/1/2006

David W. Downs Date
Acting Chief Information Officer
Executive Office for United States Attorneys
U.S. Department of Justice

System Description: The Case Management Applications provide case management and resource management for the 94 individual United States Attorneys Offices (USAOs) through the LIONS and USA-5 databases. LIONS is a case management system which allows offices to track civil and criminal cases and appeals. USA-5 is a resource management database which tracks information pertaining to personnel resource allocations.

The Case Management Applications is currently operational.

System Purpose: LIONS allows individual districts to maintain information on pending workloads and provides a variety of reporting views of the data. In addition, LIONS provides key data to the Executive Office for United States Attorneys (EOUSA) management to respond to numerous requests for statistical information from other government agencies, Congress, and the public. USA-5 summarizes the personnel resources allocated to the USAOs on a monthly basis and allows EOUSA the opportunity to use the Congressionally appropriated resources. In the course of serving this purpose, the Case Management Applications must collect and maintain certain personal information which identifies criminal defendants.

Assessment:

1. What information is to be collected?

   A clear relationship has been established between the personal information to be collected and Case Management Applications operational requirements. The personal information to be collected is pertinent to the stated Case Management Applications purpose and only information that is required is collected. The personal information to be collected and maintained by Case Management Applications is:

   a. USA-5
      i. System Manager Name
   b. LIONS
      i. Email address of agent
      ii. Fax number of agent
      iii. First name of agent
      iv. Last name of agent
      v. Pager number of agent
      vi. Phone number of agent
      vii. Salutation of agent
      viii. Title of agent
      ix. First name of an alias

x. System generated value for use in a sounds-like search on the first name of an alias
xi. System-generated sequence number that identifies the alias
xii. Last name of the alias
xiii. System-generated value for use in a sounds-like search on the last name of an alias
xiv. First name of the participant
xv. System-generated value for use in a sounds-like search on an archived participants first
xvi. name
xvii. Last name of the participant
xviii. System-generated value for use in a sounds-like search on an archived participant's last
xix. name
xx. Name of the bondsman or bonding company
xxi. Date of Defendant's birthday
xxii. Last name of a contact person when the participant is a business
xxiii. First name of a contact person when the participant is a business
xxiv. IRS Employer Identification Number when the participant is a business
xxv. Name of the Employer
xxvi. Internal Number assigned by the FBI to a defendant
xxvii. First name of a participant in a given record
xxviii. System-generated value for use in a sounds-like search on the first name of a participant
xxix. First line of a participant's address
xxx. Second line of participant's address
xxxi. Third line of a participant's address
xxxii. The name of a city where the participant resides
xxxiii. The country where a participant resides
xxxiv. Fax number of a participant
xxxv. Home phone number of a participant
xxxvi. The state where the participant resides
xxxvii. The zip code where the participant resides
xxxviii. Code that describes the immigration status of the participant
xxxix. Code that indicates the participant is a juvenile
xl. Last name of the participant
xli. System-generated value for use in a sounds-like search on the last name of a participant
xlii. Internal number assigned by the U.S. Marshals to the participant
xliii. National Provider Identification
xliv. First line of a participant's office address
xlv. Second line of a participant's office address
xlvi. Third line of a participant's office address
xlvii. City of a participant's office

xlviii. County of a participant's office
xlix. Fax number of the participant's office
l. Telephone number of the participant's office
li. State of the participant's office
lii. Zip code of the participant's office
liii. Local Police Department ID number of the participant
liv. Code that identifies the participant's role in the civil/criminal action
lv. Participant's salutation
lvi. Code that describes security associated with the participant
lvii. SSN of participant
lviii. Participant title
lix. System-generated sequence number that identifies the staff member making the request
lx. System-generated sequence number that identifies the security case staff group
lxi. Phone number of an employee
lxii. User Name assigned to staff member authorizing use of the LIONS application

2. Why is the information being collected?

The Case Management Applications collects personal information necessary for civil and criminal case tracking.

3. What is the intended use of the information?

The Case Management Applications data is used by the USAOs to manage litigation. The EOUSA uses the data to justify budget requests, allocate resources among USAOs, and produce management reports. The data is also used to produce numerous periodical and ad-hoc reports for the Attorney General, Office of Management and Budget, Congress, and various federal agencies and private sector organizations. The USAOs also utilize this data to allocate resources, justify expenditures, and produce local management reports.

4. With whom will the information be shared?

The personal information will be shared only with cleared and authorized users having a legitimate need to know.

5. What opportunities will individuals have to decline to provide information or to consent to particular uses of the information, and how individuals can grant consent?

As the personal information is required for litigation, individuals have no opportunity to decline to provide or consent to particular uses of the information.

6. How will the information be secured?

The information is secured with management, operational, and technical controls as delineated by NIST Special Publication 800-53 *Recommended Security Controls for Federal Information Systems*. The applied system category control set is **moderate** as defined by NIST Special Publication 800-60 *Guide for Mapping Types of Information and Information Systems to Security Categories*. The system is certified and accredited for control compliance as well as adherence to industry security best practices and mitigation of risk due to technical vulnerabilities.

The potential risk for unauthorized disclosure of personal information is mitigated by

- limiting the number of authorized system users,
- performing background investigations on candidate users,
- providing initial and annual system security training,
- identifying sealed cases,
- vetting Freedom of Information Act (FOIA) requests,
- limiting physical access to the system, and
- monitoring network activity with a continuously monitored intrusion detection System.

7. Is the system of records being created under the Privacy Act, 5 U.S.C. 552a?

Yes. The information collected and maintained by Case Management Applications is governed by the Privacy Act. The information may be disclosed without the individual's consent, but only as permitted by the Privacy Act, the Freedom of Information Act, and in accordance with established Case Management Applications policy and procedure.