

Privacy Impact Assessment

for the

Master Index Application

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).

<u>/signed/</u>	<u>5/25/2006</u>
Michael Vasquez	Date
Program Manager, Master Index System	
United States Attorney's Office, District of Columbia	
U.S. Department of Justice	

<u>/signed/</u>	<u>Monty Wilkinson for</u>	<u>5/25/2006</u>
Kenneth Wainstein		Date
System Owner, Master Index System		
United States Attorney, District of Columbia		
U.S. Department of Justice		

<u>/signed/</u>	<u>5/31/2006</u>
William G. Stewart, II	Date
Acting Assistant Director, Freedom of Information & Privacy Staff	
Executive Office for United States Attorneys	
U.S. Department of Justice	

<u>/signed/</u>	<u>6/1/2006</u>
David W. Downs	Date
Acting Chief Information Officer	
Executive Office for United States Attorneys	
U.S. Department of Justice	

System Description: The Master Index (MI) application provides automated data consolidation from multiple information sources. MI indexes key information to enable complex data searches and queries.

System Purpose: The MI application provides investigators and prosecutors the ability to link multiple crimes and cases, thereby supporting prosecutorial and investigative decisions. In the course of serving this purpose, the MI application maintains certain personal information which identifies criminal defendants, informants, crime victims, and witnesses.

Assessment:

1. What information is to be collected?

The MI application stores the following information:

- a. Name,
- b. Date of Birth,
- c. Social Security Number
- d. Residence Address,
- e. Aliases,
- f. Arrest Location, and
- g. Affiliated Locations.

2. Why is the information being collected?

The information is collected to pursue justice more effectively and efficiently, by merging “information islands” that can be queried as a single entity.

3. What is the intended use of the information?

The intended use of the information is to correlate and de-conflict case information, improving the coordination of investigative and prosecutorial efforts. The MI application can automatically transmit alerts to notify users of linkages to specific locations or persons of interest, thereby promoting operational efficiencies.

4. With whom will the information be shared?

MI information sharing is limited to authorized users within the District of Columbia United States Attorney's office (DC USAO). Users include investigators, prosecutors, and authorized support staff adjudicated to have a legitimate need for system access.

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?

Individuals are involuntarily added into the Master Index application when they have any involvement in an investigation or case in which the USAO DC has jurisdiction. Upon case closure, defendants may apply to be removed from the system. Individuals do not have the opportunity to 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 best security 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,
- ▶ 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 the MI application 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 policy and procedure.