United States Department of Justice
Antitrust Division

Management Information System (MIS)
Privacy Impact Assessment

Prepared By
United States Department of Justice
Antitrust Division

21-JUNE-2007

Introduction

The Department of Justice (DOJ) Antitrust Division (ATR) controls and manages a Management Information System (MIS) used to process, store and transmit information. The ATR MIS is a Sensitive But Unclassified system that supports the Antitrust Division by providing a platform for processing, storing and transmitting management, support and historic mission-based information.

The Antitrust Division makes broad use of National, Government and Department standards in assuring the protection of Privacy Act systems under its control. A key part of the standards focus on mandated Federal Information Processing Standards and associated National Institute of Standards and Technology Special Publications. The Antitrust Division has developed a managed process to ensure its automated systems security programs are current with all applicable revisions and releases of applicable Federal standards. This is complimented by activities to ensure system patches and fixes are fully current and security configuration polices are not compromised.

ATR regards the protection of information as a mandatory requirement in the enforcement of antitrust law in both criminal and civil enforcement actions. Continuing enhancement of security safeguards and procedures assist the Antitrust Division in supporting all of its security objectives through application of Federal Information Security Management Act (FISMA) requirements and industry Best Practices.

MIS PIA Framework

Document Compliance

This MIS PIA complies with the Privacy Impact Assessment Official Guidance issued by the DOJ Privacy and Civil Liberties Office, effective August 7, 2006.

Document Organization

Document Audience

This document is intended for public access.

Document Change Control

The Management Information System PIA is subject to a formal configuration control process to provide for tracking of changes.

MIS PIA Point of Contact

Mr. Thomas King
ATR Executive Officer
Patrick Henry Building
601 D Street NW, Washington, DC 20530
Telephone: 202-514-4005
E-mail: THOMAS.KING@USDOJ.GOV

Section 1.0
The System and the Information Collected and Stored within the System.

1.1 What information is to be collected?

MIS stores ATR management, support and mission-based information. The information is collected consistent with OMB Circular A-11 and the fulfillment of antitrust enforcement activities.

MIS applications currently include Information in Identifiable Form (IIF) in the general categories and for the particular groups listed below:

Data Type	Data Obtained From
Name	Company, Law Firm, Government Staff, Contractor Staff
Address	Company, Law Firm, Government Staff, Contractor Staff
Telephone Number	Company, Law Firm, Government Staff, Contractor Staff
Social Security Number	Government Staff
Staff ID	Government Staff, Contractor Staff
E-mail	Government Staff; Contractor Staff
Gender	Government Staff
Home Address	Government Staff
Home Telephone Number	Government Staff
Race	Government Staff
Disability Status	Government Staff
Salary	Government Staff
Contractor Billing Rates	Contractor Staff
Date of Birth	Government Staff

1.2 From whom is the information collected?

Information is collected from parties to, or targets of, criminal or civil antitrust investigations. Information is also collected from ATR government and contractor personnel who support the Division's mission.

Section 2.0
The Purpose of the System and the Information Collected and Stored within the System.

2.1 Why is the information being collected?

Information is collected to support ATR's mission; specifically promotion and protection of the competitive process and the United States economy through enforcement of antitrust law. Information stored within MIS represents the institutional knowledge of the Division. Information is also collected to support ATR's management and operations.

2.2 What specific legal authorities, arrangements, and/or agreements authorize the collection of information?

ATR is authorized to collect mission-based information under the provisions of the Sherman Antitrust Act, the Clayton Antitrust Act, and the Hart-Scott-Rodino Act. In addition, ATR is authorized to collect management and support information under the provisions of OMB Circular A-11.

2.3 Privacy Impact Analysis: Given the amount and type of information collected, as well as the purpose, discuss what privacy risks were identified and how they were mitigated.

Privacy risks would result from a breach to ATR's security safeguards as implemented on MIS, which could subsequently compromise the confidentiality, integrity and availability of information. This breach would occur, primarily, through unauthorized access that would enable an adversary to disclose, damage the integrity of, or prevent the availability of information used to support the enforcement of antitrust laws and executive operations.

The risk of data compromise, or the theft of backup tapes, is mitigated by several steps. Physical security, such as guards, access badges and security cameras help ensure there is no unauthorized access to component facilities. Unauthorized access to the system itself is addressed by network intrusion detection systems, firewall log monitoring, malware detection and correction software. To prevent unauthorized use by agency employees, audit logs are kept and checked at regular intervals. Unauthorized use by a Federal employee will be subject to strict penalties.

ATR implements security controls as mandated in Security Requirements for Federal Information and Information Systems, and Recommended Security Controls for Federal Information Systems. Implementation of these controls and associated risks and mitigation is reflected in required security documentation.

Section 3.0
Uses of the System and the Information.

3.1 Describe all uses of the information.

The information that MIS applications process, store and transmit is used to support the Division's mission, including files such as public court and administrative filings, complaints, indictments, and final judgments, as well as statements of policy and interpretations, staff manuals, guidelines, press releases, speeches, Congressional testimony, work product, and business review letters. Management and support records include identification of personnel who work on the Division's cases and the number of labor hours invested in these cases. The MIS stores a body of historic information in databases that are accessible to authorized Division users.

Information used in MIS applications that is subject to the Privacy Act includes the following general categories:

- Planning and Resource Allocation -- ATR Intranet, Central Files Tracking System, Matter Tracking System, Time Reporting System.
- Personal Identity and Authentication Information -- Human Resources System.
- Payments Information -- Employee Time Reporting System.
- Human Resources -- Human Resources System, Recruitment Tracking System for Attorneys, Recruitment Tracking System for Paralegals, Employee Time Reporting System.
- Information and Technology Management -- Human Resources System, Recruitment Tracking System for Attorneys, Recruitment Tracking System for Paralegals, Employee Time Reporting System, Field Office Matter Tracking System, FOIA Tracking System.
- Litigation and Judicial Activities -- ATR Intranet, Appellate Docket System, Civil Non-Merger Tracking System, Correspondence and Complaint Tracking System, Criminal Case Sentencing System, Economic Analysis Group Tracking System, Economic Analysis Group Working Papers, Field Office Matter Tracking System, Hart-Scott-Rodino Tracking System, Legislative Tracking System, Matter Tracking System.

3.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern? (Sometimes referred to as data mining.)

No.

3.3 How will the information collected from individuals or derived from the system, including the system itself be checked for accuracy?

The historic mission-based information provided to MIS is processed, stored, and transmitted as-is. MIS applications include transaction validation controls (e.g., an end date does not precede an associated start date) and certain format validation controls (e.g., number of digits in a Social Security Number) for management and support information.

3.4 What is the retention period for the data in the system? Has the applicable retention schedule been approved by the National Archives and Records Administration (NARA)?

Most of the information in the Management Information System (MIS) generally is permanent. The system, however, includes certain administrative data that is valid for a limited period and either updated or removed from the System as it becomes obsolete. Consultation between ATR and the National

Archives and Records Administration is ongoing on the issue of historical records and their disposition. Given that the ATR MIS serves both current operational needs as well as long-term knowledge management requirements for preserving institutional history and facilitating research on historical matters that related to current matters, ATR expects constantly to be enhancing the historical data in this repository, rather than archiving and removing it from the system.

3.5 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above-described uses.

The key MIS controls to assure that information is handled in accordance with its prescribed use include:

- Technical Class Controls
  - Access Controls:
    - Account Management
    - Access Enforcement
    - Separation of Duties
    - Least Privilege
    - Unsuccessful Login Attempts
    - System Use Notification
    - Session Lock
    - Supervision and Review -Account Management
  - Audit Controls:
    - Auditable Events
    - Audit Analysis, Monitoring, and Reporting
  - Identification and Authentication:
    - Authenticator Management
- Management Class Controls
  - Security Planning, Policy, and Procedures
    - Rules of Behavior
  - Systems and Services Acquisition Policy and Procedures
    - Software Usage Restrictions
    - Security Engineering Principles
- Operational Class Controls
  - Security Awareness and Training Policy and Procedures
    - Security Awareness
    - Security Training

Implementation of these controls is documented in the MIS System Security Plan that addresses all of the areas identified above, including how ATR employees are granted system access based upon their organizational role and need to know, authorizing officials, technical aspects of authentication management, software use and engineering, and the auditing of access files to ensure the protection of data maintained by ATR.

ATR is required to address continual statutory and Department-level requirements to substantiate that its handling of information is compliant. For example, ATR was recently required to provide submissions in support of DOJ Memorandum Privacy and Safeguarding of Personally Identifiable Information dated 10-July-2006. Furthermore, ATR issued ATR Directive 2710.4 Safeguarding Sensitive Information dated 11-July -2006 to assure Division compliance. From a technical perspective, continuous monitoring requirements provide assurance that privacy-applicable controls are consistent with MIS Certification and Accreditation.

Section 4.0
Internal Sharing and Disclosure of Information within the System.

4.1 With which internal components of the Department is the information shared?

ATR shares MIS data, as appropriate, with the:

- Office of the Inspector General
- Justice Management Division (JMD).

4.2 For each recipient component or office, what information is shared and for what purpose?

All the information described in Section 1.1 may be shared. The purpose of this sharing is outlined below.

- Office of the Inspector General -- Management and support information is provided to assist with audit requirements.
- Justice Management Division -- Management and support information is provided for the ongoing operations of the Department of Justice, e.g., personnel, employee time-accounting, vendor payments. Historic mission-specific information is provided to JMD for uploading to the Division's Internet website once it has been identified as public-releasable.

4.3 How is the information transmitted or disclosed?

No other DOJ components have end-user access to MIS. Information is:

- Exchanged via internal e-mail
- Exchange via DOJ-approved courier delivery
- Hand-carried

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

The fundamental privacy risk lies in unauthorized disclosure based on methods of sharing. The two methods and the mitigation of potential risks are as follows:

- Information delivered by courier or hand-carried is subject to media labeling controls. Transport of this information is subject to DOJ controls for media transport.

- E-mail is subject to the Division's infrastructure security controls.

All DOJ components are subject to DOJ Order 2640.1 and DOJ Order 2640.2E and the associated Information Technology Security Standards.

Section 5.0
External Sharing and Disclosure

5.1 With which external (non-DOJ) recipient(s) is the information shared?

Information may be shared with the:

- Federal Trade Commission (FTC).
- Office of Management and Budget (OMB)
- Government Accountability Office (GAO)
- Congress

Private Sector:
The Antitrust Division's Internet web site (www.usdoj.gov/atr) contains content that has been identified as publicly releasable information in accordance with a tightly controlled review process.

5.2 What information is shared and for what purpose?

- Mission-specific information may be shared under inter-agency cooperation agreements.
- Clearance and pre-merger data may be shared with the FTC as appropriate in support of HSR filings.
- Information from the Matter Tracking System may be been shared with OMB, GAO, and Congress.

Private Sector
The ATR Internet site contains public documents including court and administrative findings such as complaints, indictments, and final judgments, as well as guidelines, press releases, speeches, Congressional testimony, and business review letters. The site's Privacy Act and Disclaimer of Information notice outlines any collection of information from visitors to this site and any use of such information. In addition, the handling of any information actively provided by visitors to this site is addressed in the published notice.

5.3 How is the information transmitted or disclosed?

Information shared with the FTC is transmitted via a secure system interconnection.

Private Sector
JMD is responsible for uploading MIS historic mission-based information to the ATR Internet website. ATR transmits information to JMD via secure internal connections.

5.4 Are there any agreements concerning the security and privacy of the data once it is shared?

The provisions regarding sharing of information with the FTC are documented in an ATR-FTC Memorandum of Understanding.

Private Sector
The ATR Internet website Privacy Policy identifies privacy and security conditions.

5.5 What type of training is required for users from agencies outside DOJ prior to receiving access to the information?

There are no antitrust-specific courses offered to employees of other agencies that receive information from the Antitrust Division. However, all Federal Agencies are required to implement Standards of Ethical Conduct for Employees of the Executive Branch (5 CFR 2635) via Rules of Behavior per Office of Management and Budget (OMB) Circular A-130, Appendix III, Security of Federal Automated Information Resources.

5.6 Are there any provisions in place for auditing the recipients' use of the information?

There are no provisions in place at this time for auditing recipient use of information. However, if ATR suspected or became aware of misuse, it would use its full authority promptly to resolve the issue.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

The predominant privacy risk attributable to sharing data with the FTC lies in a breach to confidentiality. To mitigate this risk ATR and FTC have instituted several technical, operational and management controls. Secure transfer protocols are deployed in the transmission of information; access authorized controls are enforced and reviewed using a documented procedure; and a Memorandum of Understanding is in place.

Private Sector
The delivery of the content from the MIS staging server to the JMD servers for Internet deployment is access-controlled to assure accountability.

Section 6.0
Notice

6.1 Was any form of notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

The ATR System of Records listing is provided at Appendix A of this PIA. Any Privacy Act information that may be collected is related to Division law enforcement purposes.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

No. Any Privacy Act information that may be collected is related to Division law enforcement purposes.

6.3 Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?

No. Any Privacy Act information that may be collected is related to Division law enforcement purposes.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

The predominant privacy risk lies in improper disclosure. All DOJ government and contractor staff are aware of penalties regarding improper use of information per Entry On Duty training materials and Rules of Behavior.

Section 7.0
Individual Access and Redress

7.1 What are the procedures which allow individuals the opportunity to seek access to or redress of their own information?

Individuals may make a request for access to or amendment of their records under the Privacy Act unless the particular System of Records is exempted from the access and amendment provisions.

7.2 How are individuals notified of the procedures for seeking access to or amendment of their information?

Notice of an individual's rights under the Privacy Act is provided through publication in the Federal Register of a System of Records Notice and in Departmental regulations describing the procedures for making access/amendment requests.

7.3 If no opportunity to seek amendment is provided, are any other redress alternatives available to the individual?

No.

7.4 Privacy Impact Analysis: Discuss any opportunities or procedures by which an individual can contest information contained in this system or actions taken as a result of agency reliance on information in the system.

Information on Government employees or contractors may be addressed through a written request for correction if necessary. This process also applies to business or private individuals who may request a

correction to publicly available information. An individual may file a lawsuit under the Privacy Act after following appropriate administrative processes.

Section 8.0
Technical Access and Security

8.1 Which user group(s) will have access to the system?

The following user groups have access to MIS:

- All Antitrust Division staff are required to use the Division's Time Reporting System (TRS).
- MIS Privileged Users, including Network Administrators, Database Administrators, Application Developers and Web Analysts have access to MIS applications. These privileged users include Government personnel and contractors.
- Subject-Matter Experts whose privileges to management and support and mission-specific information are based on job description.

8.2 Will contractors to the Department have access to the system? If so, please submit a copy of the contract describing their role with this PIA.

Contractors have access to the system in the capacities referenced in Section 8.1. Contract documents are available but not attached and may be provided by the ATR Point of Contact.

8.3 Does the system use "roles" to assign privileges to users of the system?

MSS implements three basic roles for MIS:

- End-User
- Developer
- System Administrator/Database Administrator

8.4 What procedures are in place to determine which users may access the system and are they documented?

The procedures in place to determine which users may access the system are documented in the MIS System Security Plan that addresses all of the areas identified in Section 3.5 of this PIA, including how ATR employees are granted system access based upon their organizational role and need to know, authorizing officials, technical aspects of authentication management, and software use and engineering to ensure the protection of data maintained by ATR. The MIS System Security Plan also includes details regarding password management, account management, and auditing for each user group, in accordance with DOJ Order 2640.2E.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

Individuals have specific roles that limit them to the data they enter or have specific rights to address. Actual assignments of roles and rules are established for ATR in its MIS System Security Plan that

addresses such areas as how ATR employees are granted system access based upon their organizational role and need to know, authorizing officials, technical aspects of authentication management, software use and engineering, and the auditing of access files to ensure the protection of data maintained by ATR. The use of JMD-mandated tools for security configuration compliance enables this verification, including, for example, whether guest/anonymous accounts are disabled and identifiers are unique.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

The following in-place auditing measures and technical safeguards are applied to prevent misuse of data. ATR constantly evaluates new technologies and procedures to enhance these capabilities. These controls include:

- Authenticator/Password Management -- Application and monitoring of initial distribution, composition, history, compromise, and change of default authenticators.

- Account Management -- Application and monitoring of account establishment, activation, modification, disabling, removal (including unnecessary/defunct accounts) and review, all of which support implementation of need-to-know.

- Access Enforcement -- Application and monitoring of access privileges.

- Least Privilege -- Provision of the minimum tools required for a user to perform his/her function.

- Unsuccessful Login Attempts -- MIS automatically locks the account until released by a System Administrator when the maximum number of unsuccessful attempt is exceeded.

- Audit trails are generated by MIS applications. The audit trails facilitate intrusion detection and are a detective control for identifying data misuse. The MIS also is configured to protect audit information and tools from unauthorized access, modification and deletion. Audit notifications are generated in response to pre-specified triggers.

Auditing measures and technical safeguards employed by the Antitrust Division are:

- Required by FISMA
- Configured in accordance DOJ Order 2640.2E
- Consistent with the FEA Security and Privacy Profile

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

All employees are required to complete online information systems security training as part of annual training for DOJ employees. A certificate of completion is logged for employees after successful completion of the training. Also, new employees receive training on the use of particular MIS applications before they are granted access to the system. Users are reminded periodically about Division policies in these areas and their requirements to comply with these policies.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

The data are secured in accordance with the DOJ schedule-driven implementation of FISMA requirements as recorded in the JMD Trusted Agent application. The last Certification & Accreditation (C&A) was completed in 2003. MIS is currently undergoing C&A with a target date of re-accreditation of December 2006.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

Privacy risks associated with unauthorized disclosure of information are mitigated through implementation of technical controls associated with need-to-know and least privilege, ensuring that users have no more privileges to data than required to effect their official duties. In addition, deterrent controls in the form of warning banners, privileged rules of behavior, confidentiality agreements and auditing are in place. Finally, exit procedures for departing employees and contractors include the prompt disabling of accounts and access rights to all data.

Section 9.0 Technology

9.1 Were competing technologies evaluated to assess and compare their ability to effectively achieve system goals?

Yes. As the ATR Management Information System was initially developed many years ago, software tools were competitively identified to ensure the best and most cost effective products were chosen. In subsequent years, as ATR has upgraded and improved its MIS, enhancements have been developed and deployed by ATR staff. With all acquisitions of new or upgraded hardware, software or other products, a cost-benefit analysis has been performed in accordance with DOJ requirements. MIS investments are pursued in accordance with the relevant provisions of the Department of Justice Systems Development Life Cycle Guidance and Federal Acquisition regulations.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

ATR implements data integrity controls to protect data from accidental or malicious alteration or destruction and to ensure that the information is accurate and has not been altered. In addition, ATR employs an intrusion detection system to detect vulnerabilities, changes to the network, and traffic anomalies. Further, ATR backs up data regularly and controls access to data stored in the MIS. As part of ATR's decision-making process regarding security, it performed a requirements analysis December 7, 2001, under the direction of the DOJ Program Management Office (PMO). This document outlined the business, functional and technical requirements for the ATR environment. To ensure a secure environment, as well as to protect the integrity and availability of data, the requirements analysis identified the constraints and conditions adhered to during system deployment.

9.3 What design choices were made to enhance privacy?

ATR's security strategy includes protecting ATR assets from outside attackers as well as from internal security violations. To protect personally identifiable and proprietary information, ATR implemented an incident response plan and a MIS computer security policy. ATR also requires users to sign General User Rules of Behavior, which address accountability by requiring ATR personnel to protect any and all sensitive information stored or processed by ATR computer systems. ATR also employs auditing controls, an intrusion detection system, secure router configurations, inactivity logouts and firewalls. ATR installs security software on laptops to enhance the security of data.

Conclusion

MIS is used to process, store, and transmit information that supports Antitrust Division operations for management and support, and historic mission-specific purposes. Securing this information and assuring its proper use is critical to the success of these operations.

MIS applications are secured via access authorization, authentication rules, and audit controls. These technical controls are supplemented by procedural controls such as Account Management Reviews, Rules of Behavior, Confidentiality Agreements, and Security Awareness and Training to mitigate risks regarding unauthorized access and subsequent potential privacy violations.

ATR has consistently regarded the privacy ramifications of information that is processed, stored, and transmitted on MIS as critical in supporting antitrust enforcement activities and executive operations and pursues its security objectives through application of FISMA requirements and industry Best Practices. Management review, continual enhancement, and continuous monitoring of MIS technical and procedural controls are of the utmost importance in protecting privacy information while also ensuring that ATR maintains continuity in its operations.

Appendix A: ATR SORN

SYSTEM	TITLE	DATE PUBLISHED	FEDERAL REGISTER
ATR-001	Antitrust Division Expert Witness File	10-13-89	54 FR 42061
ATR-003	Index of Defendants in Pending and Terminated Antitrust Cases	10-10-95	60 FR 52690
ATR-004	Statements by Antitrust Division Officials (ATD Speech File)	10-10-95	60 FR 52691
ATR-005	Antitrust Caseload Evaluation System (ACES) - Time Reporter	10-17-88	53 FR 40502
ATR-006	Antitrust Caseload Evaluation System (ACES) - Monthly Report	02-20-98* 03-29-01	63 FR 8659* 66 FR 17200
ATR-007	Antitrust Division Case Cards	10-10-95	60 FR 52692
ATR-009	Public Complaints and Inquiries File	11-17-80	45 FR 75902
ATR-014	Civil Investigative Demand (CID) Tracking System	10-10-95	60 FR 52694

Last publication of complete notice
Source: http://jmdint01.atrnet.gov/jmd/privacy/#ATR on date of issuance of this PIA.