

**United States Department of Justice
Antitrust Division**

**Management Information System (MIS)
Privacy Impact Assessment**

**Prepared By
United States Department of Justice
Antitrust Division**

29-SEPTEMBER-2006

Approval Signature Page

I recommend approval of the Antitrust Division Information Systems Support Group Management Information Systems Privacy Impact Assessment

_____	_____
Durwin Smith System Owner, Management Information Systems Chief, Management Systems Staff	Date

_____	_____
Carl Anderson Chief, Information Systems Support Group	Date

_____	_____
Thomas King Executive Officer, Antitrust Division	Date

I approve the Antitrust Division Information Systems Support Group Management Information Systems Privacy Impact Assessment

_____	_____
Jane Horvath Chief Privacy and Civil Liberties Officer	Date

Table of Contents

Introduction 1
MIS PIA Framework 2
Section 1.0 The System and the Information Collected and Stored within the System. 3
Section 2.0 The Purpose of the System and the Information Collected and Stored within the System. 3
Section 3.0 Uses of the System and the Information..... 4
Section 4.0 Internal Sharing and Disclosure of Information within the System. 7
Section 5.0 External Sharing and Disclosure..... 8
Section 6.0 Notice 9
Section 7.0 Individual Access and Redress..... 10
Section 8.0 Technical Access and Security 11
Section 9.0 Technology..... 13
Conclusion 14
Appendix A: ATR SORN 16
Appendix B: References 17
Appendix C: Abbreviations and Acronyms..... 19

Introduction

The Department of Justice (DOJ) Antitrust Division (ATR) Information Systems Support Group (ISSG) Management Systems Staff (MSS) owns the ATR Management Information Systems (MIS) that is used to process, store and transmit information. The ATR MIS is a Sensitive But Unclassified (SBU) system has been implemented under the provisions of the Federal Information Security Management Act (FISMA, Public Law 107-347) and Department of Justice (DOJ) Order 2640.2E Information Technology Security.

The mission of the Antitrust Division is to promote and protect the competitive process and the American economy through enforcement of the antitrust laws. The antitrust laws apply to virtually all industries and to every level of business, including manufacturing, transportation, distribution, and marketing. They prohibit a variety of practices that restrain trade, such as price-fixing conspiracies, corporate mergers likely to reduce the competitive vigor of particular markets, and predatory acts designed to achieve or maintain monopoly power. The ATR-MIS supports the antitrust mission by providing a platform that enables the processing, storage and transmission of management and 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 usage focuses on the FISMA-mandated (FISMA Sec. 303 (b)(1)(A)) Federal Information Processing Standards (FIPS) and associated National Institute of Standards and Technology (NIST) Special Publications (SPs). The Antitrust Division has developed a managed process to ensure that its security program is current with all applicable revisions and releases of FIPS, NIST SPs, and OMB Memoranda in order to protect its assets. This programmatic effort is complimented by scanning activities to ensure that the system's patches and fixes are fully current, and that its security configuration polices are not compromised.

ATR regards the protection of information security, as defined in 44 U.S.C. Section 3542, as a mandatory requirement in the enforcement of antitrust law in both criminal and civil enforcement actions. The MIS implementation and continuing enhancement of security safeguards and procedures is aligned with supporting all of ATR's security objectives via application of FISMA requirements and industry Best Practices.

MIS PIA Framework

The MIS PIA Framework provides programmatic information associated with the development and management of the MIS PIA.

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

This MIS PIA applies the DOJ Privacy Impact Assessment Template (v3) as follows:

- Introduction;

- Responses to questions, and summaries requested in Sections 1 through 9 of the afore-referenced template;

- Conclusion.

The following appendices are included:

- Appendix A: ATR SOR

- Appendix B: References

- Appendix C: Abbreviations and Acronyms

Document Audience

This document is intended for public access in accordance with OMB M-03-22 Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, Attachment A/I.A.1.

Document Change Control

The MIS PIA is subject to the MSS Configuration Control process as documented in the MSS Configuration Management Plan.

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 and support, and mission-based information, as defined in the Federal Enterprise Architecture (FEA) Business Reference Model. The information is collected via executive operations as required by OMB Circular A-11 and the execution of antitrust enforcement activities.

MIS applications currently include the Information in Identifiable Form (IIF) listed below, as defined in OMB Memorandum M-03-22/Attachment A/II.A.2.

- 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?

The information is collected to support ATR's mission; specifically promotion and protection of the competitive process and the United States economy via the enforcement of antitrust laws. Information stored within MIS represents the institutional knowledge of the Division's spectrum of operations. Information is also collected to support ATR's executive 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.
- 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.

From an information technology perspective, privacy risks would result from a breach to ATR's security objectives as implemented on MIS, which could subsequently compromise the confidentiality, integrity, and availability of information. From an MIS perspective, this breach would occur, primarily, via 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 compromise of data, 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, firewalls 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 FISMA security controls as mandated in FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems," and amplified in NIST SP 800-53, "Recommended Security Controls for Federal Information Systems." The MIS implementation of these controls and associated risks and mitigation is reflected in FISMA and Justice Management Division-mandated 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 are 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 Oracle databases that are accessible to authorized Division users via the Intranet or through tools such as Business Objects.

Information used in MIS Applications that is subject to the Privacy Act maps to the following NIST SP 800-60 information and information types. The related MIS applications used to process, transmit, and store the information are also provided.

- Planning and Resource Allocation. Applicable MIS applications: ATR Intranet, Central Files

- Tracking System, Matter Tracking System, Time Reporting System.
- Personal Identity and Authentication Information. Applicable MIS application: Human Resources System.
- Payments Information. Applicable MIS application: Employee Time Reporting System.
- Human Resources: Applicable MIS applications: Human Resources System, Recruitment Tracking System for Attorneys, Recruitment Tracking System for Paralegals, Employee Time Reporting System.
- Information and Technology Management: Applicable MIS applications: 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: Applicable MIS applications: 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.)

Data mining including pattern-based querying, is employed in the course investigations using the tools of litigation support, economic analysis and management information systems. The scope of data mining is limited to DOJ Order 2640.2E requirements for Least Privilege (NIST SP 800-53/AC-6) and Need-to-Know (addressed via NIST SP 800-53/AC-2). As management information applications store historic data for the explicit purpose of knowledge management, data mining in the form of, for example, searches for patterns of conduct by specific corporations and / or individuals across historic investigative data, is an important asset in the conduct of new investigations.

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)?

There is no schedule for retiring data out of the MIS. Consultations between ATR and NARA are ongoing on the issue of historical records and how they should be addressed, given that the ATR MIS serves both current operational needs as well as long term "knowledge management" requirements preserving institutional history and facilitating research on historical matters which relate to current matters. Consequently, ATR expects to be constantly 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 (NIST SP 800-53/AC-2)
 - Access Enforcement (NIST SP 800-53/AC-3)
 - Separation of Duties (NIST SP 800-53/AC-5)
 - Least Privilege (NIST SP 800-53/AC-6)
 - Unsuccessful Login Attempts (NIST SP 800-53/AC-7)
 - System Use Notification (NIST SP 800-53/AC-8)
 - Session Lock (NIST SP 800-53/AC-11)
 - Supervision and Review -Account Management (NIST SP 800-53/AC-13)
 - Audit Controls:
 - Auditable Events (NIST SP 800-53/AU-2)
 - Audit Analysis, Monitoring, and Reporting (NIST SP 800-53/AU-6)
 - Identification and Authentication:
 - Authenticator Management (NIST SP 800-53/IA-5)
- Management Class Controls
 - Security Planning, Policy, and Procedures
 - Rules of Behavior (NIST SP 800-53/PL-4)
 - Systems and Services Acquisition Policy and Procedures
 - Software Usage Restrictions (NIST SP 800-53/SA-6)
 - Security Engineering Principles (NIST SP 800-53/SA-8)
- Operational Class Controls
 - Security Awareness and Training Policy and Procedures
 - Security Awareness (NIST SP 800-53/AT-2)
 - Security Training (NIST SP 800-53/AT-3)

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 FISMA-mandated Continuous Monitoring requirements (NIST SP 800-53/CA-7) provide assurance that privacy-applicable controls are consistent with the MIS Certification and Accreditation status.

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 in accordance with DOJ Order 2640.2E and NIST SP 800-53/MP-3. Transport of this information is subject to DOJ controls for Media Transport and is compliant with NIST SP 800-53/MP-5.
- E-mail is subject to the Division's infrastructure security controls, which are FISMA-compliant based on its current Certification and Accreditation status.

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 is shared with

- 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 per the Department of Justice review process.

5.2 What information is shared and for what purpose?

- Mission-specific information is 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 has 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 that is shared with the FTC is transmitted via a secure system interconnection that uses security mechanisms and services embedded in commercial-off-the-shelf software.

Private Sector

JMD is responsible for uploading MIS historic mission-based information to the ATR internet website. ATR transmits the 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 the sharing of information with FTC are documented in the 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 the recipients' 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 SORN listing is provided at Appendix A, ATR SOR, 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 can 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 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 three 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 (SA/DBA)

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 assignment of roles and rules are verified via the implementation of FIPS 200 Access Controls (AC) and Audit and Accountability (AU) families of controls. Additionally, the use of JMD-mandated COTS tools for Security Configuration Policy compliance enables this verification. For example, these tools identify whether:

- Guest/anonymous accounts are disabled (NIST SP 800-53/AC-2)
- Identifiers are unique (NIST SP 800-53/IA-4)

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. It should be emphasized that under the FISMA requirement for Continuous Monitoring (NIST SP 800-53/CA-7), ATR constantly evaluates new technologies and procedures to enhance these capabilities. The primary auditing measures and technical safeguards in place to prevent misuse of data are associated with access and authentication controls to prevent unauthorized disclosure and subsequent potential misuse of data. These controls include:

- Authenticator/Password management, i.e., application and monitoring of initial distribution, composition, history, compromise, and change of default authenticators (NIST SP 800-53/IA-5)
- Account Management, i.e., 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” (NIST SP 800-53/AC-2)
- Access Enforcement, i.e., application and monitoring of access privileges (NIST SP 800-53/AC-3)
- Least Privilege; i.e., provision of the minimum tools required for a user to perform his/her function (NIST SP 800-53/AC-6)
- Unsuccessful Login Attempts: i.e., GPSS automatically locks the account until released by a System Administrator when the maximum number of unsuccessful attempt is exceeded . (NIST SP 800-53/AC-7)
- 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 (NIST SP 800-53/AU Family). Audit notifications are generated in response to pre-specified triggers.

The above references auditing measures and technical safeguards are:

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

Consistent with its use of Best Practices to harden its operations, ATR also considers the following additional controls as interfacing with auditing and technical measures:

- Operational Class Controls: Baseline Configuration (CM-2); Configuration Change Control (CM-3); Media Labeling (MP-3); Media Storage (MP-4); Media Transport (MP-5); Media Sanitization

(MP-6); Flaw Remediation (SI-2); Security Training (AT-3).

- Technical Class Controls: Information Flow Enforcement (AC-4); Separation of Duties (AC-5); Supervision-Review/Access Control (AC-13); Information Remnants (SC-4).
- These measures and safeguards are managed through the following Management Class Controls: Certification, Accreditation and Security Assessments (CA-2); Continuous Monitoring (CA-7); Security Categorization (RA-2); Risk Assessment (RA-3); Risk Assessment Update (RA-4); Software Usage Protections (SA-6); Rules of Behavior (PL-4); Privacy Impact Assessment (PL-5).

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 slated for 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.

The following items are considered key in analyzing data integrity, privacy, and security for MIS applications:

- DOJ Order 2640.2E Chapter 8(b) states “Components are encouraged to use products that have been evaluated using the International Standard 15408, Common Criteria for Information Technology Security Evaluation. Accordingly, several MIS products such as the Oracle Application Server 10g and Oracle Database 10g Enterprise Edition are included in the Common Criteria’s List of Evaluated Products. Common Criteria evaluations play a significant factor in the MIS acquisition process.
- The FISMA provision “evaluate private sector information security policies and practices and commercially available information technologies to assess potential application by agencies to strengthen information security” (Section 303 (d)(2)(c)(5)) is applied extensively in MSS activities for best practices examination and in creating risk mitigation solutions. The Antitrust Division is continually looking for improved tools and practices to employ in protecting data in its systems and, upon encountering new technology or methods, implements them in support of maintaining data privacy.
- The DOJ ITIM process is responsible for ensuring that the Systems Development Life Cycle (SDLC) is followed. Systems Security in general, is covered under the DOJ’s Strategic Planning for Information Systems, which precedes the Initiation Phase. The MIS Configuration Management Plan and Systems Engineering Plan utilize the SDLC and related guidance provided in NIST SP 800-64 Security Considerations in the Information System Development Life Cycle for the express purposes of assuring that data integrity, privacy, and security are addressed.

9.3 What design choices were made to enhance privacy?

- MIS has enhanced privacy via the implementation of role-based access controls to protect confidentiality.
- MIS alignment with a dynamic security environment calls for added emphasis on privacy and security, which will be reflected in its Defense-in-Depth strategy and other planned controls cited in this PIA.

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. The proposed Defense-in-Depth implementation will increase the robustness of MIS security services, i.e., access controls, confidentiality, integrity, and non-repudiation.

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. The MIS solution is aligned with supporting all of ATR's security objectives via application of FISMA requirements and industry Best Practices. Management review, continual enhancement, and FISMA-mandated continuous monitoring of MIS technical and procedural controls are of the utmost importance in maintaining application hardening and continuity of 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.

Appendix B: References

E-Government Act of 2002, Public Law 107-347, Section 208(b)
Freedom of Information Act (FOIA) (as amended), 5 U.S.C. 552
Privacy Act (PA) of 1974 (as amended), 5 U.S.C. 552a
Regulations Implementing The Privacy Act of 1974, 36 CFR §1202
Public Availability and Use of Federal Records, 36 CFR §1250
Information related to law enforcement investigations, 36 CFR §1256.58(b)(4)
Standards of Ethical Conduct for Employees of the Executive Branch (5 CFR 2635)
OMB Circular A-II, Preparation, Submission and Execution of the Budget
OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources

OMB Memorandum M-06-19 Reporting Incidents Involving Personally Identifiable Information Incorporating the Cost for Security in Agency Information Technology Investments (12-July-2006)
OMB Memorandum M-06-16 Protection of Sensitive Agency Information (23 June 2006)
OMB Memorandum M-06-15 Safeguarding Personally Identifiable Information (22 May 2006)
OMB Memorandum M-06-02 Improving Public Access to and Dissemination of Government Information and Using the Federal Enterprise Architecture Data Reference Model
OMB Memorandum M-05-15 FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (13 Jun 2005)
OMB Memorandum M-05-08 Designation of Senior Agency Officials for Privacy (11 Feb 2005)
OMB Memorandum M-05-04 Policies for Federal Agency Public Websites (17 Dec 2004)
OMB Memorandum M-04-04 E-Authentication Guidance (16 Dec 2003)
OMB Memorandum M-03-22 Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (26 Sep 2003)
OMB Memorandum M-00-13 Privacy Policies and Data Collection on Federal Web Sites (22 June 2000)
OMB Memorandum M-01-05 Guidance on Inter-Agency Sharing of Personal Data –Protecting Personal Privacy (20 Dec 2000)
OMB Memorandum M-99-18 Privacy Policies on Federal Web Sites (2 June 1999)
OMB Memorandum M-99-05 Instructions on Complying with President's Memorandum of 14 May 1998, "Privacy and Personal Information in Federal Records" (7 Jan 1999)

Information Assurance Technical Framework, Version 3.1, September 2002
Internal Revenue Service's Privacy Impact Assessment; Federal Chief Information Officer's Council Best Practices - Privacy
Federal Enterprise Architecture Security and Privacy Profile Phase 1 Final
Standards of Ethical Conduct for Employees of the Executive Branch (5 CFR 2635)
Letter from John Spotila (Chair, CIO Council Office of Information and Regulatory Affairs) to Roger Baker (CIO, Department of Commerce Co-Chair Security, Privacy, and Critical Infrastructure Committee), on clarification of OMB Cookies Policy (5 Sep 2000)
Letter from Roger Baker (CIO, Department of Commerce Co-Chair Security, Privacy, and Critical Infrastructure Committee) to John Spotila (Chair, CIO Council Office of Information and Regulatory Affairs) on Federal agency use of Web cookies (28 July 2000)

FIPS 201-1 Personal Identity Verification (PIV) of Federal Employees and Contractors
FIPS 200 Minimum Security Requirements for Federal Information and Information Systems
FIPS 199 Standards for Security Categorization of Federal Information and Information Systems

NIST SP 800-92 Guide to Computer Security Log Management (DRAFT)

NIST SP 800-80 Guide for Developing Performance Metrics for Information Security (DRAFT)
NIST SP 800-65 Integrating Security into the Capital Planning and Investment Control Process
NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories
NIST SP 800-55 Security Metrics Guide for Information Technology Systems
NIST SP 800-53 Recommended Security Controls for Federal Information Systems
NIST SP 800-44 Guidelines on Securing Public Web Servers
NIST SP 800-37, Guide to the Security Certification and Accreditation of Federal Information Systems
NIST SP 800-30 Risk Management Guide for Information Technology Systems
NIST SP 800-18 Rev 1 Guide to System Security Plans for Federal Information Systems

DOJ Order 3011.1 Compliance with the Privacy Act
DOJ Order 2880.1B Information Resources Management Program
DOJ Order 2640.2E Information Technology Security
DOJ Order 2640.1 Privacy Act Security Regulations for Systems of Records,
DOJ Privacy Impact Assessment Official Guidance Manual April 2006
DOJ Memorandum issued on 02-May-2006, Personal Information on DOJ Websites
DOJ Memorandum issued on 10-July-2006, Privacy and Safeguarding of Personally Identifiable Information
ATR Directive 2710.4 Safeguarding Sensitive Information 11-July -2006

American National Standard *ANSI INCITS 359-2004* Role Based Access Control document (DRAFT).
Information Systems and Control Association (ISACA) IS Audit Guideline G31-Privacy

Appendix C: Abbreviations and Acronyms

ATR	Antitrust Division
C&A	Certification & Accreditation
DBA	Database Administrator
DOJ	Department of Justice
FEA	Federal Enterprise Architecture
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FTC	Federal Trade Commission
GSS	General Support System
IATF	Information Assurance Technical Framework
ISSG	Information Systems Support Group
JMD	Justice Management Division
MA	Major Application
MIS	Management Information Systems
MSS	Management Support Staff
MTS	Matter Tracking System
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
RBAC	Role-Based Access Control
SBU	Sensitive But Unclassified
SC	Security Category
SDLC	System Development Life Cycle
SORN	System of Records Notification
SP	Special Publication
SSP	System Security Plan
UPI	Unique Project Identifier