

**United States Department of Justice  
Antitrust Division**

---

**General Purpose Support System (GPSS)  
Privacy Impact Assessment**

---

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

**21-JUNE-2007**

**Approval Signature Page**

I recommend approval of the Antitrust Division General Purpose Support System (GPSS) Privacy Impact Assessment:



Cheryl Porpora  
Chief, Office Automation Staff

6-21-07

Date



Carl Anderson  
Chief, Information Systems Support Group

6/21/2007

Date



Thomas King  
Executive Officer, Antitrust Division

6/21/2007

Date

I approve the Antitrust Division General Purpose Support System (GPSS) Privacy Impact Assessment:



Jane Horyath  
Chief Privacy and Civil Liberties Officer

6/22/07

Date

## **Introduction**

The Department of Justice (DOJ) Antitrust Division (ATR) controls and manages a General Purpose Support System (GPSS) that is used to process, store and transmit information. The GPSS is a Sensitive But Unclassified system that supports the Antitrust Division's mission through the establishment, maintenance and delivery of office automation applications to its users.

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 security as a critical factor in the enforcement of antitrust law in both criminal and civil enforcement actions. Continuing enhancement of security safeguards assist the Division in fulfilling its security mandate for a hardened computer infrastructure and secure office automation services.

## **GPSS PIA Framework**

### **Document Compliance**

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

### **Document Organization**

Introduction

GPSS PIA Framework

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

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

Section 3.0 Uses of the System and the Information

Section 4.0 Internal Sharing and Disclosure of Information within the System

Section 5.0 External Sharing and Disclosure

Section 6.0 Notice

Section 7.0 Individual Access and Redress

Section 8.0 Technical Access and Security

Section 9.0 Technology

Conclusion

Appendix A: ATR SORN

### **Document Audience**

This document is intended for public access.

### **Document Change Control**

The GPSS PIA is subject to formal change control procedures and tracking.

## GPSS 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?

- Investigatory information required to carry out the civil and criminal investigatory responsibilities of the Antitrust Division, including documents collected through subpoenas and Civil Investigative Demands under Antitrust Division authorities.
- Contract proposals, which may contain contractor resumes.
- Contact lists, which contain contractor names and telephone numbers.
- Information in Identifiable Form (IIF) from many companies and individuals that are party to antitrust enforcement activities, and from ATR staff as shown below.

<u>Data Type</u>	<u>Data Obtained From</u>
Name	Company, Individual, ATR staff
Social Security Number	ATR staff
Address: Company	Individual, ATR staff
Telephone Number	Company, Individual, ATR staff
E-mail	Company, Individual, ATR staff
Date of Birth	Individual
Travel Records	Company, Individual
Credit Card details	Company, Individual
Criminal History	Company, Individual
Business Classification	Company

### 1.2 From whom is the information collected?

Information is collected from any party to, or target of, ongoing criminal or civil antitrust investigations. Publicly available information also is collected, such as company name, company address, company phone number and email. This information is used to confirm information previously provided by companies and individuals in response to law enforcement requests. Information also is provided by 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 the Antitrust Division's mission, specifically promotion and protection of the competitive process and the United States economy through enforcement of antitrust laws. Although ATR implements all required safeguards for IIF, this information is secondary to the primary information requirements, which focus on economic and market data. For example, the Division may send subpoena to Company A, asking for its records of sales from 2004-2005. The company may respond with invoices that potentially could include a customer's IIF.

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

ATR is authorized to collect information under the provisions of the Sherman Antitrust Act, the Clayton Antitrust Act, and the Hart-Scott-Rodino Act.

### **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.**

The predominant concern is a breach of system privacy safeguards. This breach would occur 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.

To mitigate known risks, the following measures are in place:

- Division staff generally asks that parties providing information to the Division not provide information such as Social Security numbers. Any information received is treated confidentially and only revealed to those who have a need-to-know.
- Various statutes provide criminal penalties to those who mishandle information, and staff is informed of these consequences.
- Contract staff sign confidentiality forms.
- Data is kept in cipher-locked rooms in the case of grand jury data and in secure areas for civil matters. These rooms are located in secure, guarded and/or alarmed office space.

ATR is currently addressing the implementation of additional security controls as mandated in Security Requirements for Federal Information and Information Systems and amplified in Recommended Security Controls for Federal Information Systems. Implementation of these controls is reflected in required system security documentation.

## **Section 3.0 -- Uses of the System and the Information**

### **3.1 Describe all uses of the information.**

The information that GPSS processes, stores and transmits to support the ATR Mission includes the following general categories:

- Administrative Management

- Financial Management
- General Government
- Human Resources
- Information and Technology Management
- Internal Risk Management and Mitigation
- Knowledge Creation and Management
- Legislative Relations
- Litigation and Judicial Activities
- Planning and Resource Allocation
- Public Affairs
- Regulatory Development
- Revenue Collection
- Supply Chain Management

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?

Information collected from subjects of an investigation or witnesses is subjective and requires subsequent validation by investigators to verify its accuracy. Validation is performed through subsequent interviews, searches of other databases, and other law enforcement methods. The Division may demand that parties verify that submissions represent accurate copies of their records. Comparisons are made among industry respondents to provide a verification of the data. Employee information is verified through agency personnel channels.

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)?

Consistent with records retention schedules approved by NARA, official files of the Antitrust Division, including information maintained in the GPSS, are retained at the Federal Records Center for 30 years after the close of the matter and then transferred to the National Archives for permanent retention. The only exception to this disposition is for banking case files that are retained by Federal Records Center for 20 years after the close of a matter and then destroyed. Copies of official documents and other related information of historical value to ATR may be retained in GPSS until they no longer provide a useful reference for subsequent ATR enforcement responsibilities.

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.

Key GPSS controls to assure information is handled in accordance with its prescribed use include:

- Technical 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

ATR is required to address 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 in July 2006. Furthermore, ATR issued ATR Directive 2710.4 Safeguarding Sensitive Information in July 2006 to assure Division compliance. From a technical perspective, continuous monitoring requirements provide assurance that privacy-applicable controls are consistent with GPSS 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 data, as needed and appropriate, as part of the investigative process. Data submitted in conjunction with criminal or civil investigations may be shared as follows:

- Criminal:
  - Federal Bureau of Investigation,
  - United States Attorney Offices
  - Criminal Division
  - Office of the Inspector General
- Civil:
  - United States Attorney Offices
  - Office of the Inspector General

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

- Specific information identified in Section 1.1 may be shared with internal DOJ components with a need to know. Information shared depends on the component's identified need and the nature of the investigation. Determinations of information that may be shared are made by the Division's legal staff, working in consultation with the requesting government organization.
- In some cases, a DOJ component, such as the FBI, may work at an ATR site on ATR matters. In addition, Division staff will at times partner with a local United States Attorneys' Office (USAO) to work on a specific investigation where the USAO has specific industry expertise or knowledge of a particular geographic location in which the Division is conducting an investigation.
- On rare occasions, data received in an ATR investigation may relate to an ongoing Criminal Division investigation and has been shared with that Division. Any data shared is specific to a defined law enforcement need-to-know.

4.3 How is the information transmitted or disclosed?

Information is:

- exchanged via internal e-mail subject to GPSS controls
- exchanged 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 GPSS 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?

To support ongoing antitrust enforcement activities, information may be shared with the following external entities:

Criminal:

- Investigative Agencies
  - Defense Contract Investigatory Services

- Department of Transportation
  - State Attorneys General
  - Outside experts working under contract to ATR on specific matters
- Civil:
- Federal Trade Commission
  - State Attorneys General
  - Industry experts working under contract to ATR on specific matters

## 5.2 What information is shared and for what purpose?

Non-DOJ recipients serve as contract experts in their noted areas and assist in the analysis of the data. State Attorneys General staff may assist with joint investigations and other filings. Evidentiary information such as exhibits, affidavits, etc., which may be based on information produced during discovery, may also be shared by court order and/or local rules of evidence.

## 5.3 How is the information transmitted or disclosed?

Information is hand-delivered to any outside parties or shared over secure computer networks.

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

Data may be shared under court order. Outside experts and others, including individuals at other government agencies, must either sign confidentiality agreements before receiving such data or be allowed such access as part of a legitimate law enforcement activity.

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

All government agencies implement Standards of Ethical Conduct for Employees of the Executive Branch (5 CFR 2635) via Rules of Behavior per OMB Circular A-130, Appendix III.

## 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 a recipient's 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.

Privacy risks in the form of disclosure and modification are mitigated through procedural means such as the use of confidentiality agreements with contract consultants and other outside parties. Some information is subject to protective orders that limit disclosure of information. These orders are case-specific, and may vary based on the parties that are involved. Some information is subject to Federal Rule of Criminal Procedure 6(e), that addresses secrecy in grand jury proceedings.

## 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 Notices 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 groups have access to the ATR General Purpose Support System. Each member of a group has read-write permissions for files within the group. The permissions are implemented technically through Windows Directory Services that enable a shared information infrastructure for locating, managing, administrating, and organizing common items and network resources.

- Users -- The user group has rights to shared data on the ATR GPSS. This group also has access to specific files within each user's section.
- ATR Personnel Staff -- The personnel group has access to ATR personnel data on the ATR GPSS.
- Domain Administrator -- Administrators have full rights to the ATR GPSS.
- Local Administrators -- Local administrators have full rights within their local group.
- ATR Field Office Personnel Staff -- Local Division computer administrators have full rights within their local group.

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?

GPSS users are assigned to group based on their job function.

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

All Antitrust Division users have access to the GPSS. The level of access is determined by each user's job function (attorney, paralegal, HR Specialist, IT Specialist, etc.). Documented Entry On Duty/Exit Standard Operating Procedures are followed to ensure that each user has only the access necessary to perform his/her job.

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

- GPSS manages information system accounts in accordance with applicable DOJ account management policies and procedures. Each user account is specific to a particular user.
- ATR assigns responsibilities to specific parties and specific actions are defined to ensure that information system accounts are managed correctly.
- Information system accounts are managed consistently across the organization.
- GPSS has established procedures for establishing, activating, modifying, disabling, and removing user accounts.
- Procedures are followed in accordance with the Division's System Operating Plan and Windows Directory Services.
- Use of information system access controls is reviewed and supervised by the Operations Manager. Inappropriate access is investigated and documented and reported to the GPSS Information Systems Security Officer.

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

- 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 -- GPSS automatically locks the account until released by a System Administrator when the maximum number of unsuccessful attempts is exceeded.
- System Use Notification -- A user has to acknowledge Department policies regarding use before access is granted.
- Session Lock -- A user has to re-authenticate after a specified period of inactivity.

- Remote access is controlled and monitored. Encryption is used to protect the confidentiality of remote access sessions through the use of secure remote access tokens.
- Audit trails are generated by the GPSS. The audit trails facilitate intrusion detection and are a detective control for identifying data misuse. The GPSS also is configured to protect audit information and tools from unauthorized access, modification and deletion.

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. New employees receive training on the use of the system 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 July 2005.

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 General Purpose Support 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 GPSS, 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 is performed in accordance with DOJ requirements. GPSS 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 on the GPSS. As part of ATR's decision-making process regarding security, it performed a requirements analysis December 7, 2001, under the direction of the DOJ Justice Consolidated Office Network (JCON) 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 GPSS 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 on or processed by ATR computer systems. ATR's standard desktop configuration includes access control features (e.g., inactivity time outs) and ATR's standard network architecture employs auditing controls, requires intrusion detection devices and firewalls on all external connections, and secures router configurations. ATR installs encryption software on laptops to enhance the security of data.

## Conclusion

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

The GPSS security solution helps ensure ATR's security mandate for a hardened infrastructure and secure office automation services. Management review, continual enhancement, and FISMA-mandated continuous monitoring of GPSS technical configuration and procedural controls, are of the utmost importance in maintaining network infrastructure security and continuity of operations.

Access authorization, authentication rules, and audit controls have been configured to implement and monitor need-to-know. These technical controls are supplemented by procedural controls such as Rules of Behavior, Confidentiality Agreements, and Security Awareness and Training to mitigate risks regarding unauthorized access.

**Appendix A: ATR SORN**

<b>SYSTEM</b>	<b>TITLE</b>	<b>DATE PUBLISHED</b>	<b>FEDERAL REGISTER</b>
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.