U.S. DEPARTMENT OF JUSTICE

PRIVACY IMPACT ASSESSMENT FOR THE UNIFIED FINANCIAL MANAGEMENT SYSTEM

Version 1.0

UFMS-D-DOJ-SS-0190

FINAL

August 2008

One System, One Vision

UNIFIED FINANCIAL MANAGEMENT

Contact Point
Phillip Slayden, UFMS Program Security Manager
UFMS Program Management Office
Department of Justice
(202) 514-1984

Reviewing Official
Vance Hitch
Chief Information Officer
Department of Justice
(202) 514-0507

Approving Official
Kenneth Mortensen
Acting Chief Privacy Officer and Civil Liberties Officer
Department of Justice
(202) 353-8878

DOCUMENT CHANGE HISTORY

Version	*Date*	*A, M, D**	*Description of Changes*	*Change Request Number*
1.0	08/01/08	A	Initial Release.	N/A

***A** - ADDED **M** - MODIFIED **D** - DELETED

ACCEPTANCE

Prepared By:

UFMS Security Management Team

Reviewed By:

/s/ **9/15/08**

Phillip Slayden Date
UFMS Program Security Manager

Approved By:

/s/ **9/25/08**

Kenneth Mortensen Date
Acting Chief Privacy Officer and Civil Liberties Officer

TABLE OF CONTENTS

TABLES

INTRODUCTION

The Department of Justice (DOJ) Unified Financial Management System (UFMS) is a financial/procurement management system owned by the DOJ Deputy Assistant Attorney General for Administration (DAAG) / Controller. The UFMS is being implemented to improve the existing and future financial management and procurement operations across DOJ. UFMS is planned to replace six (6) core financial management systems and multiple procurement systems currently operating across DOJ with an integrated Commercial Off-the-Shelf (COTS) solution. UFMS will allow the DOJ to streamline and standardize business processes and procedures across all Components. The system will provide secure, accurate, timely, and useful financial data to financial and program managers across the Department and produce Component and Department-level financial statements. In addition, the system will assist the DOJ by improving financial management performance and aid Department Components in addressing the material weaknesses and non-conformances in internal controls, accounting standards and systems security identified by the DOJ Office of the Inspector General (OIG). Finally, the system will provide procurement functionality to streamline business processes, provide consolidated management information and the capability to meet all mandatory requirements of the Federal Acquisition Regulation (FAR) and the Justice Acquisition Regulations (JAR).

The vision of the UFMS Program is to improve the Department's financial management performance by providing the Components with an enterprise-wide Financial Management System (FMS) and standard processes that enable effective management of financial resources in support of the Department's mission, objectives, and strategic goals. The mission of the UFMS Program is to implement a secure, integrated, and unified financial management system, supported by standard processes and compliant with applicable statutes and regulations. Meeting the UFMS Program Mission will provide:

- Information for managers at all levels to make sound business decisions for their assigned areas of responsibility
- Opportunities for improved efficiency from standardized business practices
- Enhanced system security and financial accountability
- Support to Government-wide financial and procurement management initiatives

This UFMS Privacy Impact Assessment (PIA) adheres to Federal and DOJ guidelines and is performed in accordance with the e-Gov initiative to ensure the security and privacy of Information in Identifiable Form (IIF; also known as Personally Identifiable Information, PII) from or about members of the public. Privacy risks will be assessed throughout the lifecycle of UFMS. The UFMS PIA will be updated, as needed to reflect any changes to the system, business processes, or the collection and handling of information that is individually identifiable within UFMS.

1. THE SYSTEM AND THE INFORMATION COLLECTED AND STORED WITHIN THE SYSTEM

The following questions are intended to define the scope of the information in the system, specifically the nature of the information and the sources from which it is obtained.

1.1 What information is to be collected?

As a financial/procurement management system, UFMS collects information used to reserve, obligate, process, and affect collection or payment of funds (e.g., vouchers, excluding payroll vouchers), invoices, purchase orders, travel advances, and travel/transfer vouchers. In addition, documentation reflecting information about payments due to or made to, claims made by, or debts owed by the individuals covered by this system is also collected. The UFMS comprises information such as fees, fines, penalties, overpayments, and/or other assessments in order to comply with reporting regulations. Individuals covered by this system include Federal government employees and supporting system personnel.

The UFMS processes, stores, and transmits both Federal Employee and business partner information in identifiable form, as defined in OMB Memorandum M-03-22/Attachment A/II.A.2. This memorandum directs the UFMS to conduct reviews of how information about individuals is handled, how information is used when collecting new information, and how the UFMS collects PII. The following is a list of PII data that is transmitted to/from external business partners or stored within the UFMS.

- Address
- E-mail
- First Name
- Last Name
- Telephone Number
- Credit Card Numbers
- Social Security Number (SSN)
- Taxpayer Identification Number (TIN)
- Banking Information (Account number only).

The following table lists PII data that is imported into the UFMS application from external business partners/interfaces.

Table 1. UFMS Inbound PII

UFMS INBOUND PII			
Central Contractor Registration (CCR)	Vendor Record Updates Vendor Master Files.	(i) TIN/SSN (ii) First Name (iii) Last Name (iv) Bank Acct #.	(i-iv) Identification, Vendor Payment & Reporting.
Credit Card (Chase/MasterCard)	Daily Transactions Card Management MasterCard 1099.	(i) TIN/SSN (ii) Credit Card numbers (iii) Cardholder Name (iv) Cardholder Address.	(i) Account query, validation and reporting (ii) Identification (ii-iv) Used to store credit card holder information.

UFMS INBOUND PII			
EXTERNAL AGENCY	**DESCRIPTION**	**PII DATA**	**DATA USE**
National Finance Center (NFC)	NFC Payroll NFC Personnel.	(i) SSN (ii) First Name (iii) Last Name (iv) Bank Acct # (v) Compensation and Benefits.	(i-iii) Identification & Reporting (iv) Identification, Vendor Payment & Reporting (v) Reporting.
Treasury	Master Account File Collections Banking Information (routing number only).	(i) First Name (ii) Last Name (iii) Address (iv) Phone #.	(i-iv) Reporting.

The following table lists PII data that is exported from the UFMS application to external interfaces.

Table 2. UFMS Outbound PII

UFMS OUTBOUND PII			
EXTERNAL AGENCY	**DESCRIPTION**	**PII DATA**	**DATA USE**
Federal Business Opportunities (FedBizOpps)	Announcements Solicitations.	(i) E-mail (ii) First Name (iii) Last Name (iv) Phone #.	(i-iv) Contact Identification.
Federal Procurement Data System – Next Generation (FPDS)	Award and Order Information.	(i) E-mail (ii) First Name (iii) Last Name (iv) Address (v) Phone #.	(i-v) Award Identification.
Internal Revenue Service (IRS)	1099 TIN Verification.	(i) TIN/SSN (ii) Name (iii) Address (iv) Phone #.	(i-iv) Reporting.
Department of the Treasury (Treasury)	Disbursements Voucher and Schedule of Payments Collections Reporting.	(i) E-Mail (ii) Name (iii) Address (iv) Phone # (v) Bank Acct #.	(i-v) Vendor billing/payments and identification.
Department of State (DoS)	Disbursements.	(i) Payee Address (ii) Payee Name (iii) Payee Bank #.	(i-iii) Disbursements.
e-Travel (eTS)	Fund and Travel Transactions.	TBD	(i) Accounting event information (ii) User/Traveler Profile (iii) Dimension and funding data.

TBD = To Be Determined; not yet implemented and/or active

The following table lists the PII data that is internal to the UFMS system. The Vendor Self Service (VSS) portal sits within the UFMS environment at the Justice Data Center - Washington (JDC-W) facility, and as such is an internal source. Commercial vendors can register via VSS to submit quotes/bids against Requests for Quotations (RFQs) and solicitations. Vendors can also login to submit electronic invoices and view the status of payments.

Table 3. UFMS Internal PII

UFMS INTERNAL PII			
EXTERNAL AGENCY	**DESCRIPTION**	**PII DATA**	**DATA USE**
Vendor Self Service (VSS)	Solicitations Offers Awards Invoices Billing Payment Information.	(i) Email (ii) SSN (iii) First Name (iv) Last Name (v) Address.	(i-v) Used for procurement contact information.

1.1.1 General Data Flow

The following describes the external business partners/interfaces and the general information flow to and from the UFMS application.

Central Contractor Registration
The Central Contractor Registration (CCR) is the government-wide repository for vendor information. The agency facilitates the transfer of vendor information from CCR to the UFMS Central Contractor Registration Connector (CCRC) interface. A real-time daily CCRXML sensitive data extract is downloaded, extracted, and updated into the UFMS information system. Refer to Table 1, UFMS Inbound PII, for CCR PII information. Stakeholders involved include Defense Logistics Agency (DLA) as the sending agency, UFMS as the receiving agency, DOJ Component Officers and Procurement Officials as the users.

Credit Card
A banking/credit institution connects with UFMS' Credit Card interface to propagate credit card transaction information and cardholder account data into UFMS. Credit card files are loaded into UFMS for payments to be established and disbursed and for transactions to be reconciled. Three types of data are created: (i) Activity data, which produces a daily file of charges, (ii) 1099 data, which creates a list of aggregate purchases, and (iii) management data, which generates a list of card characteristics and card numbers. In addition to the transaction data, the banking/credit institution distributes credit card account maintenance data. Stakeholders involved include Bank/Credit institution as the sending agency, UFMS as the receiving agency, Credit institution provider (for 1099), Component analysts, and Department analysts.

Department of Treasury
The Department of Treasury (Treasury) interface facilitates DOJ's disbursement of commercial and employee payments, collections, and government-wide financial reporting. Treasury interfaces with UFMS through three functional areas including Payment Disbursement, Collections, and Reporting, and each functional area may import and export data. The Treasury interface consists of bi-directional processes to export payment, collection, and financial reporting information from UFMS as well as import payment confirmation and reporting reconciliation data into UFMS. UFMS exports payment disbursement information in the form of check or Electronic File Transfer (EFT) payment files. UFMS generates and processes collection data for export to Treasury and import into UFMS. UFMS generates financial report files for transmission to Treasury and imports financial reconciliation report files. Stakeholders involved include Department of Treasury and UFMS as both sending and receiving agency, Component Analysts, and Department Analysts.

e-Travel System
The e-Travel (eTS) provider will interface with the UFMS eTS interface and shall import travel data (authorizations, vouchers, and related accounting information) into UFMS. The interfacing agency will supply UFMS with accounting event information related to Federal travel as well as supply the eTS system with agency account code and user/traveler profile data. Data transfer from UFMS to the eTS system will consist of an export of dimension and funding data, and user/traveler profile information (e.g., Traveler Profile, e-Travel User Profile, Travel Planning and Authorization, Reservations and Ticketing, Travel Advances and Delinquent Travel Advances, Travel Vouchers and Claims, Credits and Refunds from Cancellations, Non-Federally Sponsored Travel, Account Code Structure and Workflow, Routing, Notifications and System Messages). Stakeholders involved include eTS as the sending agency, UFMS as the receiving agency, and Federal employees as the users.

Federal Business Opportunities
Federal Business Opportunities (FedBizOps), the government-wide source for procurement opportunities greater than $25,000, is a single point of entry for Federal buyers to publish purchase requirements and for vendors to obtain Federal business opportunity postings. UFMS posts announcements and solicitations to FedBizOps. An outbound connection from UFMS to FedBizOps is established in the form of a system-generated email. Stakeholders involved include UFMS as the sending agency, FedBizOps as the receiving agency, and DOJ Contracting Officers who create solicitations in FedBizOps.

Federal Procurement Data System - Next Generation
Federal Procurement Data System - Next Generation (FPDS), the government-wide central repository for procurement data, interfaces with UFMS in a bi-directional flow that moves award and order information from UFMS to FPDS. UFMS transmits information related to procurement actions. After receipt of this transmission, FPDS provides confirmation back to UFMS acknowledging successful transmission. Stakeholders involved include UFMS and FPDS as both the sending agency and receiving agency and DOJ Contracting Officers who create solicitations in FPDS.

Fixed Asset Systems
Fixed Asset systems (i.e., property management systems) across DOJ provide methods of tracking fixed asset valuation information and include various external Component property management systems and UFMS. Asset acquisition and devaluation information is transferred between UFMS and the fixed asset systems. UFMS will import and update disposition/liquidation and depreciation data from the property management systems. The fixed asset system export file data elements and format have not been determined, but may consist of acquisition cost, date, method, commodity code, contract number, item description, purchase order number, method, quantity, vendor code, and name. The import of data into UFMS will consist of the elements required to update accounts with values such as depreciation amount, liquidation/disposition date and value, and/or transfer of a capitalized asset. Stakeholders involved include custodians and employees managing assets. All stakeholders may not have been identified, as the interface is not currently in operation.

Internal Revenue Service
The UFMS exports compiled 1099 data to the Internal Revenue Service (IRS). UFMS transmits and receives vendor TINs for verification and confirmation with the IRS. UFMS connects to the IRS Filing Information Returns Electronically (FIRE) system and uploads TIN/Employee Identification Number (EIN) and IRS 1099 reporting files. Stakeholders involved include IRS and UFMS as the sending and receiving agency, Component analysts, and Department analysts.

National Finance Center
The National Finance Center (NFC) provides payroll services for the DOJ. NFC centralizes payroll disbursements for the DOJ and exports financial transactions, including employee

demographic data and banking information associated with compensation and benefits, for import into UFMS. UFMS downloads detailed and summarized compensation and benefits data as well as employee demographic and banking data from the NFC. UFMS also imports and stores the detailed compensation data for Component reporting. Stakeholders involved include NFC as the sending agency, UFMS as the receiving agency, Justice Management Division (JMD) Human Resources Systems Analysis Group (HRSAG), DOJ payroll administrators, and UFMS system users.

State Department
The Department of State (DoS) facilitates DOJ's foreign payments and confirmations. UFMS creates foreign payments and exports them DoS for disbursement. DoS exports an electronic confirmation file to both UFMS and the Department of Treasury for payment reconciliation. Stakeholders involved include DoS and UFMS as the sending agency, UFMS as a receiving agency, financial administrators, and dispatch officers.

Third-Party Bank
A Third-Party Bank (TPB) interfaces with UFMS and provides functionality to print and record accounting events associated with payments. Presentment and reconciliation information is exchanged between the bank and UFMS. UFMS will communicate the check and payment amount data with the banking institution. The export of data from UFMS for import into the TPB will consist of check data that was issued, cancelled, replaced, and/or voided the previous day. Exported data will include check numbers, amounts, and dates of checks printed the previous day. The TPB will supply check data (check numbers and amounts for checks cleared at the TPB) for import into UFMS, to include checks cleared the previous day and monthly reconciliation data. Stakeholders involved include TPB and UFMS as both the sending and receiving agency, local bank agents, Component field office personnel, and draft administrators.

Vendor Self Service
Vendor Self Service (VSS) serves as an Internet portal where vendors registered to do business with the U.S. government can log in to view and respond to DOJ procurement actions, submit electronic invoices, and view payment status of those invoices. Commercial vendors can register with VSS in order to submit quotes/bids against government RFQs and solicitations. Vendor registration information is downloaded from the VSS Internet portal and passed into UFMS. DOJ's VSS vendors can submit standalone or referenced invoices through the VSS Internet portal, after which time the invoices are imported into UFMS. VSS procurement functionality includes Solicitations, Offers, Awards, and Orders, which are created in UFMS and responded to through VSS. VSS Accounts Payable and Accounts Receivable functionality includes Invoice, Payment, Billing, and Collection information, which is sent to UFMS for processing. Stakeholders involved include government vendors, UFMS, Component analysts, and Department analysts.

1.2 From whom is the information collected?

UFMS collects procurement and financial information requested through internal Department Components, Office, Boards, and Divisions (OBDs), and from external interfacing partners.

Procurement and financial data, which includes solicitations, offers, awards, and orders, is collected from DOJ Components and OBDs. Components and OBDs are internal to DOJ and include Federal employees and contractor personnel.

External information is obtained from commercial and other Federal agencies. External commercial vendors provide information through VSS to include vendor responses to DOJ procurement actions and invoices for services rendered to DOJ. External interfacing partners include Treasury, which provides employee payment and collection and reporting disbursements, the IRS, which provides payment verification and confirmation, Mellon Bank, a TPB that provides transaction and cardholder account data, the e-Travel system, which provides travel profile data,

DOJ internal Fixed Asset systems, which provide fixed asset valuation information, DoS, which provides foreign payment, TPBs, which provide presentment and reconciliation data, and the NFC, which provides employee compensation and benefit data. For a breakdown of specific PII information collected, please see Table 1 through Table 3.

2. THE PURPOSE OF THE SYSTEM AND THE INFORMATION COLLECTED AND STORED WITHIN THE SYSTEM

The following questions are intended to clearly delineate the purpose for which information is collected in the system.

2.1 Why is the information being collected?

Data, to include PII, is collected to support the overall mission of the UFMS. The Department and Components use biographical information to support operations and accommodate business interaction. UFMS collects employee biographic and banking information for use in transactions including compensation, identification, procurement, reporting, and validation. The collection of PII data is necessary to identify requests, address requests, and provide appropriate responses to the requesting business partners or DOJ Components.

Social Security Numbers are used for Credit Card 1099 reporting, vendor record grouping, ordering, and tracking, and may be used in lieu of the Employer Identification Number (EIN) or TIN. NFC uses SSNs to add new personnel as vendors in UFMS, update existing vendors with changes, and "prevent new spending" for employee vendors that have separated from the Department or transferred to another Component in a different instance. The IRS and VSS may use SSNs for vendor verification and confirmation.

The collection of PII supports coordination among other DOJ Components and interfacing agencies, as described in Section 1.1 of this document.

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

Table 4. Authorities that Authorize the Collection of Information

• 31 U.S.C. § 3512	Describes government responsibilities to ensure effective control over, and accountability for, assets for which the agency is responsible
• 44 U.S.C. § 3101	Describes government responsibilities to make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities.
• Presidents Management Agenda	The UFMS program was initiated in support of a government-wide effort to improve financial performance, as described in the President's Management Agenda. In addition, Chapter III of the U.S. Department of Justice Strategic Plan for FY2003-2008 discusses the importance of enhancing Department-wide financial management and program

performance.

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 identified including the amount, type, and purpose of the information collected pertain to the confidentiality, integrity, and availability of the data. If information collected was inappropriately disclosed to an unauthorized individual (confidentiality), was inaccurate and/or inappropriately modified (integrity), or unavailable when needed (availability), the potential exists for fraudulent activity and/or adverse impact to the DOJ mission, objectives, or reputation. Some examples of potential risks include, but are not limited to, illegal payments and/or procurements; misuse of bank accounts and credit cards; identify theft; over-payment, under-payment or non-payment to legitimate parties; or other illegal acts. In addition, information about sensitive DOJ activities could become exposed, leading to a compromise in mission objectives (to include the success of various investigations and/or operations), or to a negative impact on the reputation of the DOJ to include embarrassment and/or loss of the general public's confidence.

To mitigate these potential risks, the UFMS application and hosting facility has implemented managerial, operational, and technical security controls consistent with DOJ Order 2640.2E (or successor) and associated information technology security standards, which are derived from National Institute of Standards and Technology (NIST) 800-53 *Recommended Security Controls for Federal Information Systems* to mitigate the identified risks.

Examples of managerial controls employed include, but are not limited to, performing certification and accreditation, developing and maintaining an up-to-date and approved system security plan, and performing risk assessments. Operational controls that have been implemented include security training and awareness that cover an individual's security-related responsibilities, development of an incident response capability, media protection policy and procedures development and enforcement, and physical and environmental protections (e.g., guards, access badge security, sign-in logs, and security cameras).

Technical controls employed include implementing access controls (e.g., role-based access controls, account management procedures to include separation of duties, principle of least privilege, need-to-know, timely account disablement/deletion, and annual account recertification), defining, introducing, and enforcing identification and authentication mechanisms; and creating system protections to include of encryption of information at rest and in transit and boundary protection technology and procedures (e.g., network intrusion detection systems, firewall log monitoring, and malware detection and correction software).

To prevent unauthorized data use by agency employees, access control audit log reviews are performed by Operations and Maintenance (O&M) personnel in accordance to DOJ and Federal requirements (e.g., NIST 800-53, DOJ IT Security Standard AU-06 Audit Monitoring, Analysis, and Reporting). All DOJ employees and contractors who have access to privacy information are required by law and by contract to protect personal information in accordance with the Privacy Act and DOJ privacy guidelines. Unauthorized use by a Federal employee is subject to strict penalties. Policies and procedures are in place and/or being developed that cover UFMS user responsibilities (e.g., handling of information and need-to-know).

3. USES OF THE SYSTEM AND THE INFORMATION

The following questions are intended to clearly delineate the intended uses of the information in the system.

3.1 Describe all uses of the information.

DOJ Components use/will use UFMS to process all of their daily financial transactions. The respective finance staffs within each Component are responsible for the Department's accounting programs, which include supporting the process of funds flowing to, from, and within the Department, providing payroll accounting services for all employees of the Department, and supervising the accounting policies, standards, systems, and activities of the Department. DOJ's Procurement Services Staff (PSS) uses UFMS for recording procurement activities related to solicitations and awards, etc.

UFMS records consist of DOJ financial and procurement data, to include all documents used to reserve, obligate, process, and affect collection or payment of funds, invoices, purchase orders, travel advances and travel/transfer vouchers. In addition, UFMS information is used to establish payments due or made, claims, or debts owed by the individuals working for DOJ or doing business with the DOJ. This includes fees, fines, penalties, overpayments, and other assessments. UFMS information is also in compliance with IRS and Treasury reporting regulations.

For more information on UFMS data use, please refer to Attachment D, Department of Justice Accounting Systems, System of Records Notice (SORN) entitled "Accounting Systems for the Department of Justice, DOJ 001," initially published in the Federal Register on June 3, 2004, (69 FR 31406) and updated January 3, 2006 (71 FR 142).

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.)

UFMS does not contain this functionality.

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

UFMS primarily receives data via manual data entry and as input (e.g., downloads) from other IT systems. UFMS implements discretionary access controls to prevent unauthorized access to and/or modification of data by UFMS users and other IT systems, which promotes integrity and accuracy of system data. To support the accuracy of data (e.g., data entry and transaction approvals), the UFMS implements role-based access controls and has a formal account management process that ensures that only authorized individuals are assigned permissions to perform authorized functions. This will minimize the risk of malicious or inadvertent modifications that affect the accuracy of data.

Financial and procurement data is verified and approved for submission into the system by finance and procurement staff managers, consistent with the UFMS workflow approval process. UFMS checks data for accuracy based on system rules and edits, and verifies that data entered in certain fields exists in reference tables. In addition, to support data accuracy, financial management and procurement staff perform regular financial audits as part of their job functions; data integrity checks are performed via workflow structure and syntax and value checks. Audit log review is performed by UFMS support staff in accordance with Federal, DOJ, and UFMS

requirements (e.g., NIST 800-53, DOJ IT Security Standard AU-06 Audit Monitoring, Analysis, and Reporting). On a daily basis, UFMS transactional table logs are reviewed to ensure no noticeable anomalies or erroneous postings exist. Suspicious activity or suspected violations are reported to appropriate UFMS Program staff, and audit records and findings are captured in a monthly report.

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)?

The data retention period for UFMS data is in accordance with the NARA approved General Records Schedule (GRS) for the protection of accounting (6 years), procurement (3 years), personnel (1 year), and electronic data (20 years). The following table describes the GRS data retention schedule for UFMS:

Table 5. Records Retention Schedule

RECORD TYPES	GENERAL RECORDS SCHEDULE	RETENTION SCHEDULE
Accounts Records	6	Destroy 6 years and 3 months after period covered by account
Expenditure Accounting Records	7	▪ Destroy Expenditures Accounting General Correspondence and Subject Files after 2 years. ▪ Destroy General Accounting Ledgers 6 years and 3 months after the close of the fiscal year involved. ▪ Destroy Appropriation Allotment files 6 years and 3 months after the close of the fiscal year involved. ▪ Destroy original Expenditure Accounting Posting and Control Files after 3 years and copies after 2 years.

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.

Data in all forms will be protected in accordance with applicable DOJ and Federal guidance, policies, and directives, based on the sensitivity/classification of the information/system. Access to information is limited to authorized personnel with a requisite background investigation/security clearance, formal authorization, and need-to-know. All UFMS information will be handled (e.g., processed, stored, transmitted, transported, and destroyed) in accordance with relevant Federal and DOJ policies, orders, and standards.

The UFMS Program labels output with the appropriate sensitivity classifications (e.g., Limited Official Use) and is marked in accordance with DOJ policies and procedures. UFMS Components are responsible for labeling/marking and removal of media, as identified under the corresponding service agreements. Labels are adhered to removable information storage media and information system output indicating the distribution limitations, security restrictions, and handling caveats of the information in accordance with DOJ security policy. However, when in transport, the Department's media have no markings or labels that overtly identify parts of any shipment as belonging to the Department.

Media Sanitization is handled in accordance with DOJ policy and procedures. Media is sanitized to include the removal of all labels, markings, and activity logs. Sanitization techniques include degaussing and overwriting memory locations, and that UFMS information is not disclosed to unauthorized individuals when such media is reused or disposed. UFMS sanitizes or destroys information system digital media before its disposal or release for reuse outside the organization to prevent unauthorized individuals from gaining access to and using the information contained on the media.

Record retention is handled in the form of server-based digitized images to which only limited workstations have access; strong passwords control access to the server from these workstations. Printed records and digital media are stored in locked file storage and are protected within secured offices during off-duty hours. UFMS ensures that only authorized users have access to information in printed form or on digital media that is removed from the information system. In addition, servers, workstations, and offices are located in controlled-access buildings. Automated mechanisms such as access card readers are employed to ensure only authorized users have access to the DOJ facility and to the suites where records are stored.

Monitoring and auditing tools are used to review user activity. Audit log reviews are performed by O&M personnel in accordance to DOJ and Federal requirements (e.g., NIST 800-53, DOJ IT Security Standard AU-06 Audit Monitoring, Analysis, and Reporting). Inappropriate access and misuse of information is immediately documented, reported, and investigated accordingly.

The UFMS Program enforces the DOJ Information Technology Security Staff (ITSS) Information Technology Security Council Information Technology Security Employee Services (ISES) Training Plan for UFMS government staff and contractor personnel.

The UFMS Program follows DOJ policy and procedures for sanctions. User non-compliance to security policies and procedures is subject to supervisory disciplinary action up to, and including, immediate termination.

4. INTERNAL SHARING AND DISCLOSURE OF INFORMATION WITHIN THE SYSTEM

The following questions are intended to define the scope of sharing both within DOJ and its Components.

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

The following internal DOJ Component organizations and OBDs use UFMS and share its information:

- Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)
- Drug Enforcement Administration (DEA)
- Federal Bureau of Investigation (FBI)
- Federal Bureau of Prisons (BOP)
- Offices, Boards and Divisions (OBDs)
    - Includes Justice Management Division (JMD)
    - Includes Procurement Services Staff (PSS)
- Office of Justice Programs (OJP)
- United States Marshals Service (USMS).

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

The Department and its Components use UFMS to process all daily financial and procurement transactions. The UFMS information flows top-down, with budgets disseminated from the higher Department level to lower Component levels, and bottom-up, with Components sharing financial reporting information with the Department level for preparation of consolidated reports. The UFMS is developed so that each Component has its own storage area intended to house Component-specific data. Information imported into UFMS is copied to each authorized Component's staging and storage area; all information is processed and maintained from the individual Component's unique set of databases. Within UFMS, Components cannot share unique Component-specific information (including PII). Component personnel cannot view and/or access another Components' financial information within UFMS.

4.3 How is the information transmitted or disclosed?

Internal information is transmitted via encrypted distribution through the Justice Unified Telecommunications Network (JUTNET). PII information is disclosed only to authorized users with the need-to-know via DOJ-managed workstations. Information is disclosed via a secure portal or secure transmission mechanism (e.g., SFTP).

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

From an information technology perspective, privacy risks may result from a breach to the UFMS security posture, which could subsequently compromise the confidentiality, integrity, and availability of information. If a breach were to occur, primarily via unauthorized access to or use of PII information, it would provide an unauthorized individual the opportunity to examine, collect, alter and/or otherwise misuse the information. In addition, if PII data is altered, integrity may be lost, resulting in fraud and abuse.

Internal sharing risks also include unauthorized staff or personnel obtaining the ability to view or modify information within UFMS. Hard and soft-copy media may be misplaced or used inappropriately within the UFMS Program.

Unauthorized physical access to UFMS data within the hosting facility is prevented through the use of guards, access badge security, sign-in logs, and security cameras, as well as via the implementation of policies and procedures that describe access requirements. Unauthorized logical access to the UFMS itself is addressed by network intrusion detection systems, firewall log monitoring, and malware detection and correction software.

Data is protected through compliance with DOJ access control policy, role-based access control for user identification/authentication, assigning and enforcing authorizations, establishing thresholds, applying information flow restrictions, automated system notifications, session termination, applying the principles of least privilege coupled with need-to-know, and using Department-approved encryption technology for data in transit.

The UFMS has established and implemented an account management process to include account justification, requirement of a background investigation and clearance, access restrictions based upon separation of duties and least privilege, strong authenticator management, re-certification efforts, and audit management. In addition, information is secured through strong encryption both in storage and in transit.

5. EXTERNAL SHARING AND DISCLOSURE

The following questions are intended to define the content, scope, and authority for information sharing external to DOJ, which includes foreign, federal, state and local government, and the private sector.

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

UFMS is or will be sharing the information with the following Federal agencies and non-government entities:

Table 6. External Entities with which UFMS will Share Information

NON-DOJ RECIPIENTS	DESCRIPTION
• Department of State (DoS)	DoS facilitates DOJ's foreign payments and confirmations.
• Department of Treasury (Treasury)	Treasury handles payments from and receipt of payments to the Federal government.
• Federal Business Opportunities (FedBizOps)	Owned by the General Services Administration, FedBizOps is a single point of entry for Federal buyers to publish and for vendors to find posted Federal business opportunities across departments and agencies.
• Federal Procurement Data System - Next Generation (FPDS)	Owned by the General Services Administration, FPDS is a government-wide central warehouse for procurement data.
• e-Travel System (eTS)	eTS provides an integrated, end-to-end web-based travel management system that is designed and specifically built for Federal travelers. (This system has not been implemented).
• Internal Revenue Service (IRS)	The IRS handles taxpayer reporting information and files information returns electronically that are exported from UFMS.
• Third-Party Bank (TPB)	TPB provides payment, presentment, and reconciliation processes for DOJ (and currently includes Mellon Bank, which is owned by Chase Bank).

5.2 What information is shared and for what purpose?

As a Department-wide financial/procurement management system, UFMS may require the following information be shared in order to process financial transactions and procurement operations:

- E-mail address and business address of contracting offices

- Name and address of awardees
- Names and phone numbers of officials established as contacts for the purpose of providing announcement information for Federal business opportunities
- Department payment/debt collection data, which is used for ongoing payroll transactions, payment collection/disbursement, and IRS reporting purposes, and includes name, address, banking information, credit card number, and social security number.

For detailed external PII sharing and the data elements shared, please refer to Table 1 through Table 3 in Section 1.1 of this document.

5.3 How is the information transmitted or disclosed?

Information shared with external organizations is transmitted via secure (encrypted) interconnection.

Only authorized users access the system via DOJ authorized workstations through controlled access points. UFMS data is not accessible to the public. The mode of transmission or disclosure is described in a Memorandum of Understanding (MOU) and/or Interconnectivity Security Agreement (ISA) and is written in accordance with DOJ security policies and approved by the UFMS Program Security Manager. In addition, all external systems must meet at minimum the same security requirements as UFMS and /or provide documentation of current acceptable IT security compliance.

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

MOUs and/or ISAs are written in accordance with DOJ security policies and approved by the UFMS Program Security Manager or designated representative for all UFMS external connections to ensure the protection and privacy of data. ISAs have been developed to cover the expectations of data protection once shared. In addition, all external systems must meet at minimum the same security requirements as UFMS and provide documentation of current acceptable IT security compliance.

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

Training is required and provided to Components prior to implementation. Any Federal agency receiving UFMS data is required to handle it in accordance with the Privacy Act and their applicable System of Records Notices (SORNs). In addition, Federal agencies and their contractors are subject to information security requirements of the Federal Information Security Management Act (FISMA), Title III if the E-Government Act, Pub. L. 107-347.

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

Provisions in place for auditing use of information are delineated within an ISA. The ISAs are developed for external business partners.

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

Privacy risks include inappropriate disclosure of sensitive information to include unauthorized individuals within a UFMS external business partner's organization who do not have a need-to-know as well as unauthorized disclosure in the transmission/exchange of information. Privacy risks are mitigated through the implementation of mechanisms that are described in data sharing

agreements such as MOUs and/or ISAs, which describe how each Component must address information exchange security, trusted behavior expectations, incident reporting, auditing, and security parameters of both the UFMS Program and external business partner.

6. NOTICE

The following questions are directed at notice to the individual of the scope of information collected, the opportunity to consent to uses of said information, and the opportunity to decline to provide information.

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 publication of this PIA and the SORN provides public notice of the collection, use, and maintenance of UFMS information to include PII. A SORN for DOJ accounting systems, to include the UFMS, has been published in the Federal register under 69 FR 31406, DOJ-001, Accounting Systems for the DOJ, in June 2004, and later modified in December 2005. A copy of this SORN is found in Appendix D. Each external business partner is responsible for notifying its personnel of appropriate data collection and use in accordance with the Privacy Act and Trade Secrets Act (18 U.S. Code 1905), the Unauthorized Access Act (18 U.S. Code 2701 and 2710), OMB Policy on Protecting PII, and local policies and directives.

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

UFMS Federal employees and business partners have the right to decline information; however, neither may be supported by the financial processes envisioned by the UFMS application. Those who do not wish to provide all of the information requested may delay or prevent processing, response, or resolution. The UFMS does not accommodate users who opt to decline from external systems providing information for import into UFMS.

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?

Federal employees do have the opportunity to consent to particular uses of information. The UFMS displays an approved system use notification message before granting system access. The system use notification message provides appropriate privacy and security notices (based on DOJ privacy and security policies) and remains on the screen until the user takes explicit action to log onto the information system. Individuals providing information indirectly to the UFMS via a business partner portal must consent to the website's local policy. The UFMS is not responsible for systems outside of its control.

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

Privacy risks identified include the failure of UFMS system users to be notified of the type of information that may be collected and Department or external agency use of that information.

DOJ has published a SORN for DOJ's accounting records. The information in this notice includes situations when DOJ may share accounting records. This notice therefore mitigates the risk of a system user not knowing why information is being collected or how the information may be used. In addition, a Department approved system use notification message is provided, which a Federal

employee must agree to before consenting to a third party's particular use of information. Only minimum information necessary to identify the individual is required for processing.

7. INDIVIDUAL ACCESS AND REDRESS

The following questions concern an individual's ability to ensure the accuracy of the information collected about him/her.

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

Individuals can seek access and redress of their information by contacting the DOJ Component from which the information originated using a Privacy Act access or amendment request. UFMS is not responsible for external business partners that export information for import into the UFMS. These collecting organizations or business partners are responsible for providing their own access and redress procedures. If imported UFMS information is identified as incorrect, UFMS users may address this information under the Contesting Record Procedures section of the SORN.

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

Notification procedures for an individual's access and amendment rights can be found under the Privacy Act of 1974 (5 U.S.C. § 552a, section d; Access to Records). Information is found via the SORN and in Departmental regulations (e.g., 28 C.F.R. §§ 16.41, .46), which describe the procedures for making access/amendment requests. Future changes in access and amendment policy and procedures will be reflected in succeeding versions of the UFMS PIA.

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

This is not applicable. There is an opportunity to seek access and redress of personal information under the Privacy Act.

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.

Individuals who wish to contest information contained in the UFMS or actions taken as a result of Department, Component or OBD reliance of the information within the system, may refer to the Privacy Act of 1974, civil remedies section G1.

8. TECHNICAL ACCESS AND SECURITY

The following questions are intended to describe technical safeguards and security measures.

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

All users who access UFMS with either general or privileged permissions obtain accounts and are assigned to roles (e.g., receive permissions) in accordance with the *UFMS Account Management Plan*, which provides guidelines around account management including guidance around roles, separation of duties, and least privilege.

General and privileged users include Component account administrators, Component account administrators, Component security administrators, Component security team, JMD O&M team, tier 1-3 help desk, and finance and procurement staff.

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.

UFMS has five (5) contracts that include Booz | Allen | Hamilton and Diamond Management & Technology Consulting for Program Support, SRA International for IV&V Services, and IBM for Integration and Implementation. Per the language included in the contracts and updated SORN, the contractors will have access to sensitive (otherwise known as "Limited Official Use"), non-sensitive materials, and classified materials. Each Component may have contractors who access the UFMS; these Components maintain individual contracts with third parties.

UFMS and its Component contractors have access to the UFMS system in the capacities referenced in Section 9.1 of this document, including the following roles:

- Component Account Administrators
- Component Security Administrators
- Component Security Team
- JMD O&M Team
- Tier 1-3 Help Desk
- Finance/Procurement Staffs.

Contractors may perform financial and procurement job duties for UFMS Components. Contract documents are available for review, but are not attached; contracts may be requested by contacting the UFMS Program.

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

The UFMS application provides access to data via Role Based Access Controls (RBAC). This functionality is built into the system and configured to the specific needs of the DOJ. RBAC is utilized by assigning various users to predefined security organizations (or groups). These predefined user groups default usage to that of least privilege and need to know.

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

Procedures are documented in the *UFMS System Security Plan* (SSP) and *UFMS Account Management Plan* (AMP). The UFMS SSP includes details regarding account management, in accordance with DOJ Order 2640.2E (or successor), Information Technology Security. In accordance with the AMP, the UFMS Program or individual Components are responsible for

requests/approvals, creation, modification, disablement/deletion, and re-certification of UFMS accounts. The AMP also describes procedures for disabling inactive accounts and waivers for separation of duties conflicts. All UFMS accounts are managed in accordance with defined guiding principles to include appropriate implementation/validation of separation of duties, least-privilege, need to know, requisite background investigation/security clearance, signed rules of behavior, etc.

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

UFMS users are granted system access based upon their organizational roles and the need to know. Files accessed are audited periodically to ensure data maintained by UFMS is protected. Auditing these files ensure that no noticeable anomalies or erroneous postings exist. Due to the complexity of the UFMS system, auditing is performed based on the needs of the Program. All requests to establish new accounts or modify the privileges of an existing account are approved by an Approving Official. Rights and privileges required for the completion of duties associated with defined roles are documented and retained by the Program or Component.

The UFMS Program Security Manager maintains oversight for assigning privileges to accounts in accordance with policy, and documents actions necessary when accounts are not maintained in compliance with policy. Each Component will review its own accounts and perform annual recertification and validation of user roles.

The UFMS Program enforces the review of audit records for indications of inappropriate or unusual activity. The assignment of roles and rules are verified via the implementation of industry recommended Access and Audit and Accountability family of controls.

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

UFMS auditing processes implement auditing measures and technical safeguards in accordance with DOJ and Federal requirements established to prevent unauthorized disclosure and subsequent potential misuse of data. These procedures include:

- Implementing System Access and Password Management and Monitoring (auditing of account creation, password activation/disabling and/or modification, access date/time, object, and other event relevant information in accordance with NIST SP 800-53, AU-3, Content of Audit Records)
- Continuous Monitoring - automated mechanisms are used to integrate audit monitoring, analysis, and reporting for response to suspicious activities. Audit records will be maintained for suspicious activity or suspected violations and will be investigated and immediately reported to the proper Department and UFMS Program management for further action. (This implementation is in accordance with NIST SP 800-53, AU-6, Audit Monitoring, Analysis, and Reporting)
- Audit Reduction - UFMS utilizes an audit log reduction, review, and reporting that provides audit reduction and report generation capabilities.

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

Annual security training and awareness is provided in accordance with DOJ and Federal policies. DOJ ITSS and UFMS provide rules of behavior (ROB) to all information system users (contractor and government) that describe user responsibilities and expected behavior with regard to information system usage. The user acknowledgement indicates the user has read, understands, and agrees to abide by the ROB. The ROB is signed by the user prior to initial authorization to access Component networks and UFMS systems.

All DOJ Components that use the web-based DOJ enterprise Computer Security Awareness Training (CSAT) course include information on the handling and processing of sensitive data (including PII). Tracking is accomplished by the DOJ Learning Management System (LMS). All persons with access to any Component network, regardless of employment status, are required to complete the CSAT course.

Components are responsible for managing their own training and access revocation for non-compliant personnel.

Components that do not employ CSAT use similar web-based IT security awareness courses, each with its own LMS, which have been reviewed to validate these Components and provide information on required topics, including PII. The Bureau of Prisons (BOP) uses a BOP-wide standard instructor-led IT security awareness course that uses the CSAT program as its basis.

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

UFMS has implemented security controls to protect the data in accordance with the DOJ and FISMA requirements as recorded in the Department's C&A tool. A C&A was completed in October 2007 and the UFMS received an Authorization to Operate (ATO) from the Authorizing Official.

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

Privacy risks for access and security controls include unauthorized disclosure and modification of PII data. UFMS mitigates unauthorized disclosure risks through establishing appropriate roles for users, implementing strong encryption for data both in storage and in transit, establishing strong authentication mechanisms, executing an annual re-certification, and implementing audit mechanisms.

Controls are validated throughout the C&A lifecycle and as risks are identified; they are mitigated via Plans of Actions and Milestones. In general, UFMS information is protected by management, technical, and operational safeguards appropriate to the sensitivity of the information. Users are properly trained in safeguarding identifying information stored within and/or processed by UFMS.

9. TECHNOLOGY

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, radio frequency identification (RFID), biometrics, and other technology.

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

In May 2003, the UFMS Program underwent an extensive multi-year procurement and selection process to select the final product to be used for the Department-wide solution. Competing technologies were evaluated prior to the selection of the UFMS solution. Criteria for selection were based upon functionality, security, and interoperability concerns that would allow for UFMS to achieve its mission requirements. UFMS was selected to better support mission and business results by providing a more centralized organizational structure to manage risk, communications, system configuration, security, and governance. The functional enhancements provided by the UFMS application decrease internal control weaknesses identified in legacy systems by DOJ auditors.

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

Security and privacy requirements were analyzed based on FIPS-199 security categorization. FIPS-199 categorizes a system as High, Medium, or Low, depending on how important the function is to the agency. The result of that analysis was that the system was rated HIGH for data confidentiality, integrity, and availability. All security controls are applied in accordance with this rating.

Requirements regarding integrity, privacy, and security were assessed throughout the system development lifecycle to include tasks such as the product selection and acceptance testing, system categorization, risk assessment, requirements analysis, security testing and evaluation, and independent certification, as well as tasks that have developed and described the system architecture and configuration(s). The Program's security team has been involved with each of these tasks and has taken the necessary steps to ensure that the UFMS is progressing through the lifecycle in compliance with applicable Federal and DOJ security policies in these areas. Furthermore, the security team ensures that the C&A lifecycle progresses parallel to the UFMS system development lifecycle to ensure that integrity, privacy, and security are analyzed and continuously monitored.

9.3 What design choices were made to enhance privacy?

The UFMS architecture design choices, which included enhanced privacy, were made in part on the ability of the information system to conform to required security standards of the Department. Further, these design choices included compliance with DOJ Order 2640.2E, 2640.1 (or successor), and the associated IT Security Standards in the areas of identification, authentication, integrity, and monitoring.

The UFMS limits its data collection to specific elements necessary to achieve its mission. The Program provides UFMS government staff and assigned contractor personnel mandated privacy training on the use and disclosure of personal data. UFMS has developed and implemented procedures and policies to ensure that no unauthorized access to records occurs and that operational safeguards are firmly in place to prevent system abuse.

UFMS considered the risks to the system and the sensitivity of the data as a basis for selecting security safeguards to provide adequate system protection. The system provides the capability to

securely authenticate users before allowing access to system resources, implements 140-2 compliant encryption, disables inactive sessions within a specified time period, and provides the capability to audit system activity and marks records. During system identification and authentication, the authenticator field is masked with asterisks. The system masks SSNs when initially used as the vendor identifier and generates an additional unique identifier for personnel within the system.

These design choices listed above limit access to personal information, thereby reducing possible privacy risks associated with the Program.

10. CONCLUSION

The UFMS stores and transmits PII that is used for financial and procurement identification and reporting; however, privacy risks associated with UFMS and its management of this data are minimal. The DOJ has developed a comprehensive security program employing management, operational, and technical security controls to effectively secure the UFMS and mitigate associated risks for the Program. The UFMS maintains a high-level of privacy protection and security commensurate with both Department and industry standards.

APPENDIX A – ACRONYMS

This section includes Program acronyms related to the UFMS PIA.

Acronym	Definition
AMP	UFMS Account Management Plan
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
ATO	Authority To Operate
BOP	Bureau of Prisons
CCR	Central Contractor Registration
CCRC	Central Contractor Registration Connector
CFO*	Chief Financial Officer
CIO*	Chief Information Officer
COTS	Commercial-Off-the-Shelf
CSAT	Computer Security Awareness Training
DCFO*	Deputy Chief Financial Officer
DEA	Drug Enforcement Administration
DIRB*	Department Investment Review Board
DLA	Defense Logistics Agency
DOJ	U.S. Department of Justice
DoS	U.S. Department of State
EFT	Electronic Funds Transfer
EIN	Employee Identification Number
eTS	eTravel System
FBI	Federal Bureau of Investigation
FedBizOpps	Federal Business Opportunities
FIRE	Filing Information Returns Electronically
FISMA	Federal Information Security Management Act of 2002 P.L. 107-347
FMS	Financial Management System
FPDS	Federal Procurement Data System
GRS	General Records Schedule
HRSAG	Human Resources Systems Analysis Group
I&I	Integration and Implementation
IIF	Information in Identifiable Form
IRS	Internal Revenue Service
ISA	Interconnectivity Security Agreement
ISES	Information Security Employee Services
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
ITSS	Information Technology Security Staff
JDC-W	Justice Data Center – Washington
JMD	Justice Management Division
JUTNET	Justice Unified Telecommunications Network
LMS	Learning Management System
MOU	Memorandum of Understanding
NARA	National Archives and Records Administration
NFC	National Finance Center
NIST	National Institute of Standards and Technology
O&M	Operations and Maintenance
OBD	Office, Boards, and Divisions
OJP	Office of Justice Programs
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information

PMO	Program Management Office
PSS	Procurement Services Staff
RBAC	Rules Based Access Controls
RFID	Radio Frequency Identification
RFQ	Request for Quotation
ROB	Rules of Behavior
SORN	Systems of Record Notice
SSN	Social Security Number
SSP	System Security Plan
TPB	Third-Party Bank
TIN	Taxpayer Identification Number
Treasury	U. S. Department of the Treasury
USDA	U.S. Department of Agriculture
UFMS	Unified Financial Management System
USMS	U.S. Marshals Service
VSS	Vendor Self-Service

* Acronyms that appear with an asterisk have not been spelled out in the body of the document.

APPENDIX B – TERMS AND DEFINITIONS

Each document must adapt to present the relevant terms and definitions required. The Terms and Definitions currently included in this template are required for all documents.

TERMS	DEFINITIONS
I&I Team	Under the direction of the UFMS PMO and UFMS Component PMO, as appropriate, the group responsible for the implementation of UFMS. Responsible for meeting the functional and technical requirements specified for UFMS, including integration and installation of Momentum Financials and integrated procurement. The UFMS PMO provides the I&I Team direction and guidance on the continued development of UFMS Foundation Build and other management issues. The UFMS Component PMOs provide direction and guidance on Component-specific issues.
Stakeholder	Individuals or groups who are affected by or who are capable of influencing the UFMS Program.
UFMS Component PMO	Group responsible for supporting the implementation, integration, and deployment phases of the UFMS Program at the Component level. The UFMS Component PMO provides guidance and oversight within the specific Component, and directs the efforts of the I&I Team within established parameters, and consistent with the UFMS foundation.
UFMS PMO Team	Group responsible for the management of the acquisition and implementation of a unified core COTS financial management and procurement system for DOJ. This group includes UFMS PMO government staff, UFMS PMO contractor support, and the I&I Team. The UFMS PMO provides overall program management, guidance, and direction; integrates and implements UFMS; and serves as the central coordination point for all program activities.
UFMS Program Team	Groups that make up the UFMS organization, including DOJ leadership (e.g., CFO, CIO, DCFO, DIRB, etc.), UFMS PMO, UFMS Component PMO, UFMS I&I Team. Also may refer to the overall UFMS deployment phases, management activities, and processes.

APPENDIX C – REFERENCE DOCUMENTS

Each document must adapt to present the relevant references and standard references required. The Program Office Charter and Program Management Plan are required for all documents. A Master Bibliography is available on the Portal in the folder labeled "Style Resources."

Unified Financial Management System:

Program Governance Plan, Version 1.0, UFMS-D-0069, February 2006.

Program Office Charter and Program Management Plan, Version 2.0, UFMS-D-0001, September 2004.

APPENDIX D – DEPARTMENT OF JUSTICE ACCOUNTING SYSTEMS SYSTEM OF RECORDS NOTICE

06/18/2007 16:42 FAX 202 307 1853 DOJ-JMD MPS 002/006

DEPARTMENT OF JUSTICE

[AAG/A Order No. 008–2004]

Privacy Act of 1974; System of Records

Pursuant to the provisions of the Privacy Act of 1974 (5 U.S.C. 552a), notice is given that the Department of Justice proposes to modify a Department-wide system of records entitled "Accounting Systems for the Department of Justice (DOJ), DOJ–001." This system of records was last published on May 28, 1999 at 64 FR 29069. Modifications include: a new method of storage and safeguards; updated and simplified routine uses; removal of the Immigration and Naturalization Service from the components covered, as INS is no longer part of DOJ; and addition of the Bureau of Alcohol, Tobacco, Firearms and Explosives, which joined the DOJ on January 24, 2003.

In accordance with 5 U.S.C. 552a(e)(4) and (11), the public is given a 30-day period in which to comment on this notice; and the Office of Management and Budget (OMB), which has oversight responsibility under the Act, requires a 40-day period in which to conclude its review of the system. Therefore, please submit any comments by July 13, 2004. The public, OMB, and the Congress are invited to submit any comments to Mary E. Cahill, Management and Planning Staff, Justice Management Division, Department of Justice, Washington, DC 20530 (Room 1400, National Place Building).

In accordance with 5 U.S.C. 552a(r), the Department has provided a report to OMB and the Congress.

Dated: May 25, 2004.

Paul R. Corts,

Assistant Attorney General for Administration.

DEPARTMENT OF JUSTICE—001

SYSTEM NAME: DOJ-001

Accounting Systems for the Department of Justice (DOJ).

SECURITY CLASSIFICATION:

Not classified.

SYSTEM LOCATIONS:

Justice Management Division, 950 Pennsylvania Ave., NW., Washington, DC 20530 [Internet Web site: *www.usdoj.gov*]; Central Offices of the Bureau of Prisons (BOP) at 320 1st St., NW., Washington, DC 20534 and Federal Prison Industries (FPI) at 400 1st St., NW., Washington, DC 20534 [Internet Web site: *www.UNICOR.Gov*]; and at any BOP/FPI Regional Offices and/or any of the BOP/FPI facilities at addresses provided in 28 CFR part 503 [and at the BOP Internet Web site: *www.bop.gov*]; Headquarters of the Drug Enforcement Administration (DEA), Office of Finance, 700 Army Navy Drive, Arlington, VA., 22202; and at DEA field offices listed as detailed in DEA–999 [and at the DEA Internet Web site: *www.dea.gov*]; Federal Bureau of Investigation (FBI) Headquarters at 935 Pennsylvania Ave., NW., Washington, DC 20535; and at FBI field offices as detailed in Justice/FBI–999 [and at the FBI Internet Web site: *www.fbi.gov*]; Office of Justice Programs (OJP), 810 7th Street, NW., Washington, DC 20531 [Internet Web site: *www.ojp.gov*]; U.S. Marshals Service (USMS), CS–3, 11th Floor, Washington, DC 20530–1000; and at 94 district offices of the USMS [listed at the USMS Internet Web site: *www.usms.gov*]; Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), 650 Massachusetts Ave., NW., Washington, DC 20226 and at field offices [listed at the ATF Internet Web site: *www.atf.gov*].

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals/persons (including DOJ employees; and including current and former inmates under the custody of the Attorney General) who are in a relationship, or who seek a relationship, with the DOJ or component thereof—a relationship that may give rise to an accounts receivable, an accounts payable, or to similar accounts such as those resulting from a grantee/grantor relationship. Included may be:

(a) Those for whom vouchers (except payroll vouchers for DOJ employees) are submitted to DOJ requesting payment for goods or services rendered including vendors, contractors, experts, witnesses, court reporters, travelers, and employees;

(b) Those to whom the DOJ is indebted or who may have a claim against the DOJ, including those named in (a) above;

(c) Those who are indebted to DOJ, *e.g.*, those receiving goods, services, or benefits from DOJ; those who are liable for damage to Government property; those indebted for travel/transfer advances and overpayments; and those owing administrative fees and/or assessments; and

(d) Those who apply for DOJ benefits, funds, and grants.

CATEGORIES OF RECORDS IN THE SYSTEM:

All documents used to reserve, obligate, process, and effect collection or payment of funds, *e.g.*, vouchers (excluding payroll vouchers), invoices; purchase orders; travel advances, travel/transfer vouchers and other such documentation reflecting information about payments due to or made to; claims made by, or debts owed by the individuals covered by this system, including fees, fines, penalties, overpayments, and/or other assessments, and to comply with reporting regulations of the Internal Revenue Service of the Department of Treasury.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

31 U.S.C. 3512; 44 U.S.C. 3101.

PURPOSE OF THE SYSTEM:

This system of records is used by DOJ officials to maintain information adequate to ensure the financial accountability of the individuals covered by this system; provide an accounting and reporting of DOJ financial activities; meet both internal and external audit and reporting requirements; maintain an accounts receivable and accounts payable; and otherwise administer these and any other related financial and accounting responsibilities.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

DOJ may disclose relevant information as follows:

(1) To the Secretary of the Treasury to effect disbursement of authorized payments.

(2) To any Federal agency or to any individual or organization for the purpose of performing audit or oversight operations of the DOJ and to meet related reporting requirements.

(3) To appropriate officials and employees of a Federal agency or entity which requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract, or the issuance of a grant or benefit.

(4) To Federal, State, local, tribal, foreign, or international licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.

(5) Where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate Federal, State, local, foreign, or tribal, law enforcement

authority or other appropriate agency charged with the responsibility of investigating or prosecuting such a violation or enforcing or implementing such law.

(6) To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion on such matters as settlement, plea bargaining, or in informal discovery proceedings.

(7) In an appropriate proceeding before a court, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator holds the records to be relevant to the proceeding.

(8) To the news media and the public pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

(9) To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

(10) To the National Archives and Records Administration in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

(11) To any Federal, State, or local agency, or tribal authority, which has a financial or other legitimate need for the information to perform official duties; or, similarly, to obtain information which would enable the Department to perform its official duties. Examples include: to permit such agency to perform accounting functions or to report to the Department of the Treasury regarding the status of a Federal employee/contractor debt owed to such Federal, State, or local agency, or tribal authority; to report on the status of Department efforts to collect such debt; to obtain information necessary to identify a Federal employee/contractor indebted to such agency; to provide information regarding the location of such debtor; or to obtain information which would permit the Department to confirm a debt and/or offset a payment otherwise due a Federal employee/contractor after any appropriate due process steps have been taken.

(12) To any Federal, State, local, or foreign agency, or tribal authority, or to any individual or organization, if there is reason to believe that such agency, authority, individual, or organization possesses information relating to a debt, the identity or location of the debtor, the debtor's ability to pay; or relating to any other matter which is relevant and necessary to the settlement, effective litigation and enforced collection of a debt; or relating to the civil action, trial or hearing concerning the collection of such debt; and if the disclosure is reasonably necessary to elicit such information and/or obtain cooperation of a witness or agency;

(13) To the U.S. Department of the Treasury, the U.S. Department of Defense, the U.S. Postal Service, or other disbursing agencies, in order to effect administrative, salary, or tax refund offset against Federal payments to collect a delinquent claim or debt owed the United States, or a State; to satisfy a delinquent child support debt; or to effect other actions required or permitted by law to collect such debt.

(14) To the U.S. Department of the Treasury any information regarding adjustments to delinquent debts, such as voluntary payments which decrease the debt, changes in the debt status resulting from bankruptcy, any increase in the debt, or any decrease in the debt resulting from changes in agency statutory requirements.

(15) To employers to effect salary or administrative offset to satisfy a debt owed the United States by the debtor or, when other collection efforts have failed, to the Internal Revenue Service (IRS) to effect an offset against Federal income tax refund due.

(16) To employers to institute administrative wage garnishments to recover debts owed the United States.

(17) To debt collection centers designated by the U.S. Department of the Treasury (or to a person with whom the DOJ has entered into a contract) to locate or recover assets of the DOJ; or for sale of a debt; or to otherwise recover indebtedness owed.

(18) In accordance with regulations issued by the Secretary of the Treasury to implement the Debt Collection Improvement Act of 1996, to publish or otherwise publicly disseminate information regarding the identity of the person and the existence of a non-tax debt in order to direct actions under the law toward delinquent debtors that have assets or income sufficient to pay their delinquent non-tax debts, but only upon taking reasonable steps to ensure the accuracy of the identity of a debtor; upon ensuring that such debtor has had an opportunity to verify, contest, and compromise a non-tax debt; and with the review of the Secretary of Treasury.

(19) To the IRS for reporting a discharged debt as potential taxable income.

(20) To the IRS to obtain taxpayer mailing addresses for debt collection use. These taxpayer mailing addresses may be disclosed

(a) To private collection contractors to locate a taxpayer and to collect or compromise a claim against, or debt of, the taxpayer, and

(b) To consumer or commercial reporting agencies to obtain a credit report.

(21) To the Department of Health and Human Services, and the Department of Labor, for computer matching in order to obtain names (including names of employees), name controls, names of employers, Taxpayer Identification Numbers, addresses (including addresses of employers) and dates of birth for the purpose of verifying identities in order to pursue the collection of debts.

(22) To other Federal or State agencies as required by law.

(23) To a consumer or commercial reporting agency in accordance with the Debt Collection Improvement Act of 1996.

(24) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records.

(25) To a person or to an entity (*e.g.*, the U. S. Department of the Treasury and/or a consumer or commercial reporting agency), Taxpayer Identification Numbers (TIN's), to report on delinquent debt and/or to pursue the collection of debt, or where otherwise necessary or required, *e.g.*, U. S. Department of the Treasury for disbursement of payments authorized—provided such disclosure is not otherwise prohibited by Section 6103 of the Internal Revenue Code, or other law.

(26) The Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of: Responding to an official inquiry by a Federal, State, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

Only as noted in Routine Use 23 above.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Magnetic disks, magnetic tapes, microfiche, microfilm, file folders, and digitized images, or any other media.

RETRIEVABILITY:

Document number, name, taxpayer identification number, digital identifiers, batch, or other identifiers.

SAFEGUARDS:

Access is limited to DOJ personnel with a need to know. Access to computerized information is generally controlled by passwords, or similar safeguard, which are issued only to authorized personnel. Records are retained in the form of digitized images on a server to which limited workstations have access. Access to the server from these workstations is controlled by passwords. Server and workstations are located in controlled-access buildings. Paper records, and some computerized media, are kept in locked files of locked offices during off duty hours. In addition, offices are located in controlled-access buildings.

RETENTION AND DISPOSAL:

Records are retained and disposed of in accordance with General Records Schedules 6 and 7.

SYSTEM MANAGER(S) AND ADDRESSES:

Director, Finance Staff, Justice Management Division (JMD), U.S. Department of Justice, 950 Pennsylvania Ave., NW., Washington, DC 20530.

Director, Federal Bureau of Prisons (BOP), 320 First St., NW., Washington, DC 20534. [The Director, BOP, is also system manager for Federal Prison Industries (FPI).]

Chief Financial Officer, Financial Management Division, Drug Enforcement Administration (DEA), 700 Army Navy Drive, Arlington, VA 22202.

Director, Federal Bureau of Investigation (FBI), 935 Pennsylvania Ave., NW., Washington, DC 20535.

Director, Accounting Division, Office of Justice Programs (OJP), 810 7th Street, NW., Washington, DC 20531.

Chief, Finance Staff, Management and Budget Division, U.S. Marshals Service, CS–3, 11th Floor, Washington, DC 20530–1000.

Office of Management/Chief Financial Officer, Bureau of Alcohol, Tobacco, Firearms and Explosives, 650 Massachusetts Ave., NW., Washington, DC 20226.

NOTIFICATION PROCEDURES:

Same as RECORD ACCESS PROCEDURES.

RECORD ACCESS PROCEDURES:

Request for access to records in this system must be in writing and should be addressed as follows:

JMD: For records of the Offices, Boards and Divisions, address requests to the system manager named above for JMD.

OJP: Address request to the system manager named above.

BOP: Address requests to the Assistant Director, Administration Division, 320 First Street, NW., Washington, DC 20534.

FPI: Address requests to Assistant Director, Federal Prison Industries, 400 First Street, NW., Washington, DC 20534.

USMS: Address requests to the system manager named above, attention: FOIA/PA Officer.

DEA: Address requests to the system manager named above.

FBI: Address requests to the system manager named above.

ATF: Address request to Disclosure Division, Privacy Act Request, Bureau of Alcohol, Tobacco, Firearms and Explosives, 650 Massachusetts Avenue, NW., Washington, DC 20226.

The envelope and letter should be clearly marked "Privacy Act Access Request." The request should include a general description of the records sought and must include the requester's full name, current address, and date and place of birth. The request must be signed and dated and either notarized or submitted under penalty of perjury. If known, the requester should also identify the date or year in which a debt was incurred, *e.g.*, date of invoice or purchase order.

CONTESTING RECORD PROCEDURES:

Individuals desiring to contest or amend information maintained in the system should direct their request according to the Record Access Procedures listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. Some information is not subject to amendment, such as tax return information. A determination whether a record may be amended will be made at the time a request is received.

RECORD SOURCE CATEGORIES:

Operating personnel, individuals covered by the system, and Federal agencies.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

[FR Doc. 04–12578 Filed 6–2–04; 8:45 am]

BILLING CODE 4410–FB–P

DEPARTMENT OF JUSTICE

Bureau of Alcohol, Tobacco, Firearms, and Explosives

Agency Information Collection Activities: Proposed Collection; Comments Requested

ACTION: 30-Day notice of information collection under review: Notice of Firearms Manufactured or Imported.

The Department of Justice (DOJ), Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) has submitted the following information collection request to the Office of Management and Budget (OMB) for review and approval in accordance with the Paperwork Reduction Act of 1995. The proposed information collection is published to obtain comments from the public and affected agencies. This proposed information collection was previously published in the **Federal Register** Volume 69, Number 61, on page 16609, on March 30, 2004, allowing for a 60 day comment period.

The purpose of this notice is to allow for an additional 30 days for public comment until July 6, 2004. This process is conducted in accordance with 5 CFR 1320.10.

Written comments and/or suggestions regarding the items contained in this notice, especially the estimated public burden and associated response time, should be directed to The Office of Management and Budget, Office of Information and Regulatory Affairs, Attention Department of Justice Desk Officer, Washington, DC 20503. Additionally comments may be submitted to OMB via facsimile to (202) 395–5806.

Written comments and suggestions from the public and affected agencies concerning the proposed collection of information are encouraged. Your comments should address one or more of the following four points:

- Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;
- Evaluate the accuracy of the agencies estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used;

subject imports, and likely impact of imports of *Subject Merchandise* on the *Domestic Industry*.

(5) A list of all known and currently operating U.S. producers of the *Domestic Like Product*. Identify any known related parties and the nature of the relationship as defined in section 771(4)(B) of the Act (19 U.S.C. 1677(4)(B)).

(6) A list of all known and currently operating U.S. importers of the *Subject Merchandise* and producers of the *Subject Merchandise* in each *Subject Country* that currently export or have exported *Subject Merchandise* to the United States or other countries since the *Order Date*.

(7) If you are a U.S. producer of the *Domestic Like Product*, provide the following information on your firm's operations on that product during calendar year 2005 (report quantity data in pounds and value data in U.S. dollars, f.o.b. plant). If you are a union/worker group or trade/business association, provide the information, on an aggregate basis, for the firms in which your workers are employed/which are members of your association.

(a) Production (quantity) and, if known, an estimate of the percentage of total U.S. production of the *Domestic Like Product* accounted for by your firm's(s') production;

(b) The quantity and value of U.S. commercial shipments of the *Domestic Like Product* produced in your U.S. plant(s); and

(c) The quantity and value of U.S. internal consumption/company transfers of the *Domestic Like Product* produced in your U.S. plant(s).

(8) If you are a U.S. importer or a trade/business association of U.S. importers of the *Subject Merchandise* from each *Subject Country*, provide the following information on your firm's(s') operations on that product during calendar year 2005 (report quantity data in pounds and value data in U.S. dollars). If you are a trade/business association, provide the information, on an aggregate basis, for the firms which are members of your association.

(a) The quantity and value (landed, duty-paid but not including antidumping duties) of U.S. imports and, if known, an estimate of the percentage of total U.S. imports of *Subject Merchandise* from each *Subject Country* accounted for by your firm's(s') imports;

(b) The quantity and value (f.o.b. U.S. port, including antidumping duties) of U.S. commercial shipments of *Subject Merchandise* imported from each *Subject Country*; and

(c) The quantity and value (f.o.b. U.S. port, including antidumping duties) of U.S. internal consumption/company transfers of *Subject Merchandise* imported from each *Subject Country*.

(9) If you are a producer, an exporter, or a trade/business association of producers or exporters of the *Subject Merchandise* in the *Subject Countries*, provide the following information on your firm's(s') operations on that product during calendar year 2005 (report quantity data in pounds and value data in U.S. dollars, landed and duty-paid at the U.S. port but not including antidumping duties). If you are a trade/business association, provide the information, on an aggregate basis, for the firms which are members of your association.

(a) Production (quantity) and, if known, an estimate of the percentage of total production of *Subject Merchandise* in each *Subject Country* accounted for by your firm's(s') production; and

(b) The quantity and value of your firm's(s') exports to the United States of *Subject Merchandise* and, if known, an estimate of the percentage of total exports to the United States of *Subject Merchandise* from each *Subject Country* accounted for by your firm's(s') exports.

(10) Identify significant changes, if any, in the supply and demand conditions or business cycle for the *Domestic Like Product* that have occurred in the United States or in the market for the *Subject Merchandise* in each *Subject Country* since the *Order Date*, and significant changes, if any, that are likely to occur within a reasonably foreseeable time. Supply conditions to consider include technology; production methods; development efforts; ability to increase production (including the shift of production facilities used for other products and the use, cost, or availability of major inputs into production); and factors related to the ability to shift supply among different national markets (including barriers to importation in foreign markets or changes in market demand abroad). Demand conditions to consider include end uses and applications; the existence and availability of substitute products; and the level of competition among the *Domestic Like Product* produced in the United States, *Subject Merchandise* produced in each *Subject Country*, and such merchandise from other countries.

(11) (Optional) A statement of whether you agree with the above definitions of the *Domestic Like Product* and *Domestic Industry*; if you disagree with either or both of these definitions, please explain why and provide alternative definitions.

Authority: These reviews are being conducted under authority of title VII of the Tariff Act of 1930; this notice is published pursuant to section 207.61 of the Commission's rules.

Issued: December 22, 2005.

By order of the Commission.

Marilyn R. Abbott,

Secretary to the Commission.

[FR Doc. 05–24585 Filed 12–30–05; 8:45 am]

BILLING CODE 7020–02–U

DEPARTMENT OF JUSTICE

[AAG/A Order No. 020–2005]

Privacy Act of 1974; System of Records

Pursuant to the provisions of the Privacy Act of 1974 (5 U.S.C. 552a), notice is given that the Department of Justice proposes to modify a Departmentwide system of records entitled "Accounting Systems for the Department of Justice (DOJ), DOJ–001." This system of records was last published on June 3, 2004 at 69 FR 31406. The major modification of the system involves the addition of certain Federal Bureau of Investigation (FBI) accounting records resulting in a new security classification. The system now contains classified documents as well as Sensitive But Unclassified (SBU) documents. Other modifications include: Minor edits to the Safeguards section regarding access; a new system manager for the Justice Management Division; additions to the Categories of Individuals Covered by the System; an addition to the Categories of Records in the System; and a minor correction to the section on Disclosure to Consumer Reporting Agencies, and non-substantive edits.

In accordance with 5 U.S.C. 552a(e)(4) and (11), the public is given a 30-day period in which to comment on this notice; and the Office of Management and Budget (OMB), which has oversight responsibility under the Act, requires a 40-day period in which to conclude its review of the system. Therefore, please submit any comments by February 13, 2006. The public, OMB, and the Congress are invited to submit any comments to Mary E. Cahill, Management and Planning Staff, Justice Management Division, Department of Justice, Washington, DC 20530 (Room 1400, National Place Building).

In accordance with 5 U.S.C. 552a(r), the Department has provided a report to OMB and the Congress.

Dated: December 15, 2005.

Paul R. Corts,

Assistant Attorney General for Administration.

Department of Justice—001

SYSTEM NAME:

Accounting Systems for the Department of Justice (DOJ).

SECURITY CLASSIFICATION:

The DOJ Accounting Systems may be Sensitive But Unclassified (SBU) or Classified.

* * * * *

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals/persons (including DOJ employees; and including current and former inmates under the custody of the Attorney General) who are in a relationship, or who seek a relationship, with the DOJ or a component thereof—a relationship that may give rise to an accounts receivable, an accounts payable, or to similar accounts such as those resulting from a grantee/grantor relationship; and federal debtors, including those who have received overpayments through direct financial assistance, those who owe debts of restitution based on civil or criminal judgments entered by federal courts, and those who have obtained insured or guaranteed loans from federal agencies, and whose delinquent debts have been sent by client federal agencies to the DOJ for enforced collection through litigation. Included may be:

(a) * * *
(b) * * *
(c) * * *
(d) * * *
(e) Those who have made partial or full payments to be applied to their federal debt.

CATEGORIES OF RECORDS IN THE SYSTEM:

(1) All documents used to reserve, obligate, process, and effect collection or payment of funds, e.g., vouchers (excluding payroll vouchers), invoices, purchase orders, travel advances, travel/transfer vouchers and other such documentation reflecting information about: (a) Payments due or made to, (b) claims made or debts owed by the individuals covered by this system, including fees, fines, penalties, overpayments, and/or other assessments; all documents used to comply with reporting regulations of the Internal Revenue Service of the Department of Treasury; and (3) all documentation and information pertaining to the receipt of payments made by or on the behalf of federal debtors against their debts and the disbursement or transfer of those payments by DOJ to the appropriate recipients.

* * * * *

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

Only as noted in Routine Use 20(b) and Routine Use 23 in the Federal Register notice of June 3, 2004 (69 FR 31406).

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

* * * * *

SAFEGUARDS:

All data will be protected in accordance with applicable DOJ and federal guidance, policies, and directives based on the security classification of the information/system. Access is limited to DOJ personnel with a need to know. Access to computerized information is controlled by passwords, or similar safeguards, which are issued only to authorized personnel. Records are retained in the form of digitized images on a server to which limited workstations have access. Passwords control access to the server from these workstations. Paper records, and some computerized media, are kept in locked files of locked offices during off duty hours. In addition, servers, workstations, and offices are located in controlled-access buildings.

* * * * *

SYSTEM MANAGER(S) AND ADDRESSES:

DAAG/Controller, Finance Staff, Justice Management Division (JMD), U.S. Department of Justice, 950 Pennsylvania Ave., NW., Washington, DC 20530.

* * *
* * *
* * *
* * *
* * *
* * *

* * * * *

[FR Doc. E5–8199 Filed 12–30–05; 8:45 am]

BILLING CODE 4410–F8–P

DEPARTMENT OF LABOR

Employment and Training Administration

Notice of Approval for Missouri for Avoidance of 2005 Credit Reduction Under the Federal Unemployment Tax Act

Sections 3302(c)(2) and 3302(d)(3) of the Federal Unemployment Tax Act (FUTA) provide that employers in a state that has an outstanding balance of advances under Title XII of the Social Security Act on January 1 of two or more consecutive years are subject to a reduction in credits otherwise available against the FUTA tax for a calendar year, if a balance of advances remains on November 10 of that year. Because the account of Missouri in the Unemployment Trust Fund had a balance of advances on both January 1, 2004, and January 1, 2005, and still had a balance on November 10, 2005, Missouri employers were potentially liable for a reduction in their FUTA offset credit for 2005.

Section 3302(g) of FUTA provides that a state may avoid credit reduction for a year by meeting certain criteria. Missouri applied for avoidance of the 2005 credit reduction under this section. Pursuant to delegation of authority to me under Secretary's Order 4–75, I have determined that Missouri meets all of the criteria of this section 3302(g) and thus qualifies for credit reduction avoidance. Therefore, Missouri employers will have no reduction in FUTA offset credit for calendar year 2005.

Dated: December 20, 2005.

Emily Stover DeRocco,

Assistant Secretary for Employment and Training.

[FR Doc. 05–24681 Filed 12–30–05; 8:45 am]

BILLING CODE 4510–30–M

NATIONAL SCIENCE BOARD

Programs and Plans Committee; Notice of Meeting

Date and Time: January 9, 2006, 10 a.m.–11 a.m. (ET)

Place: National Science Foundation, 4201 Wilson Boulevard, Arlington, VA 22230, Public Meeting Room 365.

Status: This meeting will be open to the public.

Matters To Be Considered:

Monday, January 9, 2006, Open Session

Open Session (10 a.m.–11 a.m.)

- Committee review of NSF draft Cyberinfrastructure Vision document
- Committee discussion and comments

FOR FURTHER INFORMATION CONTACT: Dr. Michael P. Crosby, Executive Officer and NSB Office Director, (703) 292–7000, *http://www.nsf.gov/nsb.*

Michael P. Crosby,

Executive Officer and NSB Office Director.

[FR Doc. E5–8216 Filed 12–30–05; 8:45 am]

BILLING CODE 7555–01–P