United States Marshals Service (USMS)

Privacy Impact Assessment
for the

Justice Prisoner and Alien Transportation System (JPATS)

JPATS Management Information System (JMIS)

Issued by:
William E. Bordley
Senior Component Official for Privacy
United States Marshals Service

Reviewed by: Luke J. McCormack, Chief Information Officer
Department of Justice

Approved by: Joo Y. Chung
Acting Chief Privacy and Civil Liberties Officer
Department of Justice

Date approved: [September 24, 2013]

(August 2010 DOJ PIA Form)

[This PIA should be completed in accordance with the DOJ Privacy Impact Assessments Official Guidance (and any supplemental guidance) posted at http://www.justice.gov/opcl/pia.htm.]

Section 1: Description of the Information System

Provide a non-technical overall description of the system that addresses:

(a) the purpose that the records and/or system are designed to serve;
(b) the way the system operates to achieve the purpose(s);
(c) the type of information collected, maintained, used, or disseminated by the system;
(d) who has access to information in the system;
(e) how information in the system is retrieved by the user;
(f) how information is transmitted to and from the system; and
(g) any interconnections with other systems.

Introduction

[Note: A description of acronyms used in this PIA is provided in Appendix A.]

The Justice Prisoner and Alien Transportation System (JPATS)[1] is responsible for the movement of prisoners or detainees for the United States Marshals Service (USMS) and Bureau of Prisons (BOP). (As of Fiscal Year (FY) 2010, JPATS no longer transports illegal aliens for U.S. Immigration and Customs Enforcement (ICE).) On a space available basis, JPATS will transport Non-Federal and military prisoners.

JPATS owns or leases aircraft and fully manages them. Ground transportation vehicles are owned and operated by USMS, BOP and other contracted facilities. JPATS schedules prisoner transportation from origin to destination on both air and ground modes.

JPATS has been operating as a revolving fund since FY 1999. As JPATS is a revolving fund, it must recover the fixed and variable costs of operations (which include the costs of JPATS employees' salaries and travel expenses). Accordingly, JPATS needs to budget and account for its fixed and variable costs so that JPATS customers can be appropriately charged depending upon customer category (such as primary (USMS and BOP), space available, or non-Federal (non-Fed)) and particular transportation modes and locations. JPATS only charges for air transportation, while ground transportation costs are picked up by the USMS and BOP offices and facilities that perform the ground transportation.

JPATS processes requests for prisoner/detainee movements (also known as Form-106 records), and

[1] JPATS is not an electronic system but instead is the name of the USMS Division that coordinates prisoner movements.

coordinators schedule these movements on trips based upon their needs and security levels. Coordinators arrange for the vehicles (cars, vans, buses, and aircraft) to move the prisoners/detainees, and prepare manifests that list prisoners/detainees that will be moved by a particular means on a particular date. Coordinators divide the country into sectors or regions; when a prisoner becomes the responsibility of another coordinator; the record is forwarded to the next coordinator.

Transportation Module

The Transportation module of JMIS allows the JPATS coordinators to fulfill their duties electronically. It provides security and medical information on prisoners/detainees to help coordinators make proper movement scheduling decisions and provides needed security and medical information to personnel transporting prisoners/detainees. Transportation coordinators can create and modify trips for prisoner/detainee movements using JMIS. The program allows a coordinator to view assigned movement request forms and schedule prisoners/detainees on new or existing trips. JMIS also generates trip manifests, which list prisoners/detainees who have been scheduled on a trip with pertinent prisoner/detainee security and medical information. JMIS transmits manifests to USMS personnel and is available in JDIS[2] and eDesignate[3] at locations where prisoners/detainees will be picked up or delivered.

Transportation Data Sources

JMIS receives prisoner data via JDIS and eDesignate on Form-106's. JPATS JMIS users have access to BOP SENTRY[4] and, when needed, may manually copy transportation-pertinent, medical, and security data from SENTRY into JMIS. Non-Fed prisoner movement requests are entered and submitted by USMS offices through JDIS and eDesignate as well. On rare occasions involving mass Non-Fed or military movements, JPATS receives a list of names and prisoner numbers of prisoners/detainees to be transported with no other data; this data is manually keyed into JMIS. If in the rare case JPATS authorizes NON-prisoners/detainees to travel on a JPATS aircraft, the data is not stored within JMIS.

Financial Module

JMIS Financials is the management tool with modules used for JPATS Budget Build, Monthly Billing for Federal and Non-Federal customers, in addition to tracking and reporting costs through a General Ledger (GL) interface with DOJ's Unified Financial Management System (UFMS). The expenses recorded in JMIS are used to develop budgets for the revolving fund and to determine the per seat, per flight-hour cost for USMS, BOP and Non-Federal prisoners/detainees. The JMIS Financials System is

[2] The Justice Detainee Information System (JDIS) is a USMS system that contains prisoner booking data and daily operations records in the USMS district offices.

[3] eDesignate (eDes) is a system used to electronically flow paperwork while detainees are going through the Federal court process.

[4] SENTRY is BOP's real-time information system consisting of various applications for processing inmate information and for property management.

built on Oracle's e-Business Suite Release 12.1.1 Federal and includes General Ledger, Budgeting, and Receivables. As of FY 2013, JPATS is using UFMS for purchasing, payments, and other financial functions.

Financial Data Sources

JMIS records data on USMS JPATS employees for budget projection purposes. This data is collected when employees are hired and updated as promotions and step increases occur. This data is entered from new-hire paperwork. JMIS also collects payroll data through its GL interface from UFMS. JMIS also contains location data on Federal, state, local and private facilities. This includes the address and phone number of the facility. The names of personnel at these facilities along with phone number and E-mail address are stored for communication purposes. If a state or local facility has contracted with JPATS to move a Non-Fed prisoner, a tax identification number is recorded for that entity. This data is manually recorded when the state or local facility contracts with JPATS to move a prisoner. This data is required by UFMS to bill and receive payments from these customers.

Interconnections

All JMIS components and data reside on the USMS Network (USMS-Net). The Transportation and Financial user interfaces in JMIS are only accessed by personnel working in JPATS offices. JMIS Transportation data is accessible by USMS District offices and BOP Institutions through JDIS and data is interfaced to eDesignate (a system managed by OFDT, a component of the USMS) accessed by USMS users. GL transactions are interfaced daily to JMIS from UFMS. Accounts Receivable (billing) data is interfaced monthly from JMIS to UFMS.

Interconnection Agreements

There is a Memorandum of Agreement (MOA) with BOP issued in July 2011. The BOP MOA establishes individual and organizational security responsibilities for protection and handling of the JMIS data/information.

Systems Hardware and Software

The JMIS database, applications, and systems consist of several in-house configured COTS products: Oracle E-Business Suite, Oracle Transportation Management, Oracle Application Express, and Oracle Business Intelligence.

Section 2: Information in the System

2.1 Indicate below what information is collected, maintained, or disseminated.

- JPATS Employees Information

Identifying numbers – *JPATS Employees*					
Social Security	X	Alien Registration		Financial account*	X
Taxpayer ID		Driver's license		Financial transaction	
Employee ID		Passport		Patient ID	
File/case ID		Credit card			
Other identifying numbers (specify):	* Archival data exists but is no longer used or collected.				

General personal data - *JPATS Employees*					
Name	X	Date of birth	X	Religion	
Maiden name		Place of birth		Financial info	
Alias		Home address*	X	Medical information	
Gender	X	Telephone number		Military service	
Age		Email address		Physical characteristics	
Race/ethnicity		Education		Mother's maiden name	
Other general personal data (specify):	* Archival data exists but is no longer used or collected.				

Work-related data - *JPATS Employees*					
Occupation	X	Work telephone no.	X	Salary (grade/step)	X
Job title		Work email address	X	Work history	
Work address	X	Business associates			
Other work-related data (specify):					

Distinguishing features/Biometrics – *JPATS Employees*					
Fingerprints		Photos		DNA profiles	
Palm prints		Scars, marks, tattoos		Retina/iris scans	
Voice recording/signatures		Vascular scan		Dental profile	
Other distinguishing features/biometrics (specify):					

System admin/audit data – *JPATS Employees*					
User ID	X	Date/time of access	X	ID files accessed	
IP address	X	Queries run		Contents of files	
Other system/audit data (specify):					

- **JMIS Prisoners/Detainees Information**

Identifying numbers – ***JMIS Prisoners/Detainees***					
Social Security		Alien Registration		Financial account	
Taxpayer ID		Driver's license		Financial transaction	
Employee ID		Passport		Patient ID	
File/case ID		Credit card			
Other identifying numbers (specify): Prisoner Number					

General personal data - ***JMIS Prisoners/Detainees***					
Name	X	Date of birth	X	Religion	
Maiden name		Place of birth		Financial info	
Alias	X	Home address		Medical information	X
Gender	X	Telephone number		Military service	
Age	X	Email address		Physical characteristics	X
Race/ethnicity	X	Education		Mother's maiden name	
Other general personal data (specify):					

Work-related data - ***JMIS Prisoners/Detainees***					
Occupation		Telephone number		Salary	
Job title		Email address		Work history	
Work address		Business associates			
Other work-related data (specify):					

Distinguishing features/Biometrics - ***JMIS Prisoners/Detainees***					
Fingerprints		Photos		DNA profiles	
Palm prints		Scars, marks, tattoos	X	Retina/iris scans	
Voice recording/signatures		Vascular scan		Dental profile	
Other distinguishing features/biometrics (specify):					

System admin/audit data - ***JMIS Prisoners/Detainees***					
User ID		Date/time of access		ID files accessed	
IP address		Queries run		Contents of files	
Other system/audit data (specify):					

Other information (specify) - ***JMIS Prisoners/Detainees***
Gang Affiliation

- **JMIS Facility/Customer Information**

Identifying numbers – ***JMIS Facility/Customer***					
Social Security		Alien Registration		Financial account	
Taxpayer ID	X	Driver's license		Financial transaction	
Employee ID		Passport		Patient ID	
File/case ID		Credit card			
Other identifying numbers (specify):					

General personal data - ***JMIS Facility/Customer***					
Name	X	Date of birth		Religion	
Maiden name		Place of birth		Financial info	
Alias		Home address		Medical information	
Gender		Telephone number		Military service	
Age		Email address		Physical characteristics	
Race/ethnicity		Education		Mother's maiden name	
Other general personal data (specify):					

Work-related data - ***JMIS Facility/Customer***					
Occupation		Telephone number	X	Salary	
Job title		Email address	X	Work history	
Work address	X	Business associates			
Other work-related data (specify):					

Distinguishing features/Biometrics - ***JMIS Facility/Customer***					
Fingerprints		Photos		DNA profiles	
Palm prints		Scars, marks, tattoos		Retina/iris scans	
Voice recording/signatures		Vascular scan		Dental profile	

Distinguishing features/Biometrics - *JMIS Facility/Customer*
Other distinguishing features/biometrics (specify):

System admin/audit data - *JMIS Facility/Customer*					
User ID		Date/time of access		ID files accessed	
IP address		Queries run		Contents of files	
Other system/audit data (specify):					

Other information (specify) - *JMIS Facility/Customer*

2.2 Indicate sources of the information in the system. (Check all that apply.)

- **JPATS Employees Information**

Directly from individual about whom the information pertains – *JPATS Employees*					
In person	X	Hard copy: mail/fax	X	Online	
Telephone	X	Email	X		
Other (specify):					

Government sources - *JPATS Employees*					
Within the Component	X	Other DOJ components		Other federal entities	
State, local, tribal		Foreign			
Other (specify):					

Non-government sources - *JPATS Employees*					
Members of the public		Public media, internet		Private sector	
Commercial data brokers					
Other (specify):					

- **JMIS Prisoners/Detainees Information**

Directly from individual about whom the information pertains – *JMIS Prisoners/Detainees*					
In person		Hard copy: mail/fax		Online	
Telephone		Email			
Other (specify):	Prisoners Information (Movement Request 106's) is provided to JMIS from two DOJ systems eDesignate & the JDIS. No prisoner information within JMIS comes directly from the prisoner.				

Government sources - *JMIS Prisoners Information*					
Within the Component	X	Other DOJ components	X	Other federal entities	
State, local, tribal		Foreign			
Other (specify):	All prisoner/detainee information comes from either eDesignate & JDIS over secure DOJ network lines.				

Non-government sources - *JMIS Prisoners Information*					
Members of the public		Public media, internet		Private sector	
Commercial data brokers					
Other (specify):					

- **JMIS Facility/Customer Information**

Directly from individual about whom the information pertains – *JPATS Facility/Customer*					
In person		Hard copy: mail/fax	X	Online	
Telephone	X	Email	X		
Other (specify):					

Government sources - *JPATS Facility/Customer*					
Within the Component	X	Other DOJ components	X	Other federal entities	
State, local, tribal	X	Foreign			
Other (specify):					

Non-government sources - *JPATS Facility/Customer*					
Members of the public		Public media, internet		Private sector	
Commercial data brokers					
Other (specify):					

2.3 Analysis: Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Please describe the choices that the

component made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

Risks that generally apply to the collection of information are that the information may be misused, improperly accessed, or improperly disclosed. For a discussion of these risks and mitigations, please see Subsections 3.5 and 4.2 and Section 6.

Currently, all JPATS data about USMS employees is required to support JPATS Human Resource requirements and payroll budget projections. In addition, the JPATS information on prisoners/ detainees is required to manage transporting the inmates and ensuring the safety of both the inmates and the public. However, the USMS is alert to reduce the amount of data collected in the systems when feasible. For example, the collection and retention personal information on USMS employees within JMIS was reduced recently due to the utilization of another system (UFMS) for purchasing and payments. JPATS no longer uses JMIS to reimburse its employees travel and other expenses and no longer adds to employee financial account information. However, due to record retention policies the historic payment data still resides within JMIS.

The nature and quality of information sources can present additional risks, particularly when the source is not the individual the information is about. As detailed in Section 5 below, however, it is neither practicable nor appropriate to obtain JPATS information directly from the prisoners/detainees. However, the prisoner/detainee information is obtained from government systems (eDesignate and/or JDIS (106's)) in which the business needs of law enforcement for accurate information help ensure reliability of the information. Similarly, information on USMS employees is directly obtained from information already contained in USMS and DOJ human resource and accounting systems in order to tie payroll records to employees to document salary for payroll budget projections. Here, too, USMS/DOJ business needs for accurate information help ensure reliability of the information.

For state and local law enforcement a tax identification number for the entity is collected as a requirement to properly bill non-federal entities through UFMS for requested prisoner/detainee movements. Contact information must also be maintained for facilities and staff that work at those facilities. Communication with personnel regarding the movement of prisoners is a necessity to maintain safe and reliable security.

<u>Section 3</u>: Purpose and Use of the System

3.1 Indicate why the information in the system is being collected, maintained, or disseminated. (Check all that apply.)

Purpose			
X	For criminal law enforcement activities		For civil enforcement activities
	For intelligence activities		For administrative matters

	To conduct analysis concerning subjects of investigative or other interest		To promote information sharing initiatives
	To conduct analysis to identify previously unknown areas of note, concern, or pattern.		For administering human resources programs
	For litigation		
X	Other (specify): To safely transport prisoners/detainees for detention and court proceedings. For budget development and billing purposes		

3.2 Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.

As detailed above in Section 1, the information maintained by JMIS is used to support correctly identifying prisoners/detainees and arranging safe and secure transportation for varying security levels of male, female & juvenile prisoners/detainees. Having the necessary personally identifiable information and medical or security information on prisoners/detainees who are being transported is vital to ensuring the law enforcement officers performing transportation can perform their duties properly and keep both those transported and the public safe.
Payroll data is used to properly budget for overtime, grade level and step/within-grade increases, and to support customer billing incident to JPATS operations as a revolving fund.

3.3 Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

Authority		Citation/Reference
X	Statute	18 U.S.C. 3149, 3193, 3604, 3621, 4002, 4006, 4086, 4285, 5001, 5003; 28 U.S.C. 509, 510, 561-567; 5 U.S.C. 301; 44 U.S.C. 3101.
	Executive Order	
X	Federal Regulation	28 CFR 0.111-.114, .123.
X	Memorandum of Understanding/agreement	MOA with BOP dated 2011. MOU with OFDT dated 2012.
	Other	

3.4 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

Records in JMIS are disposed of in accordance with records retention schedules approved by the National Archives and Records Administration (NARA) applicable to the particular records. Currently, prisoner movement information within JMIS is retained for a period of six years. This is based upon the General Records Schedule # 9, (N1-GRS-91-3, item 1a) and (N1-GRS-91-3, item 3a). The financial records in JMIS are retained for Six years and three months according to the General Records Schedule # 3 (N1-GRS-95-4 item 3a1a)

3.5 Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Risks that generally apply to the use of information are that the information may be misused or improperly disclosed. The USMS mitigates these risks by various means, including user training, audits, system security measures, purging the information when no longer needed, and adherence to applicable disclosure limitations. DOJ, USMS and JPATS have implemented administrative and technological security controls and measures to protect the information, both while in storage and in transit. Each organization that has access to JMIS information/data is responsible for the actions of its users, and sanctions will be applied for intentional or repeated misuse of the data.

- All JMIS components reside on the secure USMS Network (USMS-Net).
- Access to and disclosure of JMIS information is limited to users who have a need to know for the performance of JPATS duties and access/disclosure is limited as may be permissible under the Privacy Act, 5 U.S.C. 552a.
- Each User must complete an annual Privacy and Security awareness training.
- JPATS abides by the information retention schedules established by the National Archives and Records Administration (NARA). Each FY JPATS has automated routines that are initiated to run to purge data that is outside of the retention schedule.

Please see Subsections 4.2 and Section 6 for additional information.

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component			X	

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
DOJ components		X	X	
Federal entities	X			Summarized flight hour and cost data is provide to Department of Transportation on Government owned aircraft
State, local, tribal gov't entities	X			
Public				
Private sector	X			Contracted transportation & housing providers receive copies of JMIS manifests. Manifests contain Prisoner's Number, Name and Sex.
Foreign governments				
Foreign entities				
Other (specify):				

4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.)

Direct Access:

Each User must have an approved USMS-169 ITD User Account Request
Each User has an individual ID with password.
User's password expires after 60 days.
Each DOJ User is required to take annual privacy & Security Awareness Training.

Bulk Transfer:

All bulk transfers are performed on Secure DOJ network lines.

Case by Case:

DOJ contracted transportation & housing providers must adhere to privacy and security requirements established in the contracts.

Also, please see Subsection 3.5 and Section 6.

<u>Section 5:</u> Notice, Consent, and Redress

5.1 Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system. (Check all that apply.)

- **JPATS Employees Information**

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7.	
	Yes, notice is provided by other means.	Specify how:
	No, notice is not provided.	Specify why not:

- **JMIS Prisoners/Detainees Information**

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7.	
	Yes, notice is provided by other means.	Specify how:
	No, notice is not provided.	Specify why not:

- **JMIS Facility/Customer Information**
-

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7.	
	Yes, notice is provided by other means.	Specify how:
	No, notice is not provided.	Specify why not:

5.2 Indicate whether and how individuals have the opportunity to decline to provide information.

- **JPATS Employees Information**

	Yes, individuals have the opportunity to decline to provide information.	Specify how:
X	No, individuals do not have the opportunity to decline to provide information.	Specify why not: This information is automatically populated from information already present in other USMS systems as a condition of employment in order to tie payroll records to employees to document salary for payroll budget projections.

- **JMIS Prisoners/Detainees Information**

	Yes, individuals have the opportunity to decline to provide information.	Specify how:
X	No, individuals do not have the opportunity to decline to provide information.	Specify why not: Prisoners Movement Request information is received into JMIS from two secure DOJ systems, eDes & JDIS. No direct information is entered into JMIS from the prisoners/detainees. This information is necessary for prisoner/detainee management for law enforcement purposes; providing prisoners/detainees opportunity to decline to provide this information would be impracticable and unwarranted.

- **JMIS Facility/Customer Information**

	Yes, individuals have the opportunity to decline to provide information.	Specify how:
X	No, individuals do not have the opportunity to decline to provide information.	Specify why not: This information is necessary for prisoner/detainee transportation management for law enforcement purposes; providers must furnish this information as a condition of providing the service, but have the option to not seek to provide the service.

5.3 Indicate whether and how individuals have the opportunity to consent to particular uses of the information.

- **JPATS Employees Information**

	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how:
X	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: This information is automatically populated from information already present in other USMS systems as a condition of employment in order to tie payroll records to employees to document salary for payroll budget projections.

- **JMIS Prisoners/Detainees Information**

	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how:

X	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: Prisoners Movement Request information is received into JMIS from two secure DOJ systems eDes & JDIS. No direct information is entered into JMIS from the prisoner/detainee. This information is necessary for prisoner/detainee management for law enforcement purposes; obtaining prisoner consent for such uses would be impracticable and unwarranted.

- **JMIS Facility/Customer Information**

	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how:
X	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: Facility and Customer information is entered into JMIS from user provided data. This information is necessary for prisoner/detainee transportation management for law enforcement purposes; providers must furnish this information as a condition of providing the service, but have the option to not seek to provide the service.

5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

Prisoners/Detainees: USMS systems of records for prisoners/detainees have been exempted from the specific notice requirements of Privacy Act subsections (e)(2) and (e)(3). (See 28 CFR 16.101.) However, prisoners/detainees are provided general notice via the system of records notice published in the Federal Register and discussed in Section 7. JMIS receives Prisoner Movement Request (106's) from secure DOJ systems (eDes & JDIS). JMIS does not enter any direct input of information from the prisoner/detainee (individual). This is why JMIS does not need to provide the opportunity for consent of the prisoner. This information is necessary for prisoner/detainee management for law enforcement purposes; obtaining prisoner consent for such collection/uses would be impracticable and unwarranted.

USMS Employees: Information on USMS employees is directly obtained from information already contained in USMS and DOJ human resource and accounting systems in order to tie payroll records to employees to document salary for payroll budget projections.

Facility and Customer information is directly obtained from individuals for the purposes of receiving communications for completing the prisoner/detainee movement process. It is impracticable for customers to decline providing contact information, because they would not be able to complete the transportation mission without receiving communications.

Section 6: Information Security

6.1 Indicate all that apply.

X	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: 7/27/2013. If Certification and Accreditation has not been completed, but is underway, provide status or expected completion date:	
X	A security risk assessment has been conducted	
X	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: JMIS was tested for compliance with security controls in the following categories: Access Control; Awareness and Training; Audit and Accountability; Certification, Accreditation, and Security Assessments; Configuration Management; Contingency Planning; Identification and Authentication; Incident Response; Maintenance; Media Protection; Physical and Environmental Protection; Planning; Personnel Security; Risk Assessment; System and Services Acquisition; System and Communications Protection; and System and Information Integrity. All security controls identified by HQ ITD security have been implemented.	
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: JMIS's security controls are in a continuous monitoring phase and it receives periodic vulnerability assessments. Continuous monitoring will continue for JMIS during its remaining operational status. A re-validation of the sub-set of controls needs is underway as well as a validation of the remaining controls to grant JMIS an ATO for a full 3 years.	
X	Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information: Security control analysis entails an auditing function that aims to prevent the misuse of information.	
X	Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act.	
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy.	
X	The following training is required for authorized users to access or receive information in the system: Rules Of Behaviors, Privileged Rules Of Behaviors, DOJ Annual IT Professional training credit	
	X	General information security training
	X	Training specific to the system for authorized users within the Department.

	□	Training specific to the system for authorized users outside of the component.
	□	Other (specify):

6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure.

Access is controlled by role-based security, which permits access only to those individuals who have a need for the information for the performance of their assigned job functions. Supervisory approval is required before access is granted and access is removed when no longer needed. In addition, administrative controls such as monitoring accounts annually, maintenance and review of audit trails, help to prevent or discover unauthorized access. JMIS equipment is located in facilities where access points are controlled through card readers which recognize only personnel authorized for system related law enforcement functions. The system was tested for compliance with security controls in the following categories: Access Control; Awareness and Training; Audit and Accountability; Certification, Accreditation, and Security Assessments; Configuration Management; Contingency Planning; Identification and Authentication; Incident Response; Maintenance; Media Protection; Physical and Environmental Protection; Planning; Personnel Security; Risk Assessment; System and Services Acquisition; System and Communications Protection; and System and Information Integrity. The risk was assessed, the results formally documented, and authority to operate the system was obtained.

Some of the specific controls that address access to and modification of data include the following:

Access Controls – In accordance with USMS Standard Operating Procedure: Account Management, supervisors complete account request forms specifying that accounts are needed to perform assigned duties before personnel are given access to the system. User permissions within the system are limited based on the roles supervisors have specified for each user.

Configuration Management – Security settings are configured to the most restrictive mode consistent with information system operational requirements.

Audit and Accountability – JMIS system owner and system administrators configure the system to generate audit records for account failed and successful logon events; account management actions and user rights changes that have not been authorized; any policy changes that have not been authorized.

Data Encryption – JMIS database links and application access is protected in transit throughout the USMS Network using encrypted ODBC and HTTPS/SSL. Information is also encrypted as well from router to router across the WAN.

<u>Section 7</u>: Privacy Act

7.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

X	Yes, and this system is covered by an existing system of records notice. Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system: Substantive information in JMIS is covered by USM-005, U.S. Marshals Service Prisoner Processing and Population Management/Prisoner Tracking System (PPM/PTS) (72 FR 33515, 33519), available at this link: http://www.justice.gov/opcl/privacyact.html#USM . JMIS user information is covered by DOJ-002, Department of Justice Computer Systems Activity and Access Records (64 FR 73585). available at this link: http://www.justice.gov/opcl/privacyact.html#DOJ . Financial information (including archival information) relating to USMS employee salaries and travel is covered by JMD-003, Department of Justice Payroll System (69 FR 107), available at this link: http://www.justice.gov/opcl/privacyact.html#JMD , and/or by DOJ-001, Accounting Systems for the Department of Justice (DOJ) (69 FR 31406), available at this link: http://www.justice.gov/opcl/privacyact.html#DOJ .
	Yes, and a system of records notice is in development.
	No, a system of records is not being created.

7.2 Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

JMIS Employee Information – Is accessed via JMIS reports and used to compute future year budgets. Employee grade/step information is used to project future year salary expenses. Actual historical pay data is in a summarized format by accounting string in JMIS and is not stored by employee name or identification number.

JMIS Prisoner/Detainee Information – Is needed to perform routine functions within JMIS and is retrieved using application developed queries by Prisoner number, Name, and/or Movement ID.

JMIS Facility/Customer Information – Can be retrieved by name or facility code. It is also displayed on billing invoices. JMIS also contains a location table that holds the facility data with a location code as the unique identifier. JMIS also includes a rolodex/contact table with points of contact with their email address and the location code where they work.

Appendix A

Description of Acronyms

Acronym	**Description**	**Definition**
106 or Form 106	Prisoner Movement Request	Record request for prisoner movement from one facility to another.
BOP	Federal Bureau of Prisons	
eDes	eDesignate	OFDT System used to electronically flow paperwork while detainees are going through the Federal court process and until delivered to their designated facility.
ICE	U.S. Immigration and Customs Enforcement	Principal investigative arm of the U.S. Department of Homeland Security (DHS). Created in 2003 through a merger of the investigative and interior enforcement elements of the U.S. Customs Service and the Immigration and Naturalization Service.
ITD	Information Technology Division	USMS IT Division.
JDIS	Justice Detainee Information System	USMS system that contains prisoner booking data and daily operations in the USMS district offices.
JPATS	Justice Prisoner and Alien Transportation System	JPATS is not an electronic system but is a Division of the USMS that coordinates prisoner movements, air and ground, and also owns and operates a fleet of aircraft to transport prisoners.
OFDT	Office of the Federal Detention Trustee	Mission is to achieve efficiencies and cost reduction and avoidance in detention through process and infrastructure improvements.
PIA	Privacy Impact Assessment	
SENTRY	Inmate Management System	BOP’s real-time information system consisting of various applications for processing inmate information and for property management.
UFMS	Unified Financial Management System	DOJ’s Financial System.
USMS	United States Marshals Service	
USMS-Net	USMS Network	USMS-Net is a USMS general support system that provides USMS offices with information technology resources.