United States Marshals Service

Privacy Impact Assessment
for the
Justice Detainee Information System (JDIS)

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

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 25, 2013

(March 2012 DOJ PIA Form)

Section 1: Description of the Information System

The Justice Detainee Information System (JDIS) supports the responsibilities of the US Marshals Service (USMS) Investigative Operations Division (IOD), Prisoner Operations Division (POD), and Judicial Security Division (JSD). JDIS is designed to serve the needs of USMS criminal investigators, administrative analysts, and supervisory personnel, and the system provides each division with the information management tools to help apprehend fugitives, track and manage the custody and transportation of prisoners, conduct authorized criminal investigations, protect the federal judicial process, manage courthouse security, and process and manage inappropriate communications and/or threats to USMS protectees.

The IOD is primarily responsible for the oversight of the USMS fugitive apprehension program. They investigate and prosecute high-level money laundering and narcotics organizations, track fugitives who flee the territorial boundaries of the US, and have the statutory responsibility to extradite international and foreign fugitives after they are captured. They provide tactical and strategic intelligence assistance in support of criminal investigative operations. Through its interagency fugitive task forces, international operations, information sharing programs, and close cooperation with other federal, state, and local law enforcement agencies, IOD facilitates the timely apprehension of dangerous fugitives and helps preserve the integrity of the criminal justice system.

The POD is responsible for the national operational oversight of all detention management matters pertaining to individuals remanded to the custody of the Attorney General. They ensure the secure care and custody of these individuals through several processes to include sustenance, secure lodging and transportation, evaluating conditions of confinement, providing medical care deemed necessary, and protecting prisoner's civil rights through the judicial process.

The JSD's mission is to provide world class service to members of the federal judiciary by providing oversight, training, and operational support to 94 federal judicial district courts and 12 circuit courts. JSD is the central repository for threat and intelligence information pertaining to judicial security. JSD is responsible for all the security monitoring systems in federal buildings. JSD supports the protective mission of the USMS by collecting, analyzing, and disseminating information and protective intelligence, both classified and unclassified, in the form of threat assessments, briefings, and information bulletins.

The management functionality of JDIS is geared toward the responsibilities of headquarters (HQ) management. Example services include monitoring workload, measuring performance, allocating resources, monitoring jail and medical bills for USMS prisoners, managing USMS contracts with federal and private facilities, and managing and submitting requests for court security equipment and contract security personnel. JDIS is not a financial system and does not process or store financial data, except in the Prisoner Operation's tool.

For investigative support, JDIS contains information related to criminal offenders, missing persons, the tracking of fugitives, serving of warrants (from issuance to apprehension of the violator), and analysis in support of investigative operations, fugitive task forces, international operations, and

information sharing programs with other federal, state, and local law enforcement agencies. Records are accessed and updated as investigations are conducted about warrants for the subject, investigative details, court records and proceedings, USMS bookings of the subject, and status of the individual. Categories of individuals encompassed include those for whom federal warrants have been issued, individuals for whom state or local warrants have been issued when the warrant is part of a USMS-sponsored multi-agency task force, individuals suspected in a state's case that has been adopted by a USMS-sponsored task force, individuals for whom the USMS is conducting a criminal investigation or aiding in a criminal investigation by another law enforcement agency, sex offender registrants, missing persons (including children), and other persons related to a case such as witnesses, informants, sources, relatives, and associates. Data collected may include a wide variety of case information pertaining to a warrant, crime, fugitive, sex offender, or missing person matter, including biographical and biometric data, physical description, nature of the offense, criminal history, investigative reports, investigative notes, and witnesses' and other persons' statements.

JDIS also contains information relating to the apprehension and tracking of all prisoners/ detainees in USMS custody (under the U.S. Marshal for the respective district). JDIS helps manage the movements for prisoners/detainees in federal custody for the USMS and Bureau of Prisons (BOP) between federal courts. When a prisoner/detainee is committed to the custody of the USMS, the system is used to track transportation, housing, and care of the prisoner. (The USMS Automated Booking Station (ABS) is a major component of the system.) Categories of individuals encompassed include arrestees, fugitives, prisoners, and other individuals under custody of the USMS, other persons related to a case such as witnesses, informants, sources, relatives, associates, and attorneys, prisoner health care services providers under the USMS Managed Health Care Contract, USMS personnel (including employees, detailees, task force members, and contractors) working a custody/detention matter, and non-USMS law enforcement contacts. The system may include any and all information necessary to complete related administrative processes, safekeeping, health care, and disposition of individual federal prisoners/detainees in USMS custody, together with any related records generated during such custody. This can include a compilation of basic information on each individual taken into USMS custody including identifying data, reason for custody, court, confinement, and release information, relatives and associates information, transportation requests, incident reports, information identifiable to informants, protected witnesses, and confidential sources, and contact information for law enforcement personnel. System records also may include health care information about prisoner/ detainee medical problems, issues, or treatment, health-care providers, and billing records.

JDIS also gives JSD the ability to manage protective investigations and courthouse and other facilities security resources, conduct threat assessments and investigations, and gather and disseminate information and intelligence to ensure that justice can be administered without fear or coercion. This includes the capability to provide guidance, oversight, and coordination to the district offices that investigate threats and inappropriate communications directed to the federal judiciary, U.S. Attorneys and other court officers. Categories of individuals encompassed include those who pose a threat to USMS protectees, or who may have inappropriately communicated with or directly threatened, including federal judges, prosecutors, other court officials, U.S. Marshals, deputies, other law enforcement officers, courtroom security, and federal property and buildings staff; associates of the threat or inappropriate communication initiator; individuals reported by state or local agencies to the

USMS who have threatened to harm state or local judicial officials; and other individuals associated with persons or areas of protective interest. Data collected may include information related to the inappropriate communication or threat, including type of communication, the means by which it was issued, and information contained in the communication such as dates, locations, and events; analysis of the communication or threat and other internal USMS correspondence relating to the communication; biographical data on persons related to the matter; criminal history information; and other relevant investigative information including skills related to the nature of the threat and identifying information for assessing the potential threat of individuals who may be present in areas of USMS protective interest.

JDIS also maintains information to help the JSD accurately assess and manage the individual security needs of protectees subject to direct threats, including developing protective measures and advance planning of specific security assignments. With the information collected, USMS officials determine and carry out operating plans, funding, personnel assignments, and any special resources needed to counteract specific threat situations. Individuals encompassed include those who have been directly threatened or are subject to violent threat by virtue of their responsibilities within the judicial system, e.g., U.S. Attorneys and their assistants, federal jurists, and other court officials. Data collected may include case number, name of protected subject, name of control district and district number, type and source of threat and the means by which the threat was made, descriptive physical data of the protectee, and other information to identify security risks and plan protective measures in advance of or during periods of active protection, e.g., individual practices and routines, including associational memberships. Information regarding the expenditure of funds and allocation of resources assigned to the protectee may also be included to enable officials to develop operating plans to counteract threat situations

JDIS may also contain biographical and work related information on USMS personnel (including employees, detailees, task force members, and contractors) and non-USMS law enforcement contacts involved in a particular matter. In addition, JDIS maintains information on system users for access authentication and audit purposes.

Access to JDIS is restricted to USMS personnel and supporting contract employees who have a need for the performance of their duties. Access to personnel of federal and state agencies is restricted to those individuals who are covered by an intra-agency Memorandum of Understanding (MOU) and/or a Service Level Agreement (SLA) which set forth the rules of engagement for information sharing between an external information system and JDIS.

Information is retrieved via a secured login session, and reports may be printed where appropriate. Information is retrieved by name or personal identifier such as a social security number, a USMS registration number, or other identification number assigned to the individual. JDIS is a major application for USMS. First-time users must submit a USM-169J form to request a JCON account login name and password and have appropriate role(s) assigned to the account. Access to information in JDIS is controlled by login accounts, which grant certain permissions based on user role(s).

All JDIS online sessions are secured via Secure Socket Layer (SSL)

JDIS interconnects with other Department of Justice component systems for sharing information regarding fugitives, for booking information and designation of custody, and with other systems for purpose of ensuring medical care of prisoners.

Section 2: Information in the System

2.1 Indicate below what information is collected, maintained, or disseminated. (Check all that apply.)

Identifying numbers					
Social Security	X	Alien Registration	X	Financial account	X
Taxpayer ID	X	Driver's license	X	Financial transaction	X
Employee ID	X	Passport	X	Patient ID	X
File/case ID	X	Credit card			
Other identifying numbers (specify): FBI, prisoner/detainee, warrant, judicial record, incident report, and property numbers					

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

Work-related data					
Occupation	X	Telephone number	X	Salary	X
Job title	X	Email address	X	Work history	
Work address	X	Business associates	X		
Other work-related data (specify): Employee ID/ badge number, fax number, telephone number, email address/message routing data					

Distinguishing features/Biometrics					
Fingerprints	X	Photos	X	DNA profiles	
Palm prints		Scars, marks, tattoos	X	Retina/iris scans	

Distinguishing features/Biometrics					
Voice recording/signatures		Vascular scan		Dental profile	
Other distinguishing features/biometrics (specify):					

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

Other information (specify)
All manner of investigative/case information relevant to a particular matter as described in Section 1

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

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

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

Non-government sources					
Members of the public	X	Public media, internet	X	Private sector	X
Commercial data brokers	X				
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 include over-collection of information, collecting inaccurate information, and unauthorized access to and modification of data. The USMS investigates and attempts to verify information collected from all sources. The USMS has limited the collection of personally identifiable information to that which is necessary to enable users to access JDIS or to effectuate its mission to ensure accurate and timely serving of warrants, apprehension of fugitives, tracking of threats to protectees, managing information to provide for the adequate care, custody and medical services for federal prisoners in USMS custody, and for the management of courthouse security and resources. When conducting a criminal investigation, it is not feasible to collect information from the subject thereof. Therefore, it is necessary to collect information about the subject from various third party sources. The verification of the accuracy of information to the greatest extent possible is the means by which the risks are mitigated.

The risks associated with unauthorized access and modification is mitigated through user access security controls and audits. In accordance with federal guidelines, JDIS 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 risks were assessed, the results formally documented, and authority to operate the system was obtained. User's access and modification privileges are role based with each user assigned a unique password and the system generates an audit trail.

For additional discussion of these risks and mitigations, please see Subsections 3.5 and 4.2 and Section 6.

Section 3: 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	X	For civil enforcement activities
X	For intelligence activities	X	For administrative matters

X	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
X	For litigation		
	Other (specify): Prisoner/detainee health care; judicial protection		

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 in Section 1, the personally identifiable information (PII) collected and stored in JDIS is critical to the support of law enforcement initiatives of the USMS. The personally identifiable information such as SSN, photographs, and fingerprints are unique to the subjects and are necessary, in conjunction with other information, to identify individuals to ensure accurate and timely serving of warrants, the apprehension of fugitives, tracking of threats, the management of the care and custody and medical services for federal prisoners in USMS custody, and protection of judicial personnel and facilities. Employee information is necessary for tracking investigatory or administrative assignments and responsibilities relative to the subjects of investigation, prisoners in USMS custody and the security of courthouses or USMS facilities. System user and audit information is necessary to ensure the security of the system.

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	5 U.S.C. 301 18 U.S.C. 2250,3149, 3193, 3604, 3621, 4002, 4006, 4086, 4285 28 U.S.C. 509, 510, 561–569 42 U.S.C. 16941 44 U.S.C. 3101
	Executive Order	
X	Federal Regulation	28 CFR 0.111 and .111A

X	Memorandum of Understanding/agreement	Access to personnel of federal and state agencies is restricted to those individuals who are covered by an intra-agency Memorandum of Understanding (MOU) and/or a Service Level Agreement (SLA) which set forth the rules of engagement for information sharing between an external information system and JDIS
	Other (summarize and provide copy of relevant portion)	

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.)

JDIS General Prisoner/detainee records are destroyed after 10 years, or sooner, if ordered by the Court. Paper documents and automated files such as invoices maintained by contractors will be maintained in accordance with the General Records Schedule 6, Item 1a (Accountable Officers' Files), as published by National Archives and Records Administration (NARA), unless a longer retention period is necessary because of pending administrative or judicial proceedings. JDIS warrant information/criminal investigation records are destroyed after 55 years. JDIS inappropriate communications and threat records maintained by USMS headquarters are destroyed one year after the initiator of the threat or inappropriate communication is no longer active or the case has been closed. District files are destroyed five years after the initiator of the threat or inappropriate communication is no longer active or the case has been closed.

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.)

Potential risks include acting upon erroneous or inaccurate information, unauthorized access to and modification of data, and improper disclosure. All USMS personnel and personnel with approved access through MOU are required, on an annual basis, to take the "Department of Justice (DOJ) Information Technology Computer Security Awareness Training (CSAT) course covering computer security and information privacy via the DOJ Intranet site LearnDOJ. All personnel acknowledge the DOJ's Rules of Behavior. Users are limited to specific roles based on their position, any access to JDIS must be approved by the user's supervisor and all accounts are validated annually. Component personnel receive Privacy Act guidance annually which includes guidance regarding records security, retention and disposal as well as guidance regarding disclosure of protected records. JDIS retains records in accordance with guidance listed in 3.4 of this document. JDIS has not reached the milestone for destroying records to date. Manual purging only occurs when directions from the US Courts to USMS through the Office of General Counsel has transpired. At that time, USMS Information

Technology Department Staff will purge those records.

Please see Subsections 2.3, 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	X	X	
DOJ components	X		X	Bureau Of Prisons, Federal Bureau of Investigations, Office of the Federal Detention Trustee, United States Attorney's Office
Federal entities	X		X	El Paso Intelligence Center, Department of State, Veteran Affairs, Social Security Administration, Housing and Urban Development, Transportation Security Administration
State, local, tribal gov't entities	X			New York/New Jersey High Intensity Drug Trafficking Area,
Public	X			
Private sector	X			CVS/Caremark
Foreign governments	X			
Foreign entities	X			
Other (specify):	X			Interpol

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.)

Some of the specific controls that address disclosure of data include the following:

Personnel Security – All employees (government and contractors and personnel approved by memoranda of understanding) are required to be adjudicated prior to getting access to the JDIS. They are required to read and acknowledge the DOJ rules of behavior (ROB) and complete the annual Computer Security Awareness Training (CSAT). Users are limited to specific roles based on their position, any access to JDIS must be approved by the user's supervisor and all accounts are validated annually.

Physical and Environmental Protection – USMS controls all physical access points to facilities. The access for Headquarters space is controls by the SSO. Employees are required to display a building pass and access points are protected by surveillance cameras, alarms systems, access control pushbutton locks, and digital keypads. The office of Courthouse Management provides physical security for all districts courtrooms. They evaluate vulnerabilities of the facilities and provide the physical security necessary including cameras, monitors, intercoms, conduit and wiring, locking devices, alarms security consoles, and duress alarms for USMS staff.

Access Controls – Supervisors complete User Access Request Forms (USMS 169J) 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 assigned roles. Separation of duties is enforced so that functions of significant criticality or sensitivity are subject to control by more than one individual.

Configuration Management – Security settings are configured to the most restrictive mode consistent with information system operational requirements. Any configuration changes have to be reviewed and approved by the Configuration Control Board (CCB) prior to implementation.

Audit and Accountability – Audit logs are generated for the system. They are reviewed weekly for any suspicious or anomaly activity. Any suspicious or anomaly activities are reported to the Chief Information Security Officer (CISO) for further investigation

Also, please see Subsection 3.5 and Section 6.

Section 5: 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.)

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7.	
X	Yes, notice is provided by other means.	Specify how: By this PIA. Also, a security assessment is provided to Judicial Protectees; however, they are not required to fill it out.

X	Further notice is not provided.	Specify why not: Providing more specific information is typically impracticable and unwarranted for persons in USMS custody, who are fugitives, or who otherwise may be the subjects of law enforcement records

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

X	Yes, individuals have the opportunity to decline to provide information.	Specify how: A security assessment is provided to Judicial Protectees, however, they are not required fill it out. If they do not fill it out, their information will not be inputted.
X	No, individuals do not have the opportunity to decline to provide information.	Specify why not: For other persons, such opportunity is typically impracticable and unwarranted (e.g., for persons in USMS Custody, who are fugitives, or who otherwise may be the subjects of law enforcement records).

5.3 Indicate whether and how individuals have the opportunity to consent to particular uses of the 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 opportunity is typically impracticable and unwarranted for persons in USMS Custody, who are fugitives, or who otherwise may be the subjects of law enforcement records

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.

USMS systems of records relating to the apprehension of fugitives, tracking and managing the custody and transportation of prisoners/detainees, conduct of authorized criminal investigations, and protection of the federal judicial process have been exempted from the specific notice requirements of

Privacy Act subsections (e)(2) and (e)(3). (See 28 CFR 16.101.) However, individuals with records in these systems are provided general notice via this PIA and the system of records notice published in the Federal Register and discussed in Section 7 Individuals in these systems of records do not have the opportunity and/or right to decline to provide the information. In conducting criminal law enforcement investigations it is frequently necessary to collect information from sources other than the individual being investigated. However, the purpose for collection of individual information and the uses are limited as provided by the Privacy Act and the applicable System of Records Notice which has been published in the Federal Register. Also, where practicable and appropriate, certain categories of individuals may be provided with specific notice and opportunity to decline to provide information.

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: 06/29/2012 This is a USMS owned and operated Major Application 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. 06/29/2012
X	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: Continuous Monitoring is performed on an annual basis for USMS systems. Also all Core controls are updated as directed by DOJ on an annual basis. Scanning is done on a monthly basis and patched monthly. All change requests are submitted to the USMS Change Control Board (CCB) and must obtain Senior Management approval prior to being released in production. Scanning is done pre and post implementation to ensure no new vulnerabilities were presented. Audit logs are sent to ArcSight for monitoring by the ITD Security Staff. USMS has multiple layers of network security to include firewalls and intrusion detection systems that are monitored by the DOJ JSOC thus providing an additional layer of security in the event of an unauthorized attempt to gain access.
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: USMS ITD Security reviews the activities by users via the server syslog and by the application logs. ITD Security also conducts monthly vulnerability scans to ensure the risk are identified and mitigated within a timely manner. All change requests are submitted to the USMS Change Control Board (CCB) and must obtain Senior Management approval prior to being released in production. Scanning is done pre and post implementation to ensure no new vulnerabilities were presented. Continuous Monitoring is performed throughout the fiscal year. USMS tests DOJ directed core controls on an annual basis and performs recertification of the system every three 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: JDIS is a role based application. As such, all users in the application are vetted and have approval to perform their job related duties. Only those with need to know are allowed access to JDIS via the USMS 169J. Application, Operating System and Database logs are routed from JDIS to ArcSight. Those logs received by ArcSight are viewed by the USMS ITD Security Staff. Organizational defined events are parsed and delivered to the Information System Security Officer to review. Alerts are sent daily and monitored as such. Privileged user access is monitored via ArcSight to capture any unauthorized elevated activities.	
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:	
	X	General information security training
		Training specific to the system for authorized users within the Department.
		Training specific to the system for authorized users outside of the component.
	X	Other (specify): Rules of Behavior for General Users and Rules of Behavior for Privileged Users must be signed prior (as applicable) to be granted access to the USMS Network.

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

Access to JDIS is controlled through "roles" and "district assignments" for each user account. The system currently has 38 distinct roles for assigning distinct access privileges ranging from read-only to administrative rights within the different JDIS modules. A given user account can be assigned one or more roles. If the account has two roles, one with read-only access and another with read/write access, the user will have the higher read/write privileges within the module. Whatever the case, a user will only receive the lease privileges needed to perform their assigned duties.

In addition to "roles", some access privileges also require a given user account to have a specific "district assignment". For example, access to all functionality within the Inappropriate Communications module requires the user account to be granted both the correct role and be assigned to District T00. In addition, user accounts assigned to special HQ or Headquarters districts will have the ability to change between different USMS districts. User accounts and assigned roles will be maintained within the JDIS system by authorized account managers on the ITD Help Desk based on approved user account request (UAR) forms. Department supervisors will be responsible for identifying role(s) and approving UAR forms for their staff needing access to JDIS. User accounts inactive for 90 days are disabled. USMS conducts an annual account review of user accounts to ensure only valid users maintain access to USMS systems.

JDIS consists of Oracle Databases and as such utilizes the encryption features installed within Oracle and are part of the USMS Baseline to protect data at rest. Java Database Connectivity (JDBC) is used to encrypt data transmitted to and from the database. Two factor authentication has been

implemented for access to the USMS Network. USMS users must authenticate to the network before being granted access to JDIS. Non USMS users must have prior authorization. Those users have rules placed within the firewall allowing access from their IPs to the USMS network. Once they have connected to the application, they must supply user name and password. Only those IPs approved by the Non USMS organization and USMS are allowed access through the firewall.

Section 7: 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: USM-005, U.S. Marshals Service Prisoner Processing and Population Management/Prisoner Tracking System (PPM/PTS), Federal Register: June 18, 2007 (Volume 72, Number 116) Notices, Pages 33519-33522. USM-007, Warrant Information System (WIN), Federal Register: March 5, 2007 (Volume 72, Number 42), Notices, Pages 9777-9779. USM-009, Inappropriate Communications/Threat Information System (IC/TIS), Federal Resister June 18, 2007 (Volume 72. Number 116, Notices, Pages 33524-33526. USM-011, Judicial Protection Information System, Federal Register June 18, 2007 (Volume 72 Number 116) Notices, Pages 33527-33529. Copies of these notices are available on the DOJ website at this link: http://www.justice.gov/opcl/privacyact.html#USM .
	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.

To access JDIS, a person must have an account ID and password. Then depending upon the assigned user role, the user is able to access the information stored within JDIS. Information is retrieved by name or personal identifier such as a social security number, a USMS registration number, or other identification number assigned to the individual