Privacy Impact Assessment
for the

OneDOJ System
(formerly the Regional Data Exchange System (R-DEx)

August 7, 2008

Responsible Officials
Harrell Watkins
Deputy Director, E-Government
Justice Management Division/OCIO
(202) 514-0281

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

Approving Official
Kenneth P. Mortensen
Acting Chief Privacy and Civil Liberties Officer
Department of Justice
(202) 514-0208

Introduction

OneDOJ, a system, also known as the Regional Data Exchange system (R-DEx), is a data repository that contains controlled unclassified information (CUI) to include criminal law enforcement information from the following Department of Justice (DOJ or the "Department") investigative components: the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), Federal Bureau of Prisons (BOP); the Drug Enforcement Administration (DEA), the Federal Bureau of Investigation (FBI), and the United States Marshals Service (USMS), herein referred to as contributing agencies. The system also will (in the near future) contain criminal booking information from the Joint Automated Booking System (JABS), which is utilized by the five components and is operated by Justice Management Division (JMD) as a Department-wide solution. JABS also contains a small percentage of criminal booking records from other Federal, State, and Local Law Enforcement Agencies, as such agencies use the JABS system to collect booking information about individuals.[1]

The information in the system is contributed by the Department law enforcement entities and maintained in this system for the primary purpose of sharing criminal law enforcement information across the Department and, secondarily, with state/local/tribal law enforcement agencies in order to more effectively investigate, disrupt, and deter criminal activity, to protect the nation's security. This system is accessible to specific users in the Department's components and organizations that have an operational need and criminal law enforcement mission. The data in the system is also made available to other federal, state, local and tribal law enforcement organizations in a more limited capacity, pursuant to individual memoranda of understanding.

OneDOJ has limited data analysis capabilities that comprise of link charting and geo-mapping. A user (an analyst or investigator) enters search parameters relevant to a specific purpose (a case) and obtains search results. The user can then select a number of results and request that the tool produce a link chart of these results. The chart is based on simple matching of the information contained in the records selected by the user. The geo-mapping capability is based on geo location information contained in the records. The user may select records that have geo-location indicators and request to map them. The system produces a map with specific locations from the selected records. OneDOJ does not produce any new records. All user operations are read-only and users are not permitted to copy, print, or reproduce in any other form, information contained in or extracted from OneDOJ.

[1] There is also one set of local data still contained within the OneDOJ data set. DOJ still hosts the original pilot data for the St. Louis region. This also includes data from the Illinois State Police. This is not standard practice and will not occur with other local law enforcement entities. DOJ is working to move the local data to a locally controlled system.

Section 1
The System and the Information Collected and Stored within the System.

1.1 What information is to be collected?

The system consists of copies of controlled unclassified information (CUI) to include criminal law enforcement records collected and produced by the ATF, the BOP, the DEA, the FBI, and the USMS, including: investigative reports and witness interviews from both open and closed cases; criminal event data (e.g., characteristics of criminal activities and incidents that identify links or patterns); criminal history record information (e.g., history of arrests, nature and disposition of criminal charges, booking information, sentencing, confinement, and release); and biographic information about criminal offenders (e.g., name, address, date of birth, birthplace, physical description). The system also consists of audit logs that contain the date, time, subject and originating account of all internal and external user queries made of the system. Aside from the audit logs, as noted above, all information in OneDOJ represents copies of files from source component systems. OneDOJ has limited data analysis capabilities that comprise of link charting and geo-mapping. A user (an analyst or investigator) enters search parameters relevant to a specific purpose (a case) and obtains search results. The user can then select a number of results and request that the tool produce a link chart of these results. The chart is based on simple matching of the information contained in the records selected by the user. The geo-mapping capability is based on geo location information contained in the records. The user may select records that have geo-location indicators and request to map them. The system produces a map with specific locations from the selected records. OneDOJ does not produce any new records. All user operations are read-only and users are not permitted to copy, print, or reproduce in any other form, information contained in or extracted from OneDOJ.

Individuals covered by this system include individuals who are or were referred to in closed and pending investigative matters conducted by the ATF, the BOP, the DEA, the FBI and the USMS. These records may include personally identifiable information regarding a person's possible involvement in criminal activity. When the JABS data is added to OneDOJ in the future, these records will contain arrest information, photos and fingerprints for any individual taken into custody by federal, state, and local law enforcement agents.

According to the Law Enforcement Information Sharing Plan (LEISP) strategy document (October 2005), information that can be shared is related to three law enforcement operational capabilities to include tactical, investigative, and analytical. DOJ policy specifically restricts the sharing of certain types of sensitive information that may jeopardize the safety of the investigator or the actual investigation. The Department may not share grand jury or Title III of the Omnibus Crime Control and Safe Street Act of 1968 and Electronic Communications Privacy Act (ECPA) of 1986 information through OneDOJ. Title III, also known at the Wiretap Act, requires law enforcement to demonstrate probable cause to obtain a warrant for conducting wiretaps. The ECPA, an amendment to the Wiretap Act, extends protection to electronic communications. Information obtained as a result of wiretaps will not be shared through OneDOJ as it may jeopardize the safety of the investigator or the actual investigation. Additionally, other case information is not shared (based on agency policy) even if such information is

not classified. DOJ will routinely share law enforcement information through OneDOJ including tear lines of classified information, with all law enforcement partners with the exception of certain categories of information as identified by the Deputy Attorney General. Examples include the following:

- espionage and public corruption case information;
- information whose dissemination is prohibited under international or inter-agency agreements;
- information that would reveal sensitive undercover operations or sources and methods of information collection; and
- civil rights investigations involving color of law violations, internal investigations, and administrative cases.

Insofar as the system contains audit logs regarding inquiries, individuals who use the system to conduct such queries are also covered. Moreover, individuals and agencies who contributed information to the system are also identifiable as this functionality is essential to connect users for the purpose of collaboration and de-confliction of investigative matters. Contributor and data owner information includes the name of agency, name of specific contributor, contributor's email address and telephone number. Information contained within the audit log includes the user ID, system from which the user executed the query, and the name of user's agency.

1.2 From whom is the information collected?

Information is collected from individuals and generally by the law enforcement personnel in the course of their tactical, investigative, and analytical activities.[2] Law enforcement personnel also collect contact information from data owners or contributors so as to verify information when necessary.

The information in OneDOJ is a shareable subset of the criminal law enforcement files and data of the participating DOJ components (i.e. ATF, BOP, DEA, FBI, and USMS), which is copied and maintained in OneDOJ for use across the Department. This copied subset of information contains information on suspects and associates of suspects and does not include protected sources and methods. The data in JABS is whatever information can be collected on the individual at the time of booking. JABS is used by other federal law enforcement agencies at the time of booking. In some instances, the federal agents hand over the individual to the US Marshals for booking and processing. Depending on the situation, the USMS may also enter the individual into the system, and then the record is pushed to Criminal Justice Information Services (CJIS) for inclusion in Integrated Automated Fingerprint Identification System (IAFIS), the master system for all fingerprints.

[2] See footnote 1.

Section 2
The Purpose of the System and the Information Collected and Stored within the System.

2.1 Why is the information being collected?

The system is maintained for the purpose of ensuring that Department of Justice criminal law enforcement information is available for users at all levels of government so that they can more effectively investigate, disrupt, and deter criminal activity, including terrorism, and protect the national security. OneDOJ furthers this purpose by consolidating certain law enforcement information from other Department of Justice systems, as well as certain state and local law enforcement information, in order that it may more readily be available for sharing with other enforcement entities.

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

Authorities for the Department to enter into sharing agreements include 28 U.S.C. §§ 533 and 534; Presidential Decision Directives 39 and 62; and E.O. 13,388 and the Intelligence Reform and Terrorism Prevention Act (IRTPA) 2004, Section 1016 Information Sharing. Executive Order 13356 established the Information Sharing Council (ISC) and the Information Sharing Environment (ISE). The IRTPA also identified key agencies to deliver the infrastructure needed to operate and manage the ISE of which, the Attorney General and by association the Department of Justice, was identified as the lead Agency for Law Enforcement. OneDOJ is the primary mechanism for accomplishing this sharing mandate. Each DOJ component is authorized to collect information in the course of their missions to protect this country from criminal activities, to capture fugitives and to incarcerate convicted felons.

In addition, the Department published the Law Enforcement Information Sharing Program (LEISP) in December of 2005. Deputy Attorney General James B. Comey issued a memorandum in support of the pilot program in Seattle and Deputy Attorney General Paul J. McNulty issued a subsequent memo in December 2006. This memorandum states the directive to each of the components to share information utilizing the OneDOJ system.

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.

Misuse of information and unauthorized access to the information were identified as privacy risks. These risks are mitigated by the manual controls put in place at the component level, the access controls in the OneDOJ tool and by the nature of police work. The technology is such that the local users do not take possession of the data, rather they have results returned to their query tool for temporary viewing. Once users exit their session, they may not capture the data. Users are not permitted to print, copy, or electronically retain information without first obtaining permission from the contributing agency in accordance with Memoranda of Understanding. DOJ is using web-based technology, and the use of

caching allows us to provide temporary access to the data for a specified query. The same is true in reverse, when federal users access non-federal data, it is viewable only, until the end of the browser session. Those organizations participating in OneDOJ do not put their entire data set into the sharing system. Instead, they control extracts from their source systems to exclude certain types of sensitive information. In addition, the culture in law enforcement is to protect information closely, because of the need to protect fellow officers and prevent interference with ongoing investigations; therefore some risk is self-managed by the users who will track others that query information on their case.

Information in this system is safeguarded in accordance with federal laws, statutes, rules, and policies, including the Department's automated systems security and access policies. Paper files, data, and technical equipment are maintained in buildings with restricted access. Single users cannot add a new item without supervisor approval, which in some components is system controlled and in others it is a standard practice. Federal records in this system in all formats are disposed of in accordance with records retention schedules approved by the National Archives and Records Administration. While there is not a retention schedule specifically applicable to OneDOJ, each contributing agency is responsible for its data and records are maintained in accordance with the retention schedule applicable to the particular records maintained by the component. OneDOJ maintains complete audit logs for all adds, edits, and deletions of records. Audit logs are reviewed every three years, but are made available for review should a particular agency suspect misuse of information.

Passwords, password protection identification features, and other system protection methods also restrict access to information in this system. Only DOJ criminal investigative/analytical personnel and criminal investigative/analytical personnel from other federal, state, local or tribal law enforcement agencies by express agreement are permitted access to the system.

Several administrative and technological controls secure the information contained within OneDOJ. The Security Administrator and the System Administrator are two distinct roles within the OneDOJ application. The Security Administrator is responsible for viewing, monitoring, and archiving security logs and audit trails and has the ability to add, change, and delete users and adjust or remove their system access privileges. The System Administrator is responsible for the maintenance and operation of the system as a whole, including backing up the system and its recovery.

OneDOJ information will be used for official criminal justice purposes only. OneDOJ information cannot be accessed or used for any other noncriminal justice purpose, including general licensing, employment, eligibility for federal or state benefits, and background investigations. OneDOJ information may not be disclosed by a participating agency in response to a request made under any state or local information access law. Information in OneDOJ will only be disclosed by the contributing Agency in accordance with federal law, including the Freedom of Information Act and the Privacy Act of 1974.

User limitations were created to ensure that OneDOJ is used for law enforcement purposes only and only law enforcement personnel with a “need to know” the information contained within the system will have access to the OneDOJ system.

Section 3
Uses of the System and the Information.

3.1 Describe all uses of the information.

The Department maintains the OneDOJ system to provide authorized users with access to criminal law enforcement information collected by the Department's investigative components. Additionally, the system is maintained to provide the Department's shareable criminal law enforcement information to its federal, state, local and tribal partners in a thorough and deliberate manner. Through memoranda of understanding, OneDOJ connects with regional criminal law enforcement information consortia and organizations. The technical connections use secure virtual private networks to connect the local agency with the CJIS operations center, where the OneDOJ system is hosted. The information is shared in a systematic and ongoing manner to maximize the benefits of information gathering and analysis needed to respond to criminal threats, to support law enforcement activities, and to enhance public safety.

The Criminal Justice Information Services Division of the FBI is the system's executive agent. Each participating DOJ component contributes information to OneDOJ. Other federal, state and local law enforcement entities will use OneDOJ to make queries of structured and unstructured, free-text data regarding individuals under investigation for criminal activity.

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.)

OneDOJ has limited data analysis capabilities that comprise of link charting and geo-mapping. A user (an analyst or investigator) enters search parameters relevant to a specific purpose (a case) and obtains search results. The user can then select a number of results and request that the tool produce a link chart of these results. The chart is based on simple matching of the information contained in the records selected by the user. The geo-mapping capability is based on geo location information contained in the records. The user may select records that have geo-location indicators and request to map them. The system produces a map with specific locations from the selected records. OneDOJ does not produce any new records. All user operations are read-only and users are not permitted to copy, print, or reproduce in any other form, information contained in or extracted from OneDOJ.

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

OneDOJ is a repository of the Department's sharable law enforcement criminal investigative information. The data contained in the system are limited to copies of data individually collected and managed by the ATF, BOP, DEA, FBI and USMS. No data are collected specifically for the system.

The accuracy and the integrity of the data in OneDOJ are the responsibility of the agency contributing the data. Each of the Department's contributing agencies is also responsible for making

reasonable efforts to assure that the data are accurate, complete, timely and relevant for agency purposes. Users must also corroborate information in OneDOJ prior to using as a basis for action against someone. Each contributing agency is also responsible for updating their open investigative records as new information becomes available. As such happens, the data in OneDOJ will also be updated.

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)?

Federal records in this system in all formats are disposed of in accordance with records retention schedules approved by the National Archives and Records Administration. While there is not a retention schedule specifically applicable to OneDOJ, each contributing agency is responsible for its data and records are maintained in accordance with the retention schedule applicable to the particular records maintained by the component.

3.5 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

The DOJ has implemented administrative and technological security controls and measures to protect the information collected by law enforcement agencies, both while in storage and in transit. These measures are designed to thwart unauthorized access and inappropriate disclosure. The OneDOJ system includes robust audit capabilities. OneDOJ maintains complete audit logs for all adds, edits and deletions of records. OneDOJ components have the ability to periodically review the audit logs to ensure appropriate access to and use of information. Audit logs are reviewed every three years, but are made available for review should a particular agency suspect misuse of information

The various memoranda of understanding used to share OneDOJ data with other federal, state, local and tribal law enforcement agencies outlines policies and procedures for the handling and use of OneDOJ information. The policies and procedures cover the actions of contributing agencies (e.g., data accuracy), as well as how recipients may use OneDOJ data.

These memoranda of understanding also include sanctions for misuse of the system and/or data. Sanctions can be applied to an individual or entire agency, depending on the circumstances and severity of the misuse. Each DOJ component that contributes records to OneDOJ will periodically audit access by other agencies to ensure appropriate use of the information. Each participating DOJ component will review its own use of the OneDOJ system and will take action to address any misuse.

Each contributing agency is responsible for the actions of its users, and sanctions will be applied for intentional or repeated misuse of the data contained within and/or the system itself. The Department's Law Enforcement Information Sharing Program Coordinating Committee (LCC), under the leadership of the Deputy Attorney General, is the governance body for OneDOJ. The LCC determines appropriate sanctions. The LCC is comprised of senior operational leaders of each component and includes representation for DOJ prosecutors/attorneys.

The contributing agency and DOJ will make its best efforts and exercise due diligence to ensure that information in OneDOJ was not contributed or maintained in violation of any applicable law by the contributing agency.

Section 4
Internal Sharing and Disclosure of Information within the System.

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

Internal components of the Department which share information include ATF, BOP, DEA, FBI, and USMS. The Executive Office of United States Attorneys and the United States Attorney's Offices across the country have access to the database as required.

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

The information is criminal law enforcement information collected by the Department's investigative components. Additionally, contact information for the owner of information shared is typically part of the information that is returned to the user. The purpose is to maximize the benefits of information gathering and analysis needed to respond to criminal threats, to support law enforcement activities such as investigative case de-confliction and coordination, and to enhance public safety.

4.3 How is the information transmitted or disclosed?

An authorized user retrieves data from OneDOJ based on a query of particular person, place or thing and the system identifying what documents contain the requested information. The user can then request to view the specific documents and/or elect to make direct contact with the agency contributing the data. The data are transmitted via the Department's internal secure network.

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

Misuse of information and unauthorized access to the information were identified as privacy risks.

OneDOJ information, including analytical products derived there from, may not be used as a basis for action or disseminated for any purpose or in any manner outside the contributing agency that accessed the information, unless that agency first obtains the permission of the contributing agency. Specifically included within this prohibition are any inclusion of OneDOJ information in an official investigative or case file, and any use of OneDOJ information in the preparation of documents such as affidavits, warrants, or subpoenas.

Immediate dissemination of OneDOJ information can be made without written permission if the agency that accessed the information determines that:

(a) there is an actual or potential threat of terrorism, immediate danger of death or serious physical injury to any person, or imminent harm to the nation's security; and

(b) it is necessary to disseminate such information without delay to any appropriate recipient for the purpose of preventing or responding to such a threat.

In order to mitigate privacy risks, FBI-CJIS personnel verify the user's role via email with the component points of contact. Users are re-vetted again throughout the duration of their system usage. CJIS will conduct performance audits on the system based on an established systems audit process, already in place for other CJIS systems and programs.. CJIS has established a system to triennially audit federal, state, local, and tribal agencies that operate workstations and/or have access to devices, mobile data terminals, or personal/laptop computers that have access to OneDOJ data to ensure compliance with state and/or FBI CJIS policy, federal directives, and federal regulations.

Section 5
External Sharing and Disclosure

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

The Criminal Justice Information Services Division of the FBI is the system's executive agent. Each participating DOJ component contributes information to OneDOJ. Other federal, state and local law enforcement entities (by agreement), can make queries of the data contained within OneDOJ regarding individuals they are investigating for criminal activity. External agencies do not contribute to or take possession of OneDOJ data. The federal, state, local, and tribal law enforcement partner vets, authorizes, and provides access to their investigators and/or analysts on their respective information sharing systems. The system is set up to allow them to query OneDOJ data without ingesting the data into their local system. Conversely, DOJ and its components vet, authorize, and provide access to their investigators and/or analysts to the OneDOJ system. A secure Virtual Private Network (VPN) is established across the Internet between the two systems. Additionally, standardized information exchanges using web services enable the two systems to conduct field specific and free-text searches on their respective systems

Through memoranda of understanding and approval of the LCC, OneDOJ information will be shared with federal, state and local law enforcement entities to enable them to more effectively investigate, disrupt, and deter criminal activity, including terrorism, and protect the nation's security.

Information from OneDOJ may be disclosed:

To a criminal, civil, or regulatory law enforcement authority (whether federal, state, local, territorial, tribal, or foreign) where the information is relevant to the recipient entity's law enforcement responsibilities.

To a governmental entity lawfully engaged in collecting criminal law enforcement, criminal law enforcement intelligence, or national security intelligence information for law enforcement or intelligence purposes.

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.

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 determines the records to be relevant to the proceeding.

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

To the news media and the public pursuant to 28 C.F.R. § 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.

To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. §§ 2904 and 2906.

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.

To such recipients and under such circumstances and procedures as are mandated by federal statute or treaty.

To complainants and/or victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of the investigation or case arising from the matters of which they complained and/or of which they were a victim.

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.

To any person or entity if deemed by the Department to be necessary in order to elicit information or cooperation from the recipient for use by the Department in the performance of an authorized law enforcement activity.

To any individual, organization, or governmental entity when it is necessary to notify them of a serious terrorist threat for the purpose of guarding against or responding to such a threat.

5.2 What information is shared and for what purpose?

Information shared outside of DOJ consists of copies of controlled unclassified information (CUI) to include criminal law enforcement records collected and produced by the ATF, the BOP, the DEA, the FBI, and the USMS, including: investigative reports and witness interviews from both open and closed cases; criminal event data (e.g., characteristics of criminal activities and incidents that identify links or

patterns); criminal history record information (e.g., history of arrests, nature and disposition of criminal charges, booking information, sentencing, confinement, and release); and biographic information about criminal offenders (e.g., name, address, date of birth, birthplace, physical description). In addition, contributor and data owner contact information including the name of agency, name of specific contributor, contributor's email address and telephone number are provided so as all users can verify information when necessary.

The system is maintained to present the Department's shareable criminal law enforcement information through a strategic and deliberate approach to its federal, state, local and tribal partners. In part, the Department uses access to OneDOJ to negotiate access to regional criminal law enforcement information consortia through memoranda of understanding defining access and privacy controls for sharing criminal law enforcement information.

The purpose of sharing criminal law enforcement information with its federal, state, local and tribal partners in a systematic and ongoing manner is to maximize the benefits of information gathering and analysis needed to respond to criminal threats, to support law enforcement activities such as investigative case de-confliction and coordination, and to enhance public safety.

5.3 How is the information transmitted or disclosed?

A user retrieves data from OneDOJ based on the user making a query for particular information and the system identifying what documents contain the requested information. The user can then request to view the specific documents. Records can be retrieved by the name and/or other identifier(s) of an individual.

Federal, state and local law enforcement entities will use OneDOJ to make queries of structured and unstructured, free-text data regarding individuals they are investigating for alleged criminal activity. Data are retrieved from OneDOJ through an encrypted virtual private network connecting the federal, state, local, and tribal law enforcement agencies.

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

For each sharing arrangement, a Memorandum of Understanding (MOU) for OneDOJ governs the use of the information that users may access in OneDOJ. Specifically, no law enforcement action may be undertaken until coordinated with the originator of the information in OneDOJ. In addition to the MOU, each user is required to read and sign a 'user rules of behavior' document that addresses the user's responsibility in the handling of system data. The MOU specifically cites the CJIS Security Policy, which is a widely accepted standard and followed by over 18,000 law enforcement agencies across the country. CJIS Security Policy requires the implementation of specific technical security controls, configuration management activities, and procedures for the documentation and notification of security incidents. It provides the minimum level of Information Technology (IT) security requirements determined acceptable for the transmission, processing, and storage of OneDOJ data. Partner agencies administer their own IT

Security Programs to fully and properly implement the requirements of CJIS Security Policy to safeguard the data contained within OneDOJ.

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

All OneDOJ users, including those accessing OneDOJ information through other systems, must receive training in the operation and proper use of the OneDOJ system. DOJ provided partial funding to Automated Regional Justice Information System (ARJIS) in San Diego to create re-useable training materials for local users who access OneDOJ. DOJ recommends, but does not require that other agencies or sharing initiatives use this material when connecting their sharing system to the OneDOJ database. CJIS, as the executive agent for OneDOJ is making "train the trainer" and "train the user" sessions available for our federal, state, local, and tribal information sharing partners. Rules regarding data use and the protection of Personally Identifiable Information (PII) as it pertains to the various memoranda of understanding must be provided during any training session. Some of the partners at the local level already have mandatory training requirements for their users, especially as it relates to compliance with 28 CFR Part 23, but this varies from jurisdiction to jurisdiction.

Each OneDOJ Memorandum of Understanding clearly articulates permissible uses of the data, and this document is shared widely with the partners so that all users have access to the agreed-upon language.

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

The audit logs in the OneDOJ system comply with DOJ and FBI-CJIS standards. They were built according to FBI-CJIS policies and track user activity throughout the system, including the individual queried, the time queried and any other activity during that session. The logs are built primarily for re-active re-creation of possible misuse; however, the log data is also used for notification purposes. If the point of contact for the information sets his case for "notification," when a local officer performs a query of the targeted individual in that case, the case point of contact will be notified via email. This feature is important for connecting officers, but it is also an important tool to prevent misuse of data. Plans are being created to perform regular audits of the system, but at this point in time, DOJ and FBI technical personnel perform random audits to see who is using the system and what type of results they are getting from the data.

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

External sharing of federal law enforcement data raises the potential for misuse of information, which is a privacy risk; however, this risk can be mitigated by performing regular reviews of audit data, by properly training users, and by putting reminder messages into the login screen. This information may

also be added to annual security refresher training, as required of all federal employees. Additionally, all external links transmit data over highly secure network connections to prevent unauthorized access to the information in transit. The relevant MOU defines the proper use of OneDOJ data and types of users that should have access. OneDOJ relies on state, local, and tribal law enforcement governance boards to authorize individual users in accordance with the MOU for future access to OneDOJ.

Section 6
Notice

6.1 Was any form of notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

This information is covered by a Privacy Act System of Records Notice published in the Federal Register, at 70 Fed. Reg. 39,790 (July 11, 2005), and modified at 70 FR 72,315 (December 2, 2005), and 72 Fed. Reg. 4532 (Jan. 31, 2007).

Additionally, because the OneDOJ system contains primarily information compiled for the purpose of identifying individual criminal offenders and alleged offenders and the OneDOJ system is not the repository for the initial collection of the information, the agent or officer who originally collected the information likely did not provide any sort of Privacy Act Statement to the individual or individuals from who or about whom the information pertains. Criminal law enforcement information maintained by the contributing components is usually exempted from the Privacy Act's individual notice provisions, and the Privacy Act's (j)(2) exemption has also been claimed to exempt that same information in this system from 5 U.S.C. § 552a(e)(3). See 28 C.F.R. 16.133.

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

Because this information is collected in connection with law enforcement investigative activity, generally, the individual does not have the right or opportunity to decline to the original collection of the information. This system will provide access to information collected by an originating organization concerning individuals, which is based on their suspected involvement with criminal case investigations and law enforcement concerns.

6.3 Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?

No. There is no general opportunity to consent to particular uses of information because the information contained in the system is existing data that was lawfully gathered and maintained based on

law enforcement authority and individuals may not have an opportunity to consent to particular uses of that information.

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

The privacy risk identified would be the failure of persons to know their information may be collected and what it will be used for. The Department has published a Privacy Act System of Records Notice (SORN) for investigative records maintained in OneDOJ. The information in this notice includes entities with which and situations when the Department may share investigative records. This notice, therefore, mitigates the risk that the individual will not know why the information is being collected or how the information will be used. No other notice was provided, and no other notice is required to be provided because the information in this system is collected during law enforcement activities and it is not practicable for any other notice to be given during these activities. It should also be noted that the system has been exempted pursuant to Privacy Act subsection (j)(2) from the Act's individual notice provision (subsection (e)(3)). See 28 C.F.R. 16.133.

Section 7
Individual Access and Redress

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

Each contributing agency is responsible for maintaining accurate, timely, complete and relevant records; individual access and redress should therefore be addressed to the agency where the information about the individuals originated. The System of Records Notice (SORN) for OneDOJ is exempted from the access and amendment provisions of the Privacy Act, pursuant to (j)(2) of the Privacy Act. See 28 C.F.R. 16.133.

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

Record access and amendment procedures are described in the SORN and in Departmental regulations. As noted in Section 7.1, pursuant to regulation, the information in the system is exempt from both the access and amendment provisions of the Privacy Act.

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

No other redress is available.

7.4 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.

The standard operating procedures for OneDOJ clearly state that an investigator or officer may not take action based solely on the information in the OneDOJ database. If there is a connection between two individuals or two addresses or two automobiles, the officer/agent must validate that information. That is standard procedure in law enforcement with or without this tool.

Section 8
Technical Access and Security

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

The Department will restrict access to the OneDOJ system to authorized law enforcement personnel with a need for access such as supervisors, law enforcement agents/officers, and task force members associated with agencies that have signed the MOU. In addition, limited access to the OneDOJ system will be provided to system administration and system security personnel for purposes of conducting system operation and maintenance tasks. All such personnel (either government employees or contractors/subcontractors) shall be vetted and cleared for system access and their access shall be monitored and audited.

8.2 Will contractors to the Department have access to the system?

It is possible that contract analysts will have access to this system, if that access is provided by the law enforcement component. FBI-CJIS will not grant access to the system without someone in the component certifying that person's role and a legitimate need to access OneDOJ in order to support criminal law enforcement.

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

Yes, two levels of access: administrator and user. Furthermore, both administrators and users can be assigned access privileges for certain data sources and certain regions. Note: civilian personnel will not have assigned privileges to the system. The administrators will give access based on state or federal regulations or local authority.

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

The Deputy Attorney General, as the chair of the LEISP LCC determines who can have access to information in the OneDOJ system. The Department will document these determinations in an MOU. In accord with the MOU, partner agencies will authorize specific persons to access information in OneDOJ consistent with the determinations made by the Deputy Attorney General.

Access to OneDOJ data by system administrators and/or system security officers will be limited to only that needed to perform these functions and will be documented in the MOU regarding the OneDOJ system.

Criteria, procedures, controls and responsibilities are documented in the MOU and in OneDOJ system administration and security documentation.

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

In order to mitigate privacy risks, FBI-CJIS personnel verify the user's role via email with the component points of contact. Users are re-vetted again throughout the duration of their system usage. CJIS is going to conduct a performance based audit of the OneDOJ system. This audit will be based on an established systems audit process, already in place for other CJIS systems and programs. Now that OneDOJ has been successfully transitioned to the CJIS Division, an audit process will be developed. CJIS has established a system to triennially audit federal, state, local, and tribal agencies that operates workstations, access devices, mobile data terminals, or personal/laptop computers that has access to OneDOJ data to ensure compliance with state and/or FBI CJIS policy, federal directives, and federal regulations.

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

OneDOJ has an audit capability that will log the date, time, subject, and originating account of all user queries. The Privacy Act requires that an accounting of disclosures be maintained for 5 years or the life of the record – whichever is longer – after the disclosure of the record. CJIS will maintain audit logs in accordance with the Privacy Act. In addition, CJIS maintains records for OneDOJ system and has retained records, specifically those containing PII, since its inception. OneDOJ components have the ability to periodically review the audit logs to ensure appropriate access to and use of information. Audit logs are reviewed by OneDOJ security staff every three years, but are made available for review should a particular agency suspect misuse of information

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

Training will be required for all OneDOJ users (including those accessing OneDOJ information from other systems). The training will include procedures to ensure users know how to properly use OneDOJ information. This training will be provided to make users of OneDOJ information aware of what information can be accessed from OneDOJ and will include a description of the information contained in the system, a typology of DOJ investigative reports, third-party rules, and coordination requirements, and other appropriate information. Users will also be notified of potential sanctions for misuse of the system or any data obtained from the system.

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

Yes, the system is secured in accordance with FISMA, as are all of the DOJ systems. A C&A for OneDOJ was last completed in Q1 of 2005.

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

OneDOJ is protected by boundary protection devices (e.g., firewalls and trusted guards) at identified points of interface with networks or local systems. The OneDOJ system employs virus protection software, encryption technology during transmission to ensure data security, and intrusion detection systems. Intrusion detection systems operate in a manner that is compliant with Title 18, Section 2511 of the United States Code, and the Electronic Communications Privacy Act.

All access tools will enforce tight controls over which privileges a user is granted and under what conditions these privileges can be used. Wherever possible, user roles and access restrictions will be standardized across agencies.

Section 9
Technology

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

There are two possible alternatives to handling of this information that would have lesser impact on the privacy of individuals. The first would be to not create a system like OneDOJ. Based on the needs of the law enforcement community to share investigative information in order to protect citizens from criminal and terrorist activity, this is not a practical alternative. In addition, DOJ has been mandated by Executive Order and Congressional Legislation to share data with local law enforcement. The federal government has a responsibility to share this data, but it must be done securely and legally.

The second would be to create a “Pointer Only” system. This means that when a query was conducted, the database would retrieve information that would list the name of the investigator or Point of Contact for the information for the user to contact. A “Pointer Only” system does not meet the needs of law enforcement entities because it may be overly burdensome and time consuming to contact the investigator or point of contact for the information that a user would seek. The retrieval of comprehensive case reports from OneDOJ is more useful to law enforcement agents because they can look at the information and see if it is related to their case and not have to call a point of contact unless they think it is relevant. Because speed is often an important element in apprehending a criminal or preventing a criminal act, “pointer systems” may limit law enforcement’s ability to effectively combat crime. They also do not allow for the use of analytical tools. In order to expedite the information sharing process across varying federal, state, local, tribal law enforcement entities and effectively investigate criminal activity, it is necessary to create a system such as OneDOJ without a “Pointer Only” design.

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

The core principal for the LEISP program and for the OneDOJ program was the reliance upon standards. In order for the DOJ components to share data with locals, all involved needed to agree on the use of the National Information Exchange Model (NIEM) standard. By implementing this exchange standard into the interfaces, we are now able to query data in other systems without having to mix data sets. This allows for improved accuracy as the data reside as close to the source as possible. If DOJ were to make multiple copies of the data set, it would be likely to become outdated, and thus subject to inaccuracies. With the model first described in 2005 in the LEISP document, DOJ is introducing a process that is implement-able and provides the best protection possible, given the diverse computing environments found in law enforcement across 18,000 agencies.

9.3 What design choices were made to enhance privacy?

As stated above, the decision to connect system to system, instead of putting all the data into a single database was driven out of necessity and because it ensures the best level of protection that could be reasonably implemented in the law enforcement arena.

Conclusion

DOJ components will be sharing their controlled unclassified criminal law enforcement information with federal, state and local law enforcement agencies. OneDOJ provides a single, standards-based interface through which DOJ components will exchange information with authorized law enforcement agencies and sharing initiatives. The system also will assist agents and officers to compare information and analyze that information to determine similarities or other relationships between criminal acts and the people suspected of committing these acts. OneDOJ will provide analytical tools that can be used to correlate case information across law enforcement agencies and across, for example, geographic areas.

Signatures Page

Responsible Official

X Recommend
☐ Not Recommend

/s/
Harrell Watkins
Deputy Director, E-Government

Date: 3/5/2008

Reviewing Official

X Recommend Approve
☐ Recommend Not Approve

/s/
Vance Hitch
Chief Information Officer

Date: 3/5/2008

Approving Official

X Approved
☐ Not Approved

/s/
Kenneth P. Mortensen
Acting Chief Privacy and Civil Liberties Officer

Date: 8/7/08