Privacy Impact Assessment for the

Justice Management Division Intra-DOJ Information Exchange Architecture Infrastructure (IDEA-I)

20 AUGUST 2007

Contact Point
Boris Shur – Chief Data Architect
Dept. of Justice /Office of the Chief Information Officer
(202) 305-2714

Reviewing Official
Vance Hitch – Chief Information Officer
Dept. of Justice/Office of the Chief Information Officer
(202 514-0507

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

Introduction

The Intra-DOJ Information Exchange Architecture Infrastructure (IDEA-I) system is an enterprise solution providing a secure, automated electronic distribution facility which connects and facilitates the transfer of legacy Department data sets to new Department Information Sharing Applications. It is available to all Department personnel and systems that participate in the OneDOJ initiative. Nonetheless, IDEA-I is not an end user application, rather it is infrastructure to enable uploading and updating of user-facing applications using secure protocols for data transfer.

As a key part of the Law Enforcement Information Sharing Program (LEISP), the solution will improve the efficiency of sharing data sets within the Department. The LEISP team has identified data integration as a key capability for OneDOJ and is driving tasks and new processes through the Intra-DOJ Information Exchange Architecture Infrastructure to define supportable end-to-end processes and to create reusable and sharable technologies which reduce the operational resource demands required to achieve OneDOJ objectives. OneDOJ is an initiative to develop policies, procedures and capabilities for all appropriate Department assets (both data and services) to be made available for sharing within the Department and between the Department and its partners.

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

1.1 What information is to be collected?

The IDEA-I system does not collect information; rather the information is routed between component data sources and end user applications. The type of information routed is law enforcement data files from multiple Department data sources. Specifically, the IDEA-I system does not allow the viewing or searching of any records contained in the files. The files are sent encrypted through the system and are only decrypted upon reaching their intended destination. The solution uses Secure File Transfer Protocol (SFTP) which is a proven standard within government and within industry.

1.2 From whom is the information collected?

The information transported through the IDEA-I system comes from multiple Department and component data sources such as Bureau of Alcohol, Tobacco and Firearms (ATF), Bureau of Prisons (BOP), Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), and U.S. Marshals (USMS), to the Department information sharing applications such as but not limited to N-DEx and R-DEx.

The specific data source systems which currently will send data to N-DEx and R-DEx are ATF N-Force, BOP Sentry, BOP ITS, DEA NADDIS, and USMS WINS, FBI ACS (unclassified only). The IDEA-I system will transport and distribute this data utilizing the Law Enforcement Exchange Specification (LEXS) standards, which provide a common and standards-based approach to the information sharing applications R-DEx and N-DEx.

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

2.1 Why is the information being collected?

No new information is collected; rather IDEA-I is a technical mechanism to help the Department securely move data from existing component systems into applications built for multi-agency sharing. The data is extracted by the component that collected the data, delivered to the IDEA-I servers which, through secure protocols, transport the data to its intended repository. The information is currently shared by manual and other un-secure means, and the IDEA-I system was developed to mitigate these risks. IDEA-I also helps the Department comply with OMB Memorandum M-06-16 which specifies new rules for data protection and transmission.

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

The Department data owners who will utilize the IDEA-I to share data currently have a Memoranda of Understanding or Agreement (MOU/MOA) in place. IDEA-I is merely a transport mechanism, or service, which provides a secure, automated method of routing the data. The IDEA-I system does not itself view or allow viewing or retrieving of any information contained in the files.

The Department data owners maintain their existing MOU/MOAs and do not require separate agreements with IDEA-I. In addition, the Deputy Attorney General's memorandum to component heads dated 12/21/06 gives additional authority to components and OCIO to share more information, and is consistent with the guidance in the 9-11 Commission Report.

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.

During the system design process, risks to the data while in transit, specifically the interception of data and integrity of the data, were identified. These risks were substantially mitigated through the use of secure protocols which encrypt the data throughout the file transport process and employ error checking features to ensure every byte of data sent from one component is delivered to the intended receiving component, thereby ensuring the integrity of the data.

Digital certificates issued by DOJ PKI are used for strong authentication of users, and when paired with SFTP, provide two factor authentication. Specifics on the system design and build are contained in the certification and accreditation documents.

Section 3.0
Uses of the System and the Information.

3.1 Describe all uses of the information.

The IDEA-I system has no insight, control or awareness of how the information contained in the files will be used by the information sharing applications and their users. IDEA-I is the transport mechanism which allows files to be routed securely from Department data sources to the Department information sharing applications. The IDEA-I system is not the system of record for the data contained in these files and it does not create new files or records. Users cannot create, or modify any records in the files. The uses are the same as the existing underlying systems and IDEA-I does not introduce any new uses. It is a conduit for the transmission of data.

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.)

The IDEA-I system does not conduct any searching of the files being routed through its system. In addition, the IDEA-I system does not allow and does not itself, have the capability to view, search or retrieve records contained in the files, while being routed through the system.

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

The IDEA-I system does not check the accuracy of the data in the files. IDEA-I employs secure protocols which ensure the accuracy of the data transfer and integrity of data at the file level, and as part of the process, sends confirmation emails for both delivery and receipt of files through the system. The accuracy of the data rests with the system of record for the respective data owner. JMD/OCIO assumes that the data is accurate, and this is consistent with the guidance included in the LEISP Strategy which was first published in 2005.

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)?

As the IDEA-I system is a transport system, and not the system of record for this data, therefore a retention schedule is not applicable. The initial functionality of the IDEA-I system allows the files to be stored for one month when necessary to provide deltas, or differences, between the current and previous files. Most of the data sources do not have the capability to provide incremental updates. In the future, the files will be retained according to the retention schedules of the underlying data, encrypted and stored without end user access of any sort. This approach enhances security and privacy by making it unnecessary for the duplicate extract to be performed and transported when a new recipient requests existing data. The files will be extracted and sent to the approved recipient in a secure, automated process. Data sources will be able to see who received their data along with the date and time received, thus improving the audit capabilities.

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 IDEA-I system is designed to only allow properly authenticated system administration users to access the system and transfer files. Users of the IDEA-I system can only transfer and receive files. No misuse of the data can occur within the IDEA-I system due to its limited functionality with respect to data manipulation. Specifically, users cannot remove files from the IDEA-I system, as they do not have this type of access to the system. They can only view information about files, such as when a file was received or sent, but they will not be able to see the actual files while in the system. Existing MOU/MOAs between the Department data sources govern, among other things, the use of the data being shared.

Section 4.0 Internal Sharing and Disclosure of Information within the System.

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

The IDEA-I system is capable of distributing files between all DOJ data sources and partners who have JUTNET connectivity. Currently files will be shared between ATF, BOP, US Marshals, DEA, FBI, OFC, FTTTF and information sharing applications N-DEx and R-DEx.

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

The IDEA-I system is not included, nor concerned, with the process of determining what information is shared between the Department data sources and the purpose of such information. IDEA-I is the transport mechanism in place to facilitate the sharing of information. These requirements should be addressed in the MOU/MOA(s) between DOJ components, data sources and end-user applications.

4.3 How is the information transmitted or disclosed?

Information transported through the IDEA-I system is transmitted electronically using the secure file transfer protocol (SFTP). The frequency and amount of data transmitted between data sources and consumers will be in accordance with the respective MOU/MOA in place to authorize the sharing of the particular data being sent. As a function of secure file transfer, the file is encrypted prior to being sent, and remains encrypted until it is has reached the designated recipient(s).

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

While there is a chance for misuse of the files by the data consumer system administrator, the risk was mitigated within the IDEA-I system by not allowing that type of access to the files while they are in the system. Again, the only information accessible in the IDEA-I system is limited to information about the files, such as when they were sent and received. This was confirmed through system test and evaluation (ST&E), as part of the certification and accreditation process. The internal sharing between current components was in place prior to the inclusion of the IDEA-I in the OneDOJ initiative, so the parameters regarding the specifics of how the data is to be shared, by whom, and for what purpose, was previously clarified and authorized. The components themselves designate their user(s) who will have access to the IDEA-I system and what privileges they should have. Auditing procedures are in place to ensure policies and procedures are in place and operating properly and audit logs are reviewed regularly.

Section 5.0 External Sharing and Disclosure

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

The IDEA-I system is only available to Department data owners and end-user applications on JUTNET (Justice Network) or on the CJIS Wide Area Network, managed by the FBI. It will not transport or distribute any data to non – DOJ components.

5.2 What information is shared and for what purpose?

N/A, See 5.1.

5.3 How is the information transmitted or disclosed?

N/A, See 5.1.

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

N/A, See 5.1.

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

N/A, See 5.1.

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

N/A, See 5.1.

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

There were no risks identified for the IDEA-I system in this area, due to the fact that IDEA-I will not be available to non-DOJ recipients.

Section 6.0 Notice

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

As stated in the introduction, the IDEA-I system does not collect information from individuals. The information that is transported through the system comes from Department component entities and is not available for use of any kind while being routed through the IDEA-I system.

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

See answer in 6.1

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?

Not applicable to the IDEA-I system; see answer in 6.1

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

This specific section is not applicable to the IDEA-I system, as the system does not collect information from individuals, nor does it use, view, retrieve or search any information contained in the files.

Section 7.0 Individual Access and Redress

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

The IDEA-I system, as previously stated in this PIA, does not collect information on or from individuals. It does allow the use of any information contained in the files, for any purpose, while the file(s) is/are being transported through the system. Additionally, as IDEA-I is not the system of record for this information, any redress procedures would not apply to this system.

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

Not applicable; please see answer in section 7.1

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

Not applicable; please see answer in section 7.1

7.4 Privacy Impact Analysis: Discuss any opportunities or procedures by which an individual can contest information contained in this system or actions taken as a result of agency reliance on information in the system.

This section is not applicable to the IDEA-I system. Please refer to the answer in section 7.1

Section 8.0 Technical Access and Security

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

The user groups who may have access to the IDEA-I system are the IDEA-I system administrators, developers, contractors and designated users from the Department component data sources.

8.2 Will contractors to the Department have access to the system? If so, please submit a copy of the contract describing their role with this PIA.

Yes, the LEISP support contractors managed by OCIO, helped build and will maintain the IDEA-I tool.

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

The IDEA-I system has two basic roles which help determine user privileges.—full control and read-only. Full-control permits read write access, and read-only is self explanatory.

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

An official request from user supervisor, which includes the purpose and duties of user with respect to the IDEA-I system, initiates the Secure Shell (SSH) user account creation. SSH is utilized because it employs encryption throughout the session. Also included in the request will be the requested privileges for the user. The IDEA-I system administrators are the only users with administrative rights to the IDEA-I system. As such, upon receiving the official request, they will create the requested SSH user account (full-control/read only). These accounts will be placed in system profile-related groups. Specifically, user A from ATF will be in the ATF group, with either full control privileges or read only privileges. Users will also be authenticated prior to accessing IDEA-I through the use of digital certificates issued by the DOJ PKI (Public Key Infrastructure) system, further enhancing the security of IDEA-I.

These procedures are documented on the IDEA-I system website and in the IDEA-I System User Guide, which is also included in the certification and accreditation documents.

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

As stated in the above section 8.4, upon an official request from the component system supervisor, which serves as verification that the user does, in fact, have the need or requirement to use this system, then only then, will a SSH account be created according to the privileges authorized by the designated government official. The security policies currently in place, do not allow users access to the IDEA-I servers, and the system groups the users are placed into exist in the local security settings in Windows 2003 on each server, specifically for auditing purposes.

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

The system profile related groups the user accounts are placed into are located in Window 2003 for directory positioning, SSH authentication and auditing. Safeguards such as SSH authentication, and file permissions restrictions which keep the data available only at the file-level to prohibit the viewing, searching or retrieval of information contained in the file, are in place to prevent the possible misuse of data. In addition, system administrator activities periodically undergo review to ensure security and access policies are enforced and data is protected.

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

Users are briefed upon the secure mechanisms in place to allow the transfer of their respective data files, and more in-depth security is outlined in the system user guide. Current DOJ privacy training is adequate since all users of the IDEA-I are from DOJ components

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

Yes, the data is secured in accordance with FISMA requirements. The certification and accreditation was completed 29 June 2007.

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

The access and security controls for the IDEA-I system are standardized for all users. This eliminates certain risks inherent with having separate policies for different users of the system. No users have access to the servers or any infrastructure supporting the IDEA-I system. The users may only transport file via secure protocols which ensure the files are encrypted throughout the transport process.

Section 9.0 Technology

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

Several technology solutions provided by various vendors were evaluated during the design process for the IDEA-I system. These solutions also included various hardware platforms and storage solutions as well. The decision upon which technology to base this system, was decided by a number of factors (growth potential, adherence to industry standards, storage capacity, network integration), including effectiveness.

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

The requirement was to design a system, or infrastructure, that could satisfy the requirements of increased information sharing while ensuring the most secure, effective, and automated method of transporting data files. To that end, IDEA-I employs the use of digital certificates issued by DOJ PKI to ensure the authentication of all users, was designed to be placed in a secure network environment (JUTNET), and ensures the integrity, privacy and security of the data by utilizing SFTP for secure file transfers.

9.3 What design choices were made to enhance privacy?

The utilization of the secure file transfer protocol (SFTP), a recognized industry standard for securing data, was the primary design specification to be included in the capability of the IDEA-I system. It further enhances the security of file transfers by encrypting the data to ensure integrity and privacy throughout the transport process.

Conclusion

The IDEA-I system was designed and built as a part of the OneDOJ initiative to increase information sharing between DOJ data sources and information sharing applications. As such, the system instituted industry best practices and technologies to ensure the fundamental requirements of privacy, security and data integrity were not only met, but exceeded. By designing a system which resides on a secure network already accessible by DOJ components, thus leveraging existing network security controls, IDEA-I is able to connect users within DOJ. Data encryption, two-factor authentication and other security controls ensure the integrity and privacy protection of the information, thus mitigating the possibility of data misuse within the IDEA-I tool.

Responsible Officials

Harrell Watkins / Boris Shur

Department of Justice

Approval Signature Page

/s/ _____ Sign / Date

Kenneth Mortensen
Acting Chief Privacy and Civil Liberties Officer
Department of Justice