Justice Management Division

Privacy Impact Assessment
for the
Justice Communication System (JCS)

Issued by:
Arthur E. Gary
General Counsel and Senior Component Official for Privacy

Approved by: Erika Brown Lee, Chief Privacy and Civil Liberties Officer, Department of Justice

Date approved: [May 21, 2015]

(September 2012 DOJ PIA Form)

Executive Summary

The Justice Management Division (JMD) Justice Communication System (JCS) combines messaging systems used by participating Department of Justice (DOJ) components into a single enterprise infrastructure. Specifically, this system provides email, instant messaging, and collaboration services using commercial off-the-shelf software (COTS). Component messaging systems will be migrated into JCS in a phased approach.

The purpose of the system is to meet the messaging and collaboration requirements of participating components and to increase standardization of such functionality within the Department. A Privacy Impact Assessment (PIA) was conducted on this system because information about non-DOJ individuals is also captured by this system, even though users of the system are limited to DOJ personnel. For example, if a non-DOJ individual communicates with a DOJ user via email, the email address of the non-DOJ individual, as well as any information transmitted through the email message, will be captured. In addition, in the performance of their duties, DOJ users may transmit information about non-DOJ individuals via this system, such as in the course of civil or criminal litigation.

Section 1: Description of the Information System

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

(a) The purpose that the records and/or system are designed to serve:

> The Justice Communication System (JCS) combines messaging systems used by participating Department of Justice (DOJ) components into a single enterprise infrastructure to meet the messaging and collaboration requirements of the Department. The consolidation enhances the common messaging functionality across the Department, reduces the number of distinct messaging systems deployed, and increases standardization of functionality and configuration. This system is to replace the Justice Consolidated Office Network (JCON) mail system (JCONext Messaging / JCON Consolidated Office Automated Resource). Component messaging systems will be migrated into JCS in a phased approach, ensuring that email, calendar, and contact data is preserved.

(b) The way the system operates to achieve the purpose(s):

> JCS operates to achieve this purpose by providing three main services: email, instant messaging, and collaboration portals/repositories. The system provides these services using COTS, including Microsoft Outlook, Microsoft Exchange, Microsoft Server 2008 and 2012, Microsoft SQL Server, Microsoft Lync, Microsoft SharePoint, and Research in Motion BlackBerry software. Microsoft System Center Management Suite will be available to privileged users for system management activities, such as configuration management and server end-point protection.

(c) The type of information collected, maintained, used, or disseminated by the system:

The type of information collected, maintained, used, or disseminated by the system includes: names and contact information of DOJ users and non-DOJ individuals who communicate with DOJ users via JCS; email messages (including any attachments); message log information (including IP address of sender, date, and time); instant messages; and information stored in collaboration portals/repositories (such as spreadsheets, word processing documents, and PDF documents). The system also maintains logs of DOJ user activity.

(d) Who has access to information in the system:

Only DOJ employees and authorized contractors may have system user accounts. Component Active Directories will be used for identification and authentication of users. Non-DOJ individuals may have access to information in the system only in the sense that they may receive email messages from DOJ users containing information (email messages) that is maintained in JCS.

(e) How information in the system is retrieved by the user:

Information in the system is accessed using workstation/laptop client software, via a web browser (e.g., Outlook Web Access, SharePoint), or via a mobile device. DOJ users will have access to communications they send and receive as well as shared files from the consolidated collaboration environment. DOJ user directory information can be retrieved by DOJ users by name or other user identifier. Privileged users can retrieve audit log information by a DOJ user's name or other identifier. Depending on the application used, some information can be retrieved by text searches using standard COTS (e.g., Outlook).

(f) How information is transmitted to and from the system:

Information is transmitted to and from JCS through the connections noted in Section 1(g) below. These interconnections are all within DOJ boundaries and utilize firewalls and other applicable security measures. All email traffic that traverses to DOJ users will continue to route through the existing Secure Email Gateway (SEG), which provides anti-spam and anti-malware capabilities. All email traffic exiting or entering the DOJ network is inspected by the DOJ Trusted Internet Connection (TIC), which is monitored by the Justice Security Operations Center. Information may be transmitted through JCS via email (simple mail transfer protocol), instant messaging (standard Lync ports), and SharePoint (secure sockets layer). Remote access to the system will be accomplished using DOJ Connect with secure sockets layer encryption.

(g) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects):

There are no interconnections outside of the Department. All interconnections are within DOJ information system boundaries, including the following:

a. Justice Unified Telecommunications Network (JUTNet) (for wide-area networking connectivity).
b. Trusted Internet Connection at Justice Data Centers (for internet connectivity, including email routing to and from Internet email addresses).
c. DOJ Connect (for remote access).
d. Component Active Directories (for identification and authentication of users)

(h) Whether it is a general support system, major application, or other type of system:

JCS consists of a cluster of major applications.

Section 2: Information in the System

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

JCS collects, maintains, or disseminates the following types of information:

- DOJ user account information: This information includes names and work contact information of DOJ users. JCS also maintains logs of user activity.

- Email messages and related information: JCS maintains all email messages sent to or from DOJ users, including any attachments. JCS also collects the following items of information regarding non-DOJ individuals who communicate with DOJ users via email: name, email address, and message log information (such as internet protocol (IP) address, date of message, and time of message).

- Instant messages: JCS maintains instant messages sent between DOJ users.

- Documents uploaded to collaboration portals/repositories: Examples include word processing documents, spreadsheets, and PDF documents.

Email messages, including any attachments, and documents uploaded to collaboration portals/repositories may include significant quantities of personal information relating to the substantive work of the Department. Because of the varied nature of the Department's work and because email messages and documents maintained in JCS could conceivably include almost any type of information, it is not possible to list with certainty every item of information that will be collected, maintained, or disseminated by the system. Therefore, the items of information checked below are limited to user account information and log information maintained by JCS.

Identifying numbers					
Social Security		Alien Registration		Financial account	
Taxpayer ID		Driver's license		Financial transaction	
Employee ID		Passport		Patient ID	
File/case ID		Credit card			
Other identifying numbers (specify):					
General personal data					
Name	X	Date of birth		Religion	
Maiden name		Place of birth		Financial info	
Alias		Home address		Medical information	
Gender		Telephone number		Military service	
Age		Email address	X	Physical characteristics	
Race/ethnicity		Education		Mother's maiden name	
Other general personal data (specify):					

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

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

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

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

The sources of the information in the system are as follows:

- DOJ user account information: This information is either assigned to the individual by the Department or obtained from existing databases maintained by the Department.

- Email messages and related information: The source of an email message is the sender of the message, who could be a DOJ user, an employee of another federal agency, an

employee of a state or local government agency, an employee of a private company or law firm, a member of the public, or some other category of individual or entity. Message log information is automatically generated by the system based on the date and time of the message and the internet protocol address from which the message was sent.

- Instant messages: The sources of instant messages are DOJ users.

- Documents uploaded to collaboration portals/repositories: DOJ users upload documents to collaboration portals/repositories. (Information contained in such documents may come from any source or sources.)

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

A potential threat to privacy in light of the information collected is that the system will collect and/or maintain more information than is relevant and necessary to accomplish the Department's official duties. Although JCS is simply a portal and repository of official communications that does not restrict the type of content of information, there are still limits on the type of information that may and should be collected pursuant to federal law.

For example, to the extent that information in the system is protected by the Privacy Act of 1974, it is subject to the requirement that an agency maintain in its records only such information as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or Executive Order. Additionally, because DOJ personnel use JCS to help carry out the Department's various missions, the type of information sent through or stored in the system is limited by the various authorities delineating component missions and authorizing the collection and maintenance of information to carry out such missions. These authorities are listed in the various Privacy Act system of records notices (SORNs) that apply to the information in JCS depending on the nature of such information and how it is retrieved. The SORNs describe the categories of records and the categories of individuals about whom information may be collected, thereby placing limits on such collections.

A potential threat to privacy also exists in light of the sources of the information since much of the information maintained by JCS is not collected directly from the individual who is the subject of the information; thus, there is an increased risk that the information is inaccurate. As a portal and repository of communications, JCS itself is not the original collector of much of the information that it maintains about individuals. For example, many of the documents attached to emails or stored in collaboration repositories for official business purposes – including documents containing information about individuals – were created before they entered JCS. While the document-creation process may have involved collecting information directly from the subjects of the information, such collection took place outside of JCS. With regard to DOJ user account information (name, user ID, work contact information), such information is obtained from existing directories within the components (which have already been verified for accuracy) or is assigned to the user by JCS.

For information about security controls that have been applied to JCS, please see the responses to questions 6.1 and 6.2.

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.)

Because DOJ personnel use JCS's communication and collaboration services in furtherance of the various missions of DOJ components, the purposes and uses of the system span the range of such missions and include providing administrative support to such missions.

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	X	To promote information sharing initiatives
	To conduct analysis to identify previously unknown areas of note, concern, or pattern.	X	For administering human resources programs
X	For litigation		
	Other (specify):		

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.

JCS provides users with the following primary capabilities:

- Email: Microsoft Outlook and Exchange provide DOJ users with the ability to exchange and manage electronic messages sent between DOJ users or between DOJ users and individuals outside the Department with valid email addresses.

- Calendar: Microsoft Outlook Calendar provides a calendar and scheduling for users that is fully integrated with email, contacts, and other features. It helps keep track of appointments, events, and meetings and can indicate a user's availability.

- Instant messaging and virtual conferencing: Microsoft Lync provides JCS users with real-time communication and virtual conferencing capabilities. Using Lync, JCS users may exchange secure instant messages with other JCS users. In addition, groups of JCS users may assemble virtual conferences in which they may communicate instantaneously through instant messages and simultaneously share documents (such as PowerPoint presentations or Word documents) with one another for collaboration or presentation purposes.

- Collaboration portals/repositories: Microsoft SharePoint provides a managed collaboration solution that allows users to efficiently work together to share information, collaborate on and publish documents, implement workflows, and maintain task lists.

These capabilities facilitate official communications by allowing DOJ users to share information electronically in real time on the DOJ network and between authorized devices. Because effective communication is essential in accomplishing any objective, the uses described above support the Department's efforts in each of the areas checked in question 3.1.

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; 44 U.S.C. § 3101
	Executive Order	
	Federal Regulation	
X	Memorandum of Understanding/agreement	Service Level Agreement for DOJ Email Consolidation Project Phase I – Justice Communication System

X	Other (summarize and provide copy of relevant portion)	Various DOJ component mission authorities (including statutes, Executive Orders, and regulations). DOJ Order 2640.2F – Information Technology Security; DOJ Order 2740.1A – Use and Monitoring of DOJ Computers and Computer Systems; DOJ Order 2880.1C – Information Resources Management Program

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.)

With regard to the substantive information in the system (email messages, documents uploaded to collaboration portals/repositories, instant messages), JCS is not designated as an official record-keeping system; rather, substantive information in the system is retained and disposed of by the component in accordance with the retention schedule applicable to such information.

In accordance with DOJ IT Security Standards, all system administration/audit information (including user account information) is retained for a minimum of 30 days online (in the system itself) and 90 days offline (in backup storage). Audit logs may be stored longer upon request if needed, such as for an inquiry into a security incident. This is consistent with General Records Schedule 20-1.c, which permits agencies to delete or destroy system files such as "log-in files, password files, audit trail files, system usage files" "when the agency determines they are no longer needed for administrative, legal, audit, or other operational purposes." In general, system administration/audit information is over-written as the storage space is needed.

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 threats to privacy as a result of the Department's use of the information in JCS include the risks of unauthorized access to the information, threats to the integrity of the information resulting from unauthorized access, and unauthorized disclosure of the information. For a list and description of controls that have been put into place to safeguard against these and other risks (including mandatory training for system users regarding appropriate handling of information and automatic purging of information), please see the responses to questions 6.1 and 6.2.

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			
DOJ components	X			
Federal entities	X	X (NARA)		Records are transferred in bulk to NARA when required for record-keeping purposes.
State, local, tribal gov't entities	X			
Public	X			
Private sector	X			
Foreign governments	X			
Foreign entities	X			
Other (specify):	X			Any individual who communicates with a DOJ user via JCS.

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.)

For a list and description of controls that have been put in place in order to prevent or mitigate threats to privacy in connection with the disclosure of information, as well as to safeguard against other threats to privacy, please see the responses to questions 6.1 and 6.2.

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: A warning banner notifies DOJ users at login that any information transmitted through the system may be monitored, intercepted, searched, and/or seized by the Department and that users therefore have no reasonable expectation of privacy in such information.
	No, notice is not provided.	Specify why not:

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

	Yes, individuals have the opportunity to decline to provide information.	Specify how: .
X	No, individuals do not have the opportunity to decline to provide information.	Specify why not: All DOJ personnel are assigned JCS user accounts. JCS therefore maintains user account information as well as audit log information on all DOJ personnel. However, DOJ personnel may choose to use a means of communication other than JCS (e.g. phone, fax, etc.). Moreover, non-DOJ individuals may choose not to send email messages to DOJ users.

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: The vast majority of uses of information in JCS are communications to support the various missions of DOJ components. It would be impracticable to determine in advance every particular communication in which an individual's information will be transmitted as well as to obtain consent for each such communication.

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.

To provide transparency and allow DOJ users to understand how their communications and other information will be handled, a warning banner is displayed on the login screen that DOJ users see when they log in to their workstations or mobile devices. This banner informs users that any information that they transmit through the computer or mobile device, including information transmitted through JCS, may be monitored, intercepted, searched, and/or seized by the Department, and that users therefore have no reasonable expectation of privacy in such communications or other information.

Moreover, as noted above, JCS is a portal and repository of a variety of official communications that does not restrict the type of content of such communications. However, to the extent that content contained in such communications are protected by federal law, including the Privacy Act, notice is provided by various DOJ Privacy Act systems of records notices (SORNs), which apply depending on how information is retrieved. These notices and documents are published in the Federal Register and available to the general public. Also, as noted below in section 7, DOJ user account information and system administration/audit information is covered by the SORNs for DOJ-014, Department of Justice Employee Directory Systems, 74 Fed. Reg. 57194 (Nov. 4, 2009), and DOJ-002, Department of Justice Computer Systems Activity and Access Records, 64 Fed. Reg. 73585 (Dec. 30, 1999) (as modified in 66 Fed. Reg. 8425 (Jan. 31, 2001) and 72 Fed. Reg. 3410 (Jan. 25, 2007)).

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: December 17, 2013.
X	A security risk assessment has been conducted.
X	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: Appropriate security controls that have been identified and implemented to protect against risks identified in the security risk assessment include those listed in DOJ Security Assessment and Authorization Handbook v. 8.4, which provides the framework and direction for performing security assessments and authorizations of all DOJ IT systems, as well as those listed in response to question 6.2.
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: JCS operation teams have been consistently monitoring, testing, and evaluating the system and controls that have been applied to the system throughout the system's deployment and migration of components. DOJ IT security standards, which include monitoring, testing, and evaluation requirements, have been applied to the system, as well as Microsoft best practices. See the response to question 6.2 for additional information on monitoring, testing, and evaluation.
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: Audit logs are maintained to help ensure compliance with tiered/role-based access as well as to help safeguard against unauthorized access, use, and disclosure of information. Audit logs can only be accessed by authorized staff as required to ensure compliance with security requirements.
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
	X		Training specific to the system for authorized users within the Department.
			Training specific to the system for authorized users outside of the component.
			Other (specify):

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

Access and security controls that have been utilized to protect privacy and reduce the risk of unauthorized access and disclosure include the following:

- The system is accessible by DOJ employees and contractors only and utilizes tiered, role-based access commensurate with the user's official need to access information. Physical access to system servers is controlled through site-specific controls and agreements.
- The system is protected by multiple firewalls, an intrusion prevention system, real-time continuous monitoring using malicious code detection and protection, encryption, and other technical controls in accordance with applicable security standards (including DOJ Order 2640.2F – Information Technology Security and Federal Information Processing Standards 140-2 – Security Requirements for Cryptographic Modules).
- All email traffic routes through the existing Secure Email Gateway, which provides anti-spam and anti-malware capabilities. All email traffic entering or exiting the DOJ network is additionally inspected by the DOJ Trusted Internet Connection, which is monitored by the Justice Security Operations Center.
- All users must complete computer security awareness training annually, as well as read and agree to comply with DOJ information technology rules of behavior both prior to accessing the DOJ network and annually thereafter. System administrators must complete additional professional training, which includes security training. In addition, all users must complete privacy training on handling and protecting personally identifiable information.
- Audit logging is configured and logs are maintained separate from other system data to help ensure compliance with tiered/role-based access as well as to help safeguard against unauthorized access, use, and disclosure of information. Audit logs can only be accessed by authorized users with privileged access. System administration/audit data is automatically purged at defined intervals and in accordance with applicable retention periods.
- Responses to potential unauthorized disclosures or data breaches are covered in vendor contracts and system rules of behavior in order to ensure appropriate procedures and reporting.

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: DOJ-014, Department of Justice Employee Directory Systems, 74 Fed. Reg. 57194 (Nov. 4, 2009); DOJ-002, Department of Justice Computer Systems Activity and Access Records, 64 Fed. Reg. 73585 (Dec. 30, 1999) (as modified in 66 Fed. Reg. 8425 (Jan. 31, 2001) and 72 Fed. Reg. 3410 (Jan. 25, 2007)); and other published DOJ system of records notices depending on the nature of information in the communication or collaboration document and how the information is retrieved.
	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.

System administrators can retrieve DOJ user account information and audit log information by user name or other user identifier. DOJ users can retrieve directory information by DOJ user name. Depending on the JCS application used, DOJ users can retrieve information (such as information contained in email messages) by name or other identifiers using a full-text search capability.