Justice Management Division

Privacy Impact Assessment
for the
Justice Unified Telecommunications Network (JUTNet)
Voice Services System

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: January 5, 2015

(September 2012 DOJ PIA Form)

Section 1: Description of the Information System

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

(a) the purpose that the records and/or system are designed to serve;
(b) the way the system operates to achieve the purpose(s);
(c) the type of information collected, maintained, used, or disseminated by the system;
(d) who has access to information in the system;
(e) how information in the system is retrieved by the user;
(f) how information is transmitted to and from the system;
(g) whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects); and
(h) whether it is a general support system, major application, or other type of system.

The response should be written in plain language and should be as comprehensive as necessary to describe the system. If it would enhance the public's understanding of the system, please include system diagram(s).

As background, the Justice Unified Telecommunications Network (JUTNet) is the Department of Justice's wide area network. The subject of this privacy impact assessment is the JUTNet Voice Services system (JVS), a telephone and voicemail system that operates on JUTNet as a managed service provided by AT&T. JVS, which is designed to replace legacy telephone and voicemail systems, is comprised of two subsystems: the Cisco Unity Voicemail system (CUV) and the DOJ enterprise Voice Over Internet Protocol system (VOIP).

(a) The purpose of JVS is to provide telephone services (VOIP) and voicemail services (CUV) to the Department. As explained below, because JVS operates on JUTNet and connects phone calls using internet protocol (IP) addresses, JVS permits greater integration of telephone services and network computing services as compared with conventional telephony (e.g., transmission of phone calls over a data network, storage of voice mail messages within JVS, utilization of information stored in the Department's Global Access List).

(b) VOIP will use the JUTNet data network as well as workstation internet protocol (IP) addresses to transmit and connect internal phone calls. (For phone calls entering or exiting the Department, the system will interface with public telephone networks.) Because VOIP will operate on JUTNet, it will be able to utilize the DOJ Global Access List (GAL) (a directory of DOJ employee and contractor contact information) to facilitate various functions (e.g., routing calls, storing and retrieving voicemail messages), though the system itself will not store or maintain GAL information. JVS will also record and store voicemail messages from internal and external callers. In order to access these messages, system users must enter their password into their desktop phone.

(c) The system stores and maintains names of users (limited to DOJ employees and contractors); voicemail messages left by both users and external callers; passwords chosen by users to access their voicemail messages; phone numbers of users; IP addresses of users (though these are associated with

workstations, not individual users); and call log information (phone number of caller, date of call, time of call). Phone units with caller ID screens display call log information. Whenever a user receives a voicemail message, the phone number of the caller, date of call, and time of call (but not the name of the caller or the message itself) will also be sent to the user's Outlook account, which will display a notification that the user has received a message; this information will then be stored within Outlook.[1] AT&T will maintain call log information for 30 days in case it is needed for a specific business purpose (e.g., call quality troubleshooting); reports of such information are occasionally provided to DOJ so that it may evaluate the effectiveness of the service provider, verify billing for toll calls, and perform troubleshooting. The system also maintains audit log information of system administrator activity.

(d) A group of AT&T personnel serve as system administrators and provide support services to DOJ users. These administrators sign and agree to the DOJ privileged user rules of behavior, which limits their access to information that is necessary to perform their official duties. Ordinary users will have access to their own information, including their voicemail messages, as well as to the GAL (which is not maintained in JVS). As mentioned above, AT&T will temporarily maintain call log information in case it is needed for a specific business purpose; reports of such information will occasionally be provided to DOJ as indicated above. Because both internal and external phone units have caller ID screens, call log information will be displayed by the system.

(e) System administrators have the ability to retrieve user account information (such as name, phone number, and workstation IP address) by personal identifier such as the user's name or phone number. Additionally, audit log information of system administrator activity can be retrieved by user ID of the system administrator. In order to access their voicemail messages, users enter their password into their desktop phone.

(f) VOIP will use the JUTNet data network as well as workstation IP addresses to transmit and connect internal phone calls. For calls entering or exiting the Department, the system will interface with public telephone networks. VOIP will utilize GAL information to facilitate various functions (e.g., routing calls, storing and retrieving voicemail messages). When a user receives a voicemail message, call log information is sent to the user's Outlook account (if the user has this functionality).

(g) JVS operates on JUTNet, taps into the GAL in order to facilitate various system functions, and interfaces with public telephone networks for external calls.

(h) JVS is a major application.

Section 2: Information in the System

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

[1] Note that not all components will have this functionality.

(Check all that apply.)

Note that the system will store and maintain voicemail messages left by users as well as by external callers (which could conceivably convey any type of information). The system will also store and maintain the following information:

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			

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

Work-related data					
Occupation		Telephone number	X	Salary	
Job title		Email address		Work history	
Work address		Business associates			
Other work-related data (specify): As mentioned above, JVS utilizes GAL information, such as email addresses and other directory information, but does not store or maintain that information.					

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

System admin/audit data					
User ID	X	Date/time of access	X	ID files accessed	X
IP address	X	Queries run	X	Contents of files	
Other system/audit data (specify): Audit logs of system administrator activity indicate the activity performed such as changing, adding, or deleting a user account.					

Other information (specify)
Call log information, which includes phone number, date of call, and time of call; passwords chosen by users to access their voicemail messages.

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

Directly from individual about whom the information pertains					
In person		Hard copy: mail/fax		Online	
Telephone	X	Email			
Other (specify): Voicemail messages are received by telephone (though the individual who left the voicemail is not always the subject of the voicemail). No other information in the system is collected directly from users.					

Government sources					
Within the Component	X	Other DOJ components	X	Other federal entities	X
State, local, tribal	X	Foreign	X		
Other (specify): Because calls could originate from any location, the system could maintain voicemail messages from any type of government source, and call log information could be generated based on calls from any type of source; thus, all boxes above have been checked. User account information originates only from within the Department.					

Non-government sources					
Members of the public	X	Public media, internet	X	Private sector	X
Commercial data brokers					
Other (specify): Because calls could originate from any location, the system could maintain voicemail messages from any type of non-government source, and call log information could be generated based on calls from any type of non-government source.					

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 that exists in light of the information collected is that the system may collect more information than is relevant or necessary to accomplish the Department's official duties. For example, a member of the public who mistakenly believes that his/her personal issue is within the scope of a DOJ component's responsibility could leave a voicemail message for a DOJ employee in which he/she describes her issue, allowing JVS to record call log information as well as the voicemail message. JVS maintains only a small quantity of information concerning DOJ personnel and individuals who communicate with DOJ personnel through JVS: user account information (name,

phone number, workstation IP address); call log information (phone number of caller, date and time of call); voicemail messages (as well as passwords chosen by users to access their voicemail messages); and logs of system administrator activity. Call log information does not include names of callers or recipients. This is the minimum amount of information necessary to facilitate telephone communication among DOJ personnel and between DOJ personnel and non-DOJ personnel (as well as to comply with applicable IT security requirements). With the exception of voicemail messages (and passwords), the information is not particularly sensitive, and all the information is used only for business purposes. Further, DOJ personnel are advised to delete voicemail messages when they are no longer needed to help ensure that their voicemail boxes have enough room for future messages.

A potential threat to privacy that exists in light of the sources of information is that because most of the information maintained by the system is not collected directly from the subject of the information, there may be an increased likelihood that the information is not completely accurate.

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.)

Although the information collected and maintained by JVS supports each of the various substantive and administrative missions carried out by Department of Justice components, the core purpose of JVS is to facilitate telephone communication among DOJ personnel as well as between DOJ personnel and non-DOJ personnel in order to help components perform their official duties.

Purpose			
	For criminal law enforcement activities		For civil enforcement activities
	For intelligence activities	X	For administrative matters
	To conduct analysis concerning subjects of investigative or other interest		To promote information sharing initiatives
	To conduct analysis to identify previously unknown areas of note, concern, or pattern.		For administering human resources programs
	For litigation		
X	Other (specify): To facilitate telephone communication among DOJ personnel as well as between DOJ personnel and non-DOJ personnel in order to help DOJ components perform their official duties		

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.

Information maintained by JVS is used in order to provide IP-based telephone services and voicemail services to DOJ personnel. These services support the execution of the Department's official

duties. Only a minimal amount of information regarding individuals is used to place and receive telephone calls as well as to store and access voicemail messages. Telephone users must be uniquely identified by telephone number in order to receive calls. Records of received calls (by number) are used by the receiver to answer calls or store telephone numbers. User-chosen passwords are collected and maintained by the system to ensure that only the authorized user may access voicemail messages assigned to a particular telephone number. Call log information is maintained only temporarily in case it is needed for call quality troubleshooting or for billing issues (for toll calls). All information concerning JVS users is considered internal to DOJ and the service provider (AT&T) and is not disseminated to other agencies or individuals (except to the extent that information, such as call log information and voicemail messages, is released as a result of an outgoing call).

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; Federal Information Security Management Act, 44 U.S.C. § 3541 et seq. (collection of audit information)
	Executive Order	
	Federal Regulation	
	Memorandum of Understanding/agreement	
X	Other (summarize and provide copy of relevant portion)	Contract with AT&T to provide the managed service as part of the GSA Networx Enterprise Services contract.

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.)

As mentioned above, JVS (including information stored on the system) is operated by the service provider, AT&T. Occasionally, AT&T provides call log information to the Department so that it may evaluate the effectiveness of the service provider, verify billing charges, and perform trouble-shooting. The system maintains user account information only for the duration of a user's association with the Department. Users can save voicemail messages for as long as they need them, but users will be prompted to delete old voicemail messages when their storage capacity reaches its limit (30 or 60 minutes depending on the user). Any voicemail messages saved by a user will be deleted when the user leaves the Department. Call log information maintained by the system is generally overwritten after 30 days; to the extent that call log information has been incorporated into certain billing reports generated by AT&T and periodically provided to the Department, such information may be retained for up to three years in accordance with the retention schedule applicable to such reports (General Records Schedule 12, Communications Records, Telephone Use (Call Detail) Records – Destroy when 3 Years Old).

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 use of information in JVS 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), 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.

There is generally no need to share system data (including user account information and call log information) outside of the component. While system data is not ordinarily disclosed outside the component, users can look up a DOJ individual's contact information in the Department's Global Address List (which is not part of JVS).[2]

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component			X	
DOJ components	X			X - If requested for an authorized investigation (administrative, OIG, law enforcement).
Federal entities				
State, local, tribal gov't entities				
Public				
Private sector				
Foreign governments				
Foreign entities				

[2] Note that voicemail messages could conceivably be left with almost any type of recipient; this table reflects how other information in the system may be shared.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Other (specify):				X - As may be required by law/legal process.

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: Notice is also provided through this privacy impact assessment.
	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: To facilitate official communication, all DOJ personnel are assigned user accounts. For administrative purposes, all calls made by DOJ personnel generate call log information. With the

		exception of voicemail messages, information in the system is either assigned to users by the Department using existing directories (user account information) or is automatically generated by the system (call log information).

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 Department is not required to give users an opportunity to consent to particular uses of this information. Nevertheless, if a component wishes (for example) to suppress its users' names from showing up on caller IDs for a business purpose~~s~~, this request can be accommodated.

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.

For user account information and audit log information of system administrator activity, notice is provided by the Privacy Act system of records notice 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)).

For other information maintained by JVS, this privacy impact assessment provides notice of the maintenance of such information, as well as the safeguards that have been applied to such information.

DOJ personnel do not have an opportunity to decline to provide information. All DOJ personnel are assigned user accounts in order to facilitate official communication. All calls made by DOJ personnel generate call log information for administrative purposes. Note that information in the system is generally not collected directly from users; with the exception of voicemail messages (and voicemail passwords), information in the system is either assigned to users by the Department using existing directories (user account information) or is automatically generated by the system (call log information). Members of the public can choose not to call a DOJ telephone number.

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: 12/17/2012 If Certification and Accreditation has not been completed, but is underway, provide status or expected completion date:
X	A security risk assessment has been conducted.
X	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: As part of the security certification for JVS, a security risk assessment was completed based on applicable standards and controls issued by the National Institute of Standards and Technology (NIST) and DOJ, as tested and documented in the DOJ Cybersecurity Assessment and Management Tool (CSAM). Examples of such controls include: logical access to system databases is restricted to system administrators, who can only access such databases from AT&T's management network using unique authentication; these databases are protected from unauthorized access by a firewall, and are connected to AT&T's telephone network via restricted access to AT&T's private IP cloud; voicemail and IP telephony devices are managed in accordance with DOJ policy and vendor-recommended alerts for patches and security code updates.
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: JVS is monitored internally by DOJ, including the Justice Security Operations Center, which receives bulk data feeds of network traffic for monitoring and analysis, as well as by the service provider (AT&T) for data that traverses its private network. Security-relevant actions by system administrators are logged. System configuration changes are tested by the vendor and authorized through the federal Configuration Control Board approvals process. This process includes a security review of potential impacts, including impacts to PII and other data. Security assessments are a continuous process which begins with certification and accreditation and includes annual testing of DOJ core controls and re-testing of certain security controls each year. The service provider is required by contract to safeguard DOJ-owned data, and this performance is evaluated by the program office on an ongoing basis.
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: The system maintains audit log information of system administrator activity. Only DOJ-cleared AT&T personnel are authorized to serve as system administrators. Administrator roles are requested and assigned based on separation of duties and minimum/need-to-know access. Accounts and role privileges are reviewed by the vendor every 90 days to ensure access is valid. Administrators must sign and agree to comply with DOJ privileged user rules of behavior.
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.
	X	Training specific to the system for authorized users outside of the component (AT&T).
		Other (specify):

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

In addition to the controls described in section 6.1, the following access and security controls have been utilized to protect privacy by reducing the risk of unauthorized access and disclosure:

- JVS operates on JUTNet, which is secured at the highest level for an unclassified system against hazards such as intrusion, malware, and internet attack. JUTNet traffic is continuously monitored by DOJ security personnel within the Justice Security Operations Center. Within JUTNet, JVS is segregated from other data systems (by a dedicated firewall) in order to avoid intermingling of access, processing, or storage.
- Access to the system (as distinguished from use of the system by ordinary users) is limited to system administrators – AT&T personnel who must be cleared by DOJ and who can access the system only from the AT&T management network after providing unique authentication. System administrators must sign and agree to comply with DOJ privileged user rules of behavior. Administrator roles are assigned based on separation of duties and the principle of minimum access/need to know.
- The system generates audit log information of system administrator activity.
- The service provider, AT&T, is not authorized to disclose system information except in performance of its contract with the General Services Administration.
- Call log information is maintained for a short period of time (30 days) on limited access servers and is not routinely used by AT&T or DOJ personnel except if needed for a specific business purpose such as troubleshooting or to generate a billing report.
- Other applicable controls as required by FISMA as well as DOJ and NIST standards.

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-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))
	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.

JVS generates and maintains audit log information of system administrator activity, and such information is retrieved by administrator ID or other identifier. Additionally, for the purpose of user account administration, system administrators retrieve user account information (such as name, phone number, and workstation IP address) by personal identifier such as the user's name or phone number. User account information and audit log information is covered by 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)).

While DOJ personnel routinely search the Department's Global Address List (GAL) by name and retrieve phone numbers and other contact information, such information is part of the GAL as opposed to JVS, and is covered by DOJ-014, Department of Justice Employee Directory Systems, 74 Fed. Reg. 57194 (Nov. 4, 2009).