Department of Justice
Justice Management Division

Privacy Impact Assessment
for the
eDiscovery System

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

Approved by: Peter Winn, Acting Chief Privacy and Civil Liberties Officer, Department of Justice

Date approved: December 18, 2018]

(May 2015 DOJ PIA Form)

EXECUTIVE SUMMARY

The Department of Justice (DOJ or Department), Justice Management Division (JMD), Office of the Chief Information Officer, eDiscovery Program, is responsible for providing electronic discovery support for the DOJ senior leadership offices (Office of the Attorney General, Office of the Deputy Attorney General, and Office of the Associate Attorney General) and various other offices and components within the Department in response to Freedom of Information Act (FOIA) requests, litigation, investigations, Congressional requests, and other related matters. The eDiscovery Program utilizes its eDiscovery System to search, retrieve, process, and produce electronic records stored in various systems owned by the Department. The eDiscovery Program has utilized applications such as Clearwell and Relativity to facilitate the discovery process and may employ other applications with similar capabilities. These discovery tools make up the eDiscovery System. This Privacy Impact Assessment is being conducted because the system retrieves, processes, and stores personally identifiable information (PII).

Section 1: Description of the Information System

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

The eDiscovery System provides a tool to search, retrieve, process, and produce Electronically Stored Information (ESI) in response to FOIA and litigation requests, investigations, and other related matters. Requests for searches may be made by Department FOIA professionals, attorneys, or other designated employees in accordance with Department policy. These production requests can be extremely burdensome, often reaching back decades and can include thousands of electronic files. The eDiscovery System is designed to facilitate responses to these requests, while minimizing the time and effort required to satisfy these requests and increase the accessibility of ESI.

(b) the way the system operates to achieve the purpose(s);

Internal DOJ requestors identify custodians, search terms, and date ranges likely to return records relevant to particular requests or investigations. Internal DOJ requestors may include DOJ staff, contractors, detailees and assignees. Custodians are individuals with whom ESI is associated, such as the sender or recipient of an email. Custodians may include DOJ employees, contractors, detailees, assignees, and other individuals who maintain electronic profiles at the Department. ESI associated with selected custodians is copied to the eDiscovery System and, where necessary, converted to text searchable files. Users can then search the ESI using the identified search terms. Responsive records are then reviewed to determine whether they are relevant to a particular request. Files which may be relevant to a request are grouped into a smaller project file and provided to the internal requestor via the eDiscovery System. The internal requestor may then select, retrieve, and redact those files necessary for production in a given request. The eDiscovery Program utilizes applications such as Clearwell and Relativity to facilitate this process.

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

The eDiscovery System contains user contact information of DOJ end-users (custodians) and non-DOJ individuals who communicate with DOJ end-users, email messages (including any attachments), calendar information, audit log information, electronic files, and other electronic records maintained by the Department that may be relevant to support discovery requests as mandated by both law and policy. Such data may include significant quantities of personal information relating to substantive work of the Department. Because of the varied nature of the Department's work and because electronic records could conceivably include almost any type of PII, it is not possible to list with certainty every datum point of ESI that will be collected, maintained, or disseminated by the system. ESI collected by the eDiscovery System is grouped into project files, which are labeled and identified by an assigned case number, the requesting DOJ component, and the name of the requestor, and will include established parameters of the search (e.g., date ranges, search terms, custodians).

(d) who has access to information in the system;

eDiscovery administrators create user accounts, which are granted to users on a case-by-case basis. Only eDiscovery administrators have access to all cases and related data. eDiscovery administrators are eDiscovery Program staff, contractors, and detailees. End-users may be located within the eDiscovery Program or throughout the Department and include DOJ staff, contractors, detailees, and assignees. End-users outside the eDiscovery Program have limited access only to the cases files to which they are assigned.

(e) how information in the system is retrieved by the user;

Case data may be retrieved by the case number, custodian, or keyword search criteria.

(f) how information is transmitted to and from the system;

The eDiscovery System accesses DOJ data repositories directly and creates and imports copies of the relevant electronic files contained therein.

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

The eDiscovery System connects with other systems and databases that maintain electronic records, such as the Email and Collaboration Services (ECS), a DOJ configured deployment of Microsoft Office 365, and archival databases such as Global Services Domain (GSD) file and print servers and GSD Enterprise Vault 10 (and subsequent versions).

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

The eDiscovery system is a minor application.

Section 2: Information in the System

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

The eDiscovery System contains user contact information of DOJ custodians and non-DOJ individuals who communicate with DOJ custodians, email messages (including any attachments), calendar information, audit log information, electronic files, and other electronic records maintained by the Department that may be relevant to support discovery requests as mandated by law and policy. Such data may include significant quantities of personal information relating to substantive work of the Department. Because of the varied nature of the Department's work and because electronic records could conceivably include almost any type of PII, it is not possible to list with certainty every datum point of information that will be collected, maintained, or disseminated by the eDiscovery System. Records may include any and all of the categories of information listed below. Responsive records are provided to internal DOJ requestors in full, but may be redacted prior to distribution outside the Department.

Therefore, the items of information checked below are limited to search request parameters, administrator and end-user information, and log information, maintained by the eDiscovery System.

Identifying numbers					
Social Security		Alien Registration		Financial account	
Taxpayer ID		Driver's license		Financial transaction	
Employee ID		Passport		Patient ID	
File/case ID	X	Credit card			
Other identifying numbers (specify):					

General personal data					
Name	X	Date of birth		Religion	
Maiden name		Place of birth		Financial info	
Alias	X	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		Telephone number		Salary	
Job title		Email address		Work history	

Work-related data					
Work address		Business associates			
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	
Other system/audit data (specify):					

Other information (specify)

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	X
Telephone		Email	X		
Other (specify): Information about the specific requestor is provided via email directly to eDiscovery Program staff. Other information is stored in DOJ data repositories or accounts.					

Government sources					
Within the Component	X	Other DOJ components	X	Other federal entities	
State, local, tribal		Foreign			
Other (specify): The eDiscovery System only searches DOJ data repositories; however, initial requests may come from external entities via internal DOJ requestors. The identification of those external requestors and contact information would be maintained by the eDiscovery Program, but is not entered into the eDiscovery System. Additionally, ESI may be stored in the eDiscovery System from all of the entities listed above, either because those entities communicated with a DOJ custodian or because information from those entities or about those entities was maintained by a DOJ custodian.					

Non-government sources					
Members of the public		Public media, internet		Private sector	
Commercial data brokers					
Other (specify): The eDiscovery System only searches DOJ data repositories; however, initial requests may come from external entities via internal DOJ requestors. The identification of those external requestors and their contact information would be maintained by the eDiscovery Program, but is not entered into the eDiscovery System. Additionally, ESI may be stored in the eDiscovery System from all of the sources listed above, either because those sources communicated with a DOJ custodian or because information from those sources (i.e., daily news briefs from public media) or about those sources was maintain by the DOJ custodian.					

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.)

It is possible that in copying custodians' complete files and communications, personal data or data not relevant to a particular case or investigation will be pulled into the eDiscovery System. For this reason, only eDiscovery Program personnel and administrators are provided access to complete custodian files. Individual requestors are only provided access to those files with hits on the search terms or parameters previously set and approved in coordination with the eDiscovery Program team. Following production of the files to the internal DOJ requestors, further review is conducted to remove files not considered relevant to the specific case or investigation. Prior to release to external requestors or requestors without a need to know, redactions may be made to mask confidential or sensitive information, such as PII.

Additionally, the information sent through or stored in the eDiscovery System is governed 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 these underlying systems. In the SORNs, the agency describes the scope of the categories of records that may be collected as well as the categories of individuals about whom information may be collected.

For information about security controls that have been applied to the eDiscovery System to mitigate the privacy risks associated with the information collected, 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.)

Purpose			
	For criminal law enforcement activities		For civil enforcement activities
	For intelligence activities	X	For administrative matters
X	To conduct analysis concerning subjects of investigative or other interest		To promote information sharing initiatives
	To conduct analysis to identify previously unknown areas of note, concern, or pattern.		For administering human resources programs
X	For litigation		
X	Other (specify): To respond to FOIA requests and Congressional requests		

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.

The Department of Justice is subject to both legal obligations and policy mandates, which require the production of electronic records upon the issuance of appropriately authorized requests or legal orders. The information requested may be relevant to establishing the Department's position on or knowledge of particular areas of interest to the public (e.g., FOIA requests) or legal matters (e.g., civil and criminal litigation requests). The information may also be relevant to internal investigations, such as Inspector General or Equal Employment Oppurtunty investigations, and may be used to vet executive and judicial nominations, and for other related matters. Department policy governs authorized purposes for conducting searches of ESI.

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. §552. Public information; agency rules, opinions, orders, records, and proceedings; Inspector General Act of 1978, as Amended; 2 U.S.C. Chapter 6, Congressional and Committee Procedure; Investigations.

	Executive Order	
X	Federal Regulation	28 C.F.R Part 16—Production or Disclosure of Material or Information.
	Memorandum of Understanding/agreement	
X	Other (summarize and provide copy of relevant portion)	Federal Rules of Criminal Procedure; Federal Rules of Civil Procedure.

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.)

National Archives and Records Administration (NARA) approved Records Retention Schedule DAA-0060-2017-0007, related to records documenting compliance with preservation obligations for component information, is a functional, DOJ-wide schedule. It covers administrative and operational records created as a result of a request for Department records relevant to efforts to search, analyze, and potentially produce DOJ component information in response to a formal request for DOJ information. The schedule addresses records in the custody of the responding DOJ component that reflect communications and document the responses and actions of the responding component. This schedule does not address records produced by DOJ counsel in the context of litigation in which the Department is counsel of record and not a party to the action. The schedule deems covered records to be temporary with a retention of three years after the termination of any obligation to preserve records for litigation matters.

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.)

The eDiscovery System has access to a DOJ custodian's entire electronic profile, including emails sent to and from the custodian, calendar entries, metadata, and electronic files stored by the custodian on DOJ systems. These profiles may contain personal and sensitive information. Because of the nature of the system and the scope of information being searched, there is a risk that the eDiscovery system will over-collect information that is not considered relevant or responsive to a specific request. Additionally, there is a risk that end-users may make unauthorized disclosures or use the data in an unauthorized manner. In order to safeguard this information, users are required to complete mandatory training prior to accessing the system, which includes instructions on utilizing redaction and secondary review functions. DOJ end-users are also required to take annual privacy and security training and agree to specific Rules of Behavior upon entering the Department and accessing DOJ systems.

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component	X		X	
DOJ components	X		X	
Federal entities	X			
State, local, tribal gov't entities	X			
Public	X			
Private sector	X			
Foreign governments	X			
Foreign entities	X			
Other (specify):				

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.)

The consolidation, management, and use of ESI information as part of the eDiscovery Program for the purpose of providing DOJ with electronic discovery support creates certain privacy risks. Specifically, DOJ employees and contractors with access to review and use PII in the system create external and internal threats to the use of information.

To mitigate these risk, and as discussed in Section 6.2 below, the eDiscovery Program limits access to records based on a need-to-know. Requests for access must be approved by the JMD Deputy Assistant Attorney General for Policy, Management, and Planning. Upon receipt of authorization, requests are granted on a case-by-case basis. DOJ users located outside the eDiscovery Program are only granted limited access to ESI considered relevant or responsive to their particular projects. Although individuals outside the Department are not permitted access to the system, DOJ end-users may provide data from the eDiscovery system to the individuals and entities noted in Section 4.1, upon request. Prior to production outside the Department, ESI is further reviewed, culled, and redacted to ensure only

relevant information is shared with external requestors. DOJ users are also required to take annual privacy and security training, which contain specific guidance on the handling of sensitive information, and they must agree to specific Rules of Behavior upon entering the Department and accessing DOJ systems.

The eDiscovery System utilizes incident response plans applicable to the Justice Security Operations Center, which include continuous monitoring functions and require that incidents such as breaches be reported within one hour of identification.

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 end 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. In compliance with DOJ Order 2740.1A, internal requestors notify all current custodians that their data is being searched.
	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: Individual custodians do not have the ability to decline to provide information. Official business records are created through their work and, once created, become DOJ records, searchable and subject to discovery through a number of channels.

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: Upon entering the Department and gaining access to DOJ systems, individuals are provided with notice that data processed or retained on DOJ systems may be utilized for authorized Government purposes. Consent is provided as a condition of employment, but consent is not requested for all of the specific circumstances or uses that may arise.

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.

Prior to accessing the eDiscovery System, users are provided with the following notice:

> You are accessing a U.S. Government information system, which includes: (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only. Unauthorized or improper use of this system may result in disciplinary action, and civil and criminal penalties. By using this information system, you understand and consent to the following: You have no reasonable expectation of privacy regarding any communications transmitted through or data stored on this information system. Any communications transmitted through or data stored on this information system may be disclosed or used for any U.S. Government-authorized purpose. For further information see the Department order on Use and Monitoring of Department Computers and Computer Systems.

A similar notice is provided when DOJ personnel access DOJ systems. Prior to the search of current DOJ custodian files, the custodians are notified of the requirement to search. Former DOJ employees are not provided with notice when search requests are submitted, however, employees departing under normal circumstances are given an opportunity to remove non-business, personal communications and documents from their permanent file prior to leaving the Department.

Individuals who communicate with DOJ personnel are not provided with notice and are not given an opportunity to consent to the search and retention of those communications.

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: 10/12/2017 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: 10/12/17	
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse.	
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: Job logs are reviewed on a daily basis to ensure users are properly accessing records for approved purposes and no unauthorized access has occurred. Additionally, DOJ Cybersecurity Services Staff (CSS) uses antivirus software to detect problems. When problems arise, CSS is notified automatically and requests eDiscovery Program assistance when needed.	
X	Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act. [While contracts should contain provisions mandating compliance with the Privacy Act, the eDiscovery System owners do not have access to all of the contracts for support personnel throughout the Department; however, per Department procurement policy, any contract, order or other commitment under which the contractor, or a subcontractor, may access, collect, store, process, maintain, use, share, retrieve, disseminate, transmit, or dispose of DOJ Information, must comply with existing Federal Acquisition Regulation requirements. Individual DOJ components must monitor and ensure compliance within their organizations. All contractors supporting the eDiscovery Program are required to comply with 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.
		Other (specify):

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

The following access and security controls have been utilized to protect privacy by reducing the risk of unauthorized access and disclosure:

- The eDiscovery System has a security categorization of FISMA moderate. As a result, the eDiscovery System has assessed and implemented all applicable security controls to ensure protections commensurate with the impact to Department from any unauthorized access or disclosure of information.
- The system restricts access to those individuals with a specific need to review and process the data. Only eDiscovery Program personnel are granted access to search and retrieve all custodian data. Non-program personnel are only granted access to data that has been previously culled to isolate those electronic records, which may be relevant to their specific request.
- 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.
- 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.
- All users must complete computer security awareness training annually, as well as review 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.

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: • JUSTICE/DOJ-002, DOJ Computer Systems Activity & Access Records, last published in full at 64 FR 73585 (Dec. 30, 1999), and modified at 66 FR 8425 (Jan. 31, 2001), and 82 FR 24147 (May 25, 2017); • JUSTICE/DOJ-004, Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Records, last published in full at 77 FR 26580 (May 4, 2012),

	and modified at 82 FR 24151, 152 (May 25, 2017); • ESI created by the Senior Management Offices, Senior Leadership Offices, and Justice Management Division is covered by the Department's litigation and general leadership case file SORNs. These SORNs include, but are not limited to: o JUSTICE/CIV-001, Civil Division Case File System, last published in full at 63 FR 8659, 665 (Feb. 20, 1998) with modifications at 66 FR 8425 (Jan. 31, 2001), 66 FR 17200 (Mar. 29, 2001), 66 FR 36593 (July 12, 2001), and 82 FR 24147 (May 25, 2017); o JUSTICE/CRM-001, Central Criminal Division Index File and Associated Records, last published in full at 72 FR 44182 (Aug. 7, 2007) and modified at 82 FR 24151, 155 (May 25, 2017); o JUSTICE/OAG-001, General Files System, last published in full at 50 FR 37294 (Sept. 12, 1985) with modifications at 66 FR 8425 (Jan. 1, 2001), and 82 FR 24147 (May 25, 2017); o JUSTICE/ASG-001, General Files System of the Office of the Associate Attorney General, last published in full at 69 FR 22872 (Apr. 27, 2004) with modifications at 82 FR 24147 (May 25, 2017); o JUSTICE/DAG-013, General Files System, last published in full at 57 FR 8474 (Mar. 10, 1992) with modifications at 66 FR 8425 (Jan. 31, 2001), and 82 FR 24147 (May 25, 2017) • JUSTICE/DOJ-014, Department of Justice Employee Directory Systems, last published in full at 74 FR 57194 (Nov. 4, 2009), and modified at 82 FR 24151, 153 (May 25, 2017); • Other published DOJ SORNs depending on the nature of information in the ESI 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.

Information is organized by the custodian's name and indexed within the eDiscovery System. Once the data is indexed, the data can be retrieved by full-text search capability, including the file name, the custodian's name, search terms, etc.