Department of Justice

Civil Division

Privacy Impact Assessment
for the
Office of Litigation Support Servers Systems

Issued by:
Angie E. Cecil

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

Date approved: September 27, 2018

EXECUTIVE SUMMARY

The Civil Division's Office of Litigation Support Servers Systems (OLSSS) provides an automated litigation environment to support the management of cases for the attorneys and staff members of the Civil Division (Division), U.S. Department of Justice (DOJ). OLSSS is designed to offer a wide range of services and products that help attorneys and other professional staff acquire, organize, analyze and present evidence or other data as part of investigations and litigation. Through the use of computer data processing, image management, trial presentation systems, and other technologies, litigation materials are effectively organized so the litigating attorneys and other professional staff can rapidly locate information and make the best use of it in conducting an investigation, litigation, or settlement negotiation. OLSSS offers these services and products to Civil Division attorneys and other professional staff members by providing a flexible network infrastructure and multiple server platforms with a scale-able storage capacity designed to ensure data integrity and a secure environment necessary to support the Civil Division's varied investigations and litigation. Most cases litigated within Civil Division have data residing on the system.

The Civil Division conducted this PIA to comply with the E-Government Act of 2002, the Federal Information Security Modernization Act, the Department of Justice Security and Privacy Assessment and Authorization Handbook, and National Institute of Standards and Technology Special Publication 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. Based on these requirements, the Civil Division determined that OLSSS maintains sensitive material, including information about individuals that is protected by various privacy statutes, regulations, and guidance.

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).

a. The purpose that the records and/or system are designed to serve:
OLSSS hosts litigation support databases, document repositories, and collaborative work environments within the Department of Justice's secure Justice Consolidated Office Network (JCON). The system allows authorized DOJ trial teams and non-DOJ individuals participating

in the case, such as experts, litigation consultants, client agencies, and co-counsel, to share the same set of case data in a secure and collaborative environment.

b. The way the system operates to achieve the purpose(s):
OLSSS is a group of servers that provide a platform for a variety of software tools to support investigation and litigation efforts within the Division. A list of the software tools and applications is attached as Appendix A.

c. The type of information collected, maintained, used, or disseminated by the system:
OLSSS houses data collected in the course of a Civil Division investigation or litigation. This information may include information generated by the Division's client agencies and provided to the Division in support of an investigation or litigation, such as information related to policies, regulated industries, entities investigated by the government, or individuals. The information may be collected as part of a client-agency's investigation and provided to the Division or may be produced to the Division by an opposing party or a third party in the course of the discovery process overseen by the federal courts.

d. Who has access to information in the system:
The information maintained in OLSSS may be accessed by authorized Civil Division employees, other federal employees, and contractors. Before access is authorized, the individual's access rights and purpose for accessing the documents are reviewed by the Civil Division's IT security staff. To this end, the Civil Division places strict access controls on OLSSS via physical and electronic means in order to secure the information. For example, Civil Division employees and contractors, and all those working in a software tool or application, are only granted access to databases on the system that support a matter they are working on. Databases are case-specific. If an employee or contractor leaves or is reassigned, their account access is disabled or access to a particular database may be rescinded.

e. How information in the system is retrieved by the user:
There are several methods of retrieval in the system: file and folder access, or via unstructured query within an application. A user can retrieve information using unique identifiers such as: date of birth, name, address, Social Security Number or case file number. A user can also conduct a keyword search. File and folder searches occur in the limited file or folder designated by the search criteria; unstructured searches are conducted across the database and are not limited to a particular file or folder.

f. How information is transmitted to and from the system:
Information is transmitted to and from the system by direct ingestion to and from hard drives and network connections. The files are collected from, or may be shared with, a client agency, opposing counsel, or another party involved in the investigation or litigation.

g. Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects):
OLSSS interconnects to CIV-JCON (Justice Consolidated Office Network), which is a general support system that houses Civil Division network equipment and services, including email, system support databases, and network drives. The tools and applications that are hosted on

OLSSS are discussed in Appendix A.

h. Whether it is a general support system, major application, or other type of system: General Support System.

Section 2: Information in the System

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

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

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

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

Distinguishing features/Biometrics					
Fingerprints	X	Photos	X	DNA profiles	
Palm prints	X	Scars, marks, tattoos	X	Retina/iris scans	
Voice recording/signatures	X	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):					

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	X	Online	
Telephone		Email	X		
Other (specify): Information collected in the course of discovery may be collected from individuals who are opposing parties in the litigation. The request for such information would be through the discovery process overseen by the court. To the extent information located on OLSSS is related to the September 11 Victim Compensation Fund system, the original claim-related information would be collected from individuals. The September 11th Victim Compensation Fund PIA fully evaluates the protections for information in that system.					

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.)

As described above, the information contained in and managed on OLSSS is provided to the Civil Division in the course of litigation. The documents are typically provided by another Department of Justice component or another federal or state entity involved in the investigation. The information may also be received from an individual if the Civil Division is handling the representation of the individual or the information was submitted by the individual as part of a compensation program. Other information may be produced by the opposing party or a third party in the litigation in response to a subpoena or other discovery request. The privacy risks associated with collecting records from other entities, such as regulated entities, businesses, other government agencies, is that they will share information outside the scope of the investigation or not properly identify the data being ingested into the system as containing personally identifying information.

Preventing the exposure of the data once is it received by the Civil Division minimizes the risk that personal information will be shared outside the team of individuals working on a particular matter. To address that concern, the system is configured with multi-factor authentication, which requires all authorized users to provide two levels of authentication prior to accessing any data hosted on the system. In addition, the Civil Division places strict access controls on OLS System Servers via physical and electronic means in order to secure the information. For example, databases are case-specific and Civil Division employees and contractors are only granted access to databases on the system that support a matter they are working on. If an employee or contractor leaves or is reassigned, their account access is disabled or access to a particular database may be rescinded.

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			
[X]	For criminal law enforcement activities	[X]	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
[X]	To conduct analysis to identify previously unknown areas of note, concern, or pattern.	[ ]	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.

The Civil Division's litigation mission includes civil and criminal enforcement investigations and actions as well as defensive work on behalf of the United States government. The information collected is used to accomplish activities inherent in the Division's investigations and litigation, including: reviewing documents for relevance to claims and defenses involved in the litigation; conducting privilege reviews of documents collected in the investigation; tracking the use of documentary evidence in litigation; preparing witness kits/binders for depositions and hearings; and selecting and preparing exhibits for trial. To the extent information is hosted on OLSSS related to compensation funds administered by the Division, the information collected is necessary for the administration of claims. Collection, maintenance, and use of the information supports the Civil Division's litigation and administrative functions.

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	28 USC §§ 514-19
	Executive Order	
X	Federal Regulation	28 C.F.R. §§ 0.45-0.49, Subpart I.
	Memorandum of Understanding/agreement	
	Other (summarize and provide copy of relevant portion)	

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.)

Data will be retained in the system until the DOJ Civil Division case attorney and the Office of Litigation Support determine that the litigation materials no longer need to be stored. Information no longer needs to be maintained after a case has closed or settled, and the information is not needed for other cases or investigations. In consultation with the attorney assigned to the matter, the Office of Litigation Support will dispose of data that does not need to be maintained pursuant to the Division's obligations under the Federal Records Act. Information that must be maintained will be retained in accordance with the applicable retention schedule, outlined below. Closing a case through these steps means that the data is provided on an external hard drive or other media to the attorney handling the matter. Subsequently, the case data is deleted from OLSSS. The space previously used by the closed case is re-used and made available for other matters. A copy of the data will remain on OLSSS's backup tapes for

approximately one year after the case closes, after which the backup tape is overwritten with new data.

Files managed on OLSSS may include both federal records and non-records that are associated with a variety of different types of Civil Division's litigation case files. The retention policies for the files depend on the federal record status as well as the classification of the type of case file to which the files pertain. The Department of Justice record retention schedules are published at https://www.archives.gov/records-mgmt/rcs/schedules/index.html?dir=/departments/department-of-justice/rg-0060. Record retentions for case files range from approximately 5 years to 65 years after the case closure date. Temporary records are destroyed at the end of the retention period, and permanent records are transferred to the custody of the National Archives and Records Administration. Non-records, such as duplicates and unnecessary discovery or other submitted documents, are destroyed when no longer needed for convenience of reference.]

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.)

There is a potential risk to privacy that could result from the improper access to information in the system; however, security protections that authorize and limit a user's access to information within the system mitigate the risk. Physical controls such as secured entrances and security officers protect access to the building where the servers and workstations are located. To access the system, the Civil Division enforces Department IT security standards for accessing a network system. In addition, before a user is granted access to a system hosted on OLSSS, the user completes required security training, including cybersecurity training and privacy training targeted to the user's role. Individuals outside the Civil Division are required to sign a confidentiality agreement and rules of behavior documents before they are provided with access accounts. In addition, all contractors granted access to the system must adhere to the Department's IT security standards for reporting security incidents. When an individual is granted access to a database on the system, the access is limited to that particular database or group of files within a particular application or tool. The user does not gain open access to all applications or databases housed on OLSSS.

Information access to the system is granted on a need-to-know basis. For example, Civil Division attorneys, other staff members, other federal employees, and contractors are only granted limited access to the matters they work on, not the entire system. The System Administrators monitor system logs and errors, and perform system-wide queries to detect privacy risks. The individual tools and applications also have auditing tools to review user activity, allowing the Civil Division to monitor user access within the system. The Civil Division follows DOJ internal policies and procedures for unauthorized access or release of information from the system.

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]	[ ]	[ ]	[ ]
State, local, tribal gov't entities	[X]	[ ]	[X]	[ ]
Public	[ ]	[ ]	[ ]	[ ]
Private sector	[X]	[ ]	[ ]	[ ]
Foreign governments	[ ]	[ ]	[ ]	[ ]
Foreign entities	[ ]	[ ]	[ ]	[ ]
Other (specify):	[X]	[ ]	[X]	[Opposing counsel, expert witness]

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 Civil Division utilizes a variety of controls to prevent or mitigate threats to privacy when sharing information with entities outside of the Division. For situations in which another federal agency, component of DOJ, state or local entity, or expert witness has access to a case-specific database, security protections that authorize and limit a user's access to information within the system mitigate the risks to privacy. For example, the data maintained by OLSSS is protected through compliance with the Department's access control policy. To access the system, the Civil Division enforces Department IT security standards for accessing a network system. In addition, before a user is granted access to a system hosted on OLSSS, the user completes required security training, including cybersecurity training and privacy training targeted to the user's role. Individuals outside the Civil Division are required to sign a confidentiality agreement and rules of behavior document before they are provided with access accounts. For data in transit, the Civil Division utilizes Department-approved encryption technology and PII filtration for email services. In addition, all contractors, including expert witnesses, granted access to the system must adhere to the Department's IT security standards for reporting security incidents.

Information access to the system is granted on a need to know basis. Users both inside and outside the Civil Division are only granted limited access to the matters they work on, not the entire system. There are monitoring and auditing tools for each system to review user activity, allowing the Civil Division to monitor user access within the system. For data sets that contain particularly sensitive information, folder access is audited with greater scrutiny. The Civil Division follows DOJ internal policies and procedures for unauthorized access or release of information from the system.

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.	
[ ]	Yes, notice is provided by other means.	Specify how: [ ]
[ ]	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: [Documents are obtained through court order, warrant, subpoena, discovery requests, and other such legal means. In the context of adversarial proceedings, such as an investigation or litigation, consent, access, and amendment protections are not applicable to the records. For social media captures and web site collections, notice is not provided to individuals as the information is considered to be in the public domain.]

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: [Documents are obtained through court order, warrant, subpoena, discovery requests, and other such legal means. In the context of adversarial proceedings, such as an investigation or litigation, consent, access, and amendment protections are not applicable to the records. An opposing party may challenge the relevance of the information and not produce the information in litigation, but that challenge would be determined before the information is collected and maintained by OLSSS. For social media captures and web site collections, notice is not provided to individuals as the information is considered to be in the public domain.]

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.

[Unless individuals are opposing parties in litigation, individuals do not provide information directly to the Civil Division for use in OLSSS. In the context of adversarial proceedings, such as an investigation or litigation, consent, access, and amendment protections are not applicable to the records. Individuals who are opposing parties in litigation can object to the Division obtaining the information through the discovery process. Individuals whose information is collected in the course of litigation involving another entity, such as another government agency or business entity, may have the opportunity to consent at the collection from the other entity. If another government agency is involved in the investigation or litigation, the agency's System of Records Notice would provide notice that the information may be shared with the Department of Justice for the context of a civil or criminal investigation or litigation. For information collected from the internet, notice is not provided to individuals as the information collected is in the public domain.]

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: [12/01/2014] 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: [The Civil Division has applied the policies and procedures outlined in the DOJ Security and Privacy Authorization and Assessment Handbook and in DOJ's security tracking tool, Cyber Security and Assessment Management application.	
[X]	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: [Testing of the system is performed before an Authorization To Operate is issued as well as during operation by various IT security tools available within DOJ. Monitoring is performed in real-time by Civil Division IT staff in conjunction with Justice Management Division. Specifically, filters are in place so that Social Security Numbers cannot be transmitted by email to outside parties without Department-required encryption or other security measures. Evaluation is performed in real-time via several packages of software, in place on the local machines and listening on the network transmissions.]	
[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: [OLSSS complies with DOJ IT Security Standards-attribution to named individuals, disallowing test or training accounts, and strict compartmentalization of information and accounts.]	
[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.
	[ ]	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 information maintained on OLSSS is protected in accordance with applicable DOJ guidance, policies, and directives. OLSSS exists on a physically secure, environmentally protected, DOJ network. The network is protected by firewalls, and is administered by both DOJ and non-DOJ contractor personnel. Access to OLSSS is granted only to DOJ-approved

individuals who have signed a confidentiality agreement and system rules of behavior. Security training and a public-trust background check are performed on a regular basis on all staff who request access. Access to specific databases/folders/material is granted on a need to know basis by authorized Federal staff. Finally, all OLSSS accounts are "named user" accounts assigned to a single individual and require strong authentication. Test, training, or temporary accounts are not permitted in order to accurately log the individual accessing the information.

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/CIV-001, *Civil Division Case File System*, last published in full at 63 Fed. Reg. 8659, 665 (Feb. 20, 1998), https://www.gpo.gov/fdsys/pkg/FR-1998-02-20/pdf/98-4206.pdf.]
[ ]	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 about U.S. citizens or lawfully admitted permanent resident aliens is typically retrieved by full-text search. The search may be performed by an administrator across OLSSS or a user can conduct the search within the application database the user accesses. OLSSS privacy protections do not differ depending on whether the information about an individual is a U.S. citizen or a lawfully admitted permanent resident alien. First party's access to personal information retrieved in the system and potential amendment rights are controlled by the SORN listed above and may be covered by 5 U.S.C. § 552a(d)(5).]