[United States Department of Justice – Civil Division]

Privacy Impact Assessment
for the
Civil Division

Labat Anderson Relativity System (LARS)
and Labat Anderson Web (LAWEB)

Issued by:
[Angie E. Ceci]

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

Date approved: August 26, 2019

(May 2015 DOJ PIA Template)

EXECUTIVE SUMMARY

The Labat Anderson Relativity System (LARS) and Labat Anderson Web (LAWEB) systems provide support for the investigation and litigation functions of the Civil Division. The systems were procured via the Mega 4 contract, an indefinite delivery, indefinite quantity contract vehicle available for use by the Department of Justice (DOJ or "Department") litigating divisions, including the Civil Division ("Division"). Under Mega 4, PAE Labat, a government contractor, manages LARS and LAWEB, a child and parent system, respectively. LARS and LAWEB utilize iConnect and Relativity platforms for litigation support and allow Civil Division attorneys and staff, along with other authorized users, to review, search and run analytics on documents collected in the course of litigation or investigations. LARS and LAWEB also provide a collaborative work environment to allow authorized Civil Division trial teams and other authorized individuals participating in a case, including experts, litigation consultants, client agencies, and co-counsel, to share the same set of case data in a secure setting.

The Civil Division completed this Privacy Impact Assessment (PIA) to review and document the Division's use of LARS and LAWEB. (This PIA does not apply to other Department components' use of the systems.) The Division conducted the PIA to comply with the E-Government Act of 2002, the Federal Information Security Modernization Act of 2014 (FISMA), Department of Justice IT Security Standards and Security Authorization Process, and National Institute of Standards and Technology's Spec. Pub. 800-53 Rev. 4.

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:
The systems are used as an online web-based repository and application-hosting environment to support the Division's investigation and litigation functions. The systems host large litigation support databases, document repositories, and a collaborative work environment to allow

authorized Civil Division trial teams and other authorized individuals participating in a case, including experts, litigation consultants, client agencies, and co-counsel to share the same set of case data.

b) The way the system operates to achieve the purpose(s):
LARS and LAWEB use Relativity, iConnect, and other commercial off-the-shelf (COTS) software platforms to process, store, review, and analyze electronic documents.

c) The type of information collected, maintained, used, or disseminated by the system:
LARS and LAWEB house 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. 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 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 LARS and LAWEB may be accessed by authorized Civil Division employees, other federal employees, and other approved personnel. 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 via physical and electronic means in order to secure the information. For example, Civil Division employees and contractors 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, the account access is disabled and access to a particular database may be rescinded.

e) How information in the system is retrieved by the user:
The user retrieves the information in the system via a web browser search form that permits keyword searches applied to specific datasets for a case or matter the user is authorized to access. The search tool provides the capability through the web form; users search data across the case database by searching related keywords such as custodian names, dates, or any relevant information associated with a case or matter. The system will display the retrievable results in a web response message.

f) How information is transmitted to and from the system:
LARS and LAWEB transmit data via web based applications/systems using Hyper Text Transfer Protocol Secure (HTTPS) with Transport Layer Security (TLS) encryption using Federal Information Processing Standard (FIPS) 140-2 compliant encryption.

g) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects):
LAWEB and LARS are self-contained, contractor-owned and operated systems that do not interconnect with any other DOJ systems. The case information originates from DOJ Civil

Division or external parties via encrypted external hard drives or via secure online transport, is loaded into LAWEB and LARS, and is later retrieved via a secure web interface. The environment resides in a shared service infrastructure that connects to other contractor owned and operated systems. LARS is a sub-system of LAWEB; thus, it inherits the infrastructure, security, and monitoring controls from the parent system.

h) Whether it is a general support system, major application, or other type of system:
LARS and LAWEB are major applications.

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	

Distinguishing features/Biometrics					
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	
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	X
Telephone		Email	X		
Other (specify): Documents are obtained through litigation discovery.					

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.)

The information is collected to support the Civil Division's litigation and investigation functions. The process of collecting data is typically provided by another Department of Justice component, another federal or state entity involved in the investigation, or by the opposing party in the litigation and in response to a subpoena or other discovery request. The information may also be received from an individual if the Civil Division is handling the representation of the individual. Other information may be provided by the opposing party or third party in the litigation in response to a subpoena or other discovery request. The privacy risks associated with collecting records from other entities are that they may 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 it is 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 this end, the Civil Division places strict access controls on LARS and LAWEB via physical and electronic means. The Division utilizes an access management policy that requires all users to be authorized, all requests for access be supported with the appropriate justification, and all users to read and sign a Rules of Behavior Agreement. If an employee or contractor leaves or is reassigned, the account access is disabled, and access to a particular database is rescinded.

The system is also configured with multi-factor authentication. This requires all authorized users to provide two levels of authentication prior to accessing any data hosted on the system. Users may also request access to multiple databases, and are required to go through the request process for each database they wish to be authorized to access. The system is configured to ensure that access to a specific database and its content is restricted to only those users that have authorized access. The system is also monitored and audited to identify any unauthorized access attempts, and to verify the appropriate access levels have been granted to its users. The system is hosted behind security firewalls and intrusion detection systems. All sites are also encrypted using secure protocols (i.e. SSL & HTTPS). This ensures that all data transmissions are protected from compromise.

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
	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 actions as well as defensive work on behalf of the United States government. The information collected is used to accomplish activities related to the Division's investigations and litigation, including: reviewing documents for relevance to claims and defenses; 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. Collection, maintenance, and use of the information support 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	Please see citations included in regulation listed below.
	Executive Order	
X	Federal Regulation	28 C.F.R. §§ 0.45-0.49 Subpart I – Civil Division Federal Rules of Civil Procedure
X	Memorandum of Understanding/agreement	Federal Trade Commission (FTC)
X	Other (summarize and provide copy of relevant portion)	MEGA 4 Contract – DOJ Contract # DJJ13-C-2439

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, 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. Data will be disposed of after consultation with the case attorney. Archiving a case leaves the data with the attorney and available in another format or

location for the attorney to access in the future. The space previously utilized by the case in LARS and LAWEB is re-used (case is deleted, then space is made available elsewhere).

Files managed on LAWEB and LARS may include both federal records and non-records that are associated with different types of the Civil Division's litigation case files. The retention policies for the files depend on the federal record status and 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, 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 or storage of information longer than is required by the Civil Division's record-keeping requirements. Security protections that authorize and limit a user's access to information within the system mitigate the risk of improper access. Physical controls such as secured entrances and security officers protect access to the building in which the servers and workstations are located. To access the system, the Civil Division enforces Department standards for accessing a network system, such as Person Identity Verification (PIV) card entry. In addition, before a user is granted access to a system hosted by the Civil Division, 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.

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. Strict electronic access controls ensure that users are only able to access data collected in support of their specific investigation or litigation. Users may also request access to multiple databases, and are required to go through the request process for each database they wish to be authorized to access. The system is configured to ensure that access to a specific database and its content is restricted to only those users that have authorized access. The system is also monitored and audited to identify any unauthorized access attempts and to verify the appropriate access levels have been granted to its users.

There are monitoring and auditing tools for each system to review user activity, so the Civil Division can monitor user access within the system. Access controls are backed up by detailed audit logs that provide a detailed overview of how data has been accessed and used within the system to ensure compliance with applicable handling policies. In addition, the system generates detailed metadata and audit logging information that can help administrators manage data retention schedules as established for the system. The Civil Division follows DOJ internal policies and procedures for unauthorized access or release of information from the system. Additional information regarding cybersecurity protections are discussed in the last paragraph of Section 4.2 below.

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		X	
State, local, tribal gov't entities	X		X	
Public	X			Some of the information collected and handled during investigations and litigation becomes public through the litigation process, in accordance with applicable law and court rules.
Private sector			X	Contractors to the Department
Foreign governments				
Foreign entities				
Other (specify):			X	Opposing counsel

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.)

Security protections that authorize and limit a user's access to information within the system

mitigate the risks to privacy. Unauthorized physical access to LAWEB and LARS is limited by physical controls, such as secured entrances and security officers, who control access to the building in which the servers and workstations are located. The data maintained by LAWEB and LARS is protected through compliance with the Department's access control policy. To access the system, the Civil Division enforces Department standards for accessing a network system, such as multi-factor authentication using Person Identity Verification (PIV) card entry and role-based access controls. In addition, before a user is granted access to a system hosted on LAWEB and LARS, 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. For data in transit, the Civil Division utilizes Department-approved encryption technology and PII filtration for email services. In addition, all contractors granted access to the system must adhere to the Department's IT security standards for reporting security incidents.

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. Users outside the Civil Division may include investigators from another component or agency, partners at the United States Attorney's Office, or expert witnesses. There are monitoring and auditing tools for each system to review user activity, so the Civil Division can 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. The process for establishing and reviewing accounts includes application and monitoring of initial distribution of accounts. Credentials are controlled according to DOJ and NIST standards. The controls include password management, including password composition, history, compromise, and changes. The processes also include monitoring account establishment, activation, modification, disabling, removal (including unnecessary/defunct accounts) and review, all of which support implementation of need-to-know requirements.

Additionally, the processes include monitoring of access privileges monthly, to further enforce need-to-know protocols. When a user account is created, the account is provided the least necessary privileges for the user to perform tasks related to the investigation and litigation activities. LAWEB and LARS log and track unsuccessful logins and automatically lock the account when the maximum number of consecutive unsuccessful attempts are exceeded. A system administrator must be called to unlock the account. The system also forces re-authentication after a specified period of inactivity. For users who access LAWEB and LARS outside of a DOJ facility, remote access via Virtual Private Network is controlled and monitored. Encryption is used to protect the confidentiality of remote access sessions and secure remote access tokens are implemented to authorize and control access. Remote users are presented with Department policies regarding authorized use before login each time they are required to authenticate or re-authenticate.

The nature of the environment is to provide a secure, collaborative, web-based system for authorized users to access a central repository or stored information. The risk identified is unauthorized access to information within the system. There are monitoring and auditing tools for each system to review user activity, so the Civil Division can 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. Further, LAWEB and LARS back up data regularly and control access to

stored data.]

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 investigations and litigation, individuals typically do not have the opportunity to decline to provide information, and Privacy Act exemptions and other legal restrictions often limit access and amendment protections. An opposing party may challenge the relevancy of the information and not produce the information in litigation, but that challenge would be determined before the information is collected and maintained by LAWEB and LARS. For social media captures and web site collections, notice is not provided to individuals because 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 investigations and litigation, individuals typically do not have the opportunity to decline to provide information, and Privacy Act exemptions and other legal restrictions often limit access, and amendment protections. An opposing party may challenge the relevancy of the information and not produce the information in litigation, but that challenge would be determined before the information is collected and maintained by LAWEB and LARS. For social media captures and web site collections, notice is not provided to individuals because 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 LAWEB and LARS. In the context of investigations and litigation, individuals typically do not have the opportunity to decline to provide information, and Privacy Act exemptions and other legal restrictions often limit access, and amendment protections. 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 to 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 because 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: [3/14/2016] 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: [Completed FISMA Moderate risk evaluation via DOJ Security and Privacy Authorization and Assessment Handbook and NIST 800-53 Rev. 4.]
[X]	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: [Completed DOJ Security Authorization and Systems are under continual monitoring by the Managed System Security Provider (MSSP).]
[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: [Using the audit and accountability principles established in NIST SP 800-53. Audit Controls and Access Controls are implemented to ensure regular checking of logs, controls, and authentication management. These audits are used to verify that permissions and roles of users are accurate, ensure current processes that meet the needs of the system, and proper logging is occurring. Each system is then bound by these policies and adheres to a program plan that demonstrates compliance with the policy related to the standards documented.]
[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.

[Key information security controls based on NIST SP 800-53 and FISMA are used to provide privacy protections and ensure universal standards based on the affected areas being protected. Using these controls as guidelines, LARS and LAWEB operate on a multi-tiered approach to protect sensitive systems and the information contained within them. The technical controls implemented restrict unauthorized access to information and systems. The management controls are used to ensure rules and policies are maintained and enforceable throughout the environment. Operational controls focus on day-to-day operations and behaviors though training. The controls are designed and tailored to ensure that a high level of security is maintained and assists in the elimination of vulnerabilities that are

discovered in a timely manner. The auditing of these controls ensures compliance and relativity, so the security posture is maintained and relevant to the current needs of the system.]

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 specifically pertaining to US citizens and/or lawfully admitted permanent resident aliens can be retrieved from the system, but is handled in strict accordance with all Federal regulations regarding PII and sensitive but unclassified material. LAWEB and LARS offer a variety of retrieval solutions, which generally allow a full-text or fielded search on document data and metadata collected (e.g. date sent, from, to, cc as collected or produced via the discovery protocols). A full-text search uses the database's index to quickly sift through every word (of every record) that can be entered in the database. The user can search and retrieve a list of documents and then view the documents found by the search. A fielded search permits the user to narrow the dataset to be searched within a matter to particular fields, sets, or data. For both searches, the user can search and retrieve a list of documents and then view the documents found by the search. 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).]