

# iManage DOCUMENT MANAGEMENT SYSTEM PRIVACY IMPACT ASSESSMENT

---

Background: Rapid advancements in computer technology make it possible to store and retrieve vast amounts of data of all kinds quickly and efficiently. These advancements have raised concerns about the impact of large computerized information systems on the privacy of data subjects. Public concerns about highly integrated information systems operated by the government make it imperative to commit to a positive and aggressive approach to protecting individual privacy. We have instituted the Privacy Impact Assessment in order to ensure that the Federal Labor Relations Authority (FLRA) appropriately considers privacy issues from the earliest stages of design.

Purpose: The purpose of this Privacy Impact Assessment is to determine if your collection, maintenance, and use of data in this automated system will impact on the privacy rights of individuals. Depending on your answers, we may be required to seek additional details from you. Please direct questions to Fred Jacob, 202- 218-7906 or fjacob@fira.gov.

Authorities: 5 U.S.C. 552a, the Privacy Act of 1974, as implemented by OMB Circular A-130.

## PRIVACY IMPACT ASSESSMENT

### **Section I. Nature of the System:**

Provide the commonly used name of the system, spelling out any acronyms. If the system will be referred to by acronym, include that in the parentheses after the name.

Document Management System (“DMS”)

Provide a generalized broad description of the system and its purpose (What does this system do; what function does it fulfill?)

A Document Management System is the computer system and software used to store, manage, and track electronic documents and electronic images of paper based information. For the DMS, the FLRA has procured the FileSite Document Management System by iManage. The DMS is the primary IT file system used by the FLRA to store documents in support of the Agency's mission. It supports the major administrative and mission functions of the Agency. The DMS is accessible from all permanent FLRA locations and approved remote connections. IRMD is the business owner for the DMS.

Information stored in the DMS is in a centralized off-site “cloud” location. Physical security, software and hardware updates of the “cloud” servers containing the DMS data is controlled by iManage. Access to the cloud site is limited to a secure VPN connection by employees on the FLRA network either locally or through the FLRA VPN. Staff and managers are responsible for proper storage, handling, and use of Agency data residing in

individually assigned DMS storage spaces (“matters” and “folders”), as well as compliance with FLRA privacy policies and related records retention, litigation, e-discovery, and information security procedures.

Is the system in the development phase?

No.

Is this system required by law or Executive Order?

No.

## Section II. Data in the System:

1. Will/Does this system contain personal data elements?

No \_\_\_ (Go to Section VIII)

Yes \_\_\_X (Continue)

2. List those personal data elements or types of data elements that the system will/does contain:

The DMS does not collect data. The system stores and disseminates information in support of the Agency's mission. The DMS stores, and transmits a large volume of sensitive documents of many types, including both public and nonpublic PII. Sensitive PII may relate to specific parties, legal representatives, witnesses, FOIA requestors, FLRA employees, FLRA contractors, Personnel matters, HR documents, and others.

3. What are the sources of the personal information in the system? (Check all that apply):

X FLRA files or databases.

X Non-FLRA files or databases. (List)

Unions and law firms representing an individual or group may provide the personal information.

\_\_\_ The record subject himself.

\_\_\_ Supervisors

\_\_\_ Other third party sources (List).

4. Are the personal data elements described in detail and itemized in a record layout or other document? If yes, provide the name of the document.

Currently, the FLRA does not maintain this information.

5. Review the list of personal data elements that you currently collect. Is each data element essential to perform some official function? [Note: The question pertains only to data elements that you specifically solicit. It does NOT apply to personal data that may be voluntarily provided in a "Remarks," "Comments,"

"Explanation," or similar type of block where the individual is free to add information of his choosing.]

\_\_\_\_\_ 5a. Yes, all data elements solicited are absolutely essential. (Go to Section III).

\_\_\_\_\_ 5b. Some of the solicited data elements are nice to have but not essential.

x 5c. None of the personal data elements are necessary. The program could function effectively without personal data.

6. If you checked block 5b or 5c above, list the data elements that are not essential.

The DMS does not solicit or collect information. It stores information used by FLRA employees.

7. Do the users have an opportunity to decline to provide information or consent to particular uses of the information?

No. However they do have the option to remove any personal information before submitting, it is not required. Any documents sent to the FLRA by external users will be stored in the DMS. Internal users can bypass the DMS and store files locally, however, that process is discouraged as it is less secure and local files are not backed up.

### **Section III. Verifying Data.**

1. For data collected from sources other than FLRA records and the record subject himself, describe how the data will be verified for - -

a. Accuracy:

FLRA personnel are responsible for the accuracy of the information they provide.

b. Completeness:

FLRA personnel are responsible for the completeness of the information they store in the system.

c. Relevance:

FLRA personnel are responsible for storing relevant data.

2. Describe your procedures for determining if data have been tampered with by unauthorized persons. (Note: Do not go into so much detail as to compromise

system security).

One of the features of the DMS is the addition of more robust auditing details on a file. Any time a file is accessed in the DMS the user and time of that access are tracked in the systems audit fields. Additionally, the duration that a user checked out a file is also contained in the audit fields.

The DMS data resides on the iManage servers. iManage controls prevent non-authorized users from accessing data.

#### **Section IV. Access to the Data.**

1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others?)

All of the above could have access to the data in DMS. Access is granted on a need-to-know basis. Users' access is managed through Active Directory after the users have logged onto the FLRA network.

2. Are criteria, procedures, controls, and responsibilities regarding access documented?  
No.

3. Do other systems share data or have access to data in this system?  
No   
Yes \_\_\_ (Explain).

4. Will other non-FLRA agencies share data or have direct access to data in this system (International, Federal, State, Local, Other)?  
No  (Go to Question IV-9).  
Yes \_\_\_ (List each agency by name or type (e.g., law enforcement activities; Social Security Administration, etc.) and briefly provide the purpose of the access.

5. How will the system ensure that agencies get only the information they need to fulfill their official function?

#### **Section V. Attributes of the Personal Data**

1. Is the use of the personal data both relevant and necessary to the purpose for which the system is being/was designed?

No  (Explain)

The DMS stores files that would otherwise be on the agency's network share. The system does not collect personal information. It stores documents that may contain personal information.

Yes \_\_\_\_\_

2. Will the system derive new data or create previously unavailable data about an individual through a data aggregation process?

No  (Go to Section VI).

Yes \_\_\_\_\_(Continue)

- 2a. Will the new data be placed in the individual's employment or other type of record (whether manual or electronic) that is retrieved by name, SSN, or other personal identifier?

No \_\_\_\_

Yes\_\_\_\_(Identify the record, database, or type of record or database).

Not Applicable \_\_\_\_\_X

- 2b. Can the system make determinations about individuals or employees that would not be possible without the new data?

No –

Yes\_\_\_\_(Explain)

Not Applicable \_\_\_\_\_X

- 2c. Will the data be retrieved by personal identifier (name, SSN, employee number, computer ID number, etc.) ?

No\_\_\_\_(Go to Section VI.)

Yes\_\_\_\_(List retrieval fields.)

Not Applicable \_\_\_\_\_X

## Section VI. Maintenance and Administrative Controls.

1. Is the system using technologies in ways that the FLRA has not previously employed (e.g., Caller-ID, surveillance, etc.)?

No\_\_\_\_(Continue)

Yes  (Identify the technology and describe how these technologies affect individual privacy.)

The iManage DMS that the FLRA will be using is a “Cloud” based system that allows the FLRA to store, retrieve, and search documents more efficiently than the previous FLRA file share that the DMS replaces. Additionally, the DMS will facilitate the FLRA’s transition to an electronic (paperless) case file.

The risk to privacy that the DMS creates is that a document stored in the system could contain sensitive personal information and the system is located outside of the FLRA network on the “Cloud”. That risk is mitigated by restricting access to the document to authorized users. Additionally, the iManage DMS system’s “Cloud” architecture provides more robust security than the local FLRA file share that the DMS is replacing. All users of the system are required to login with a user name and password, consistent with NIST guidelines and all electronic traffic is encrypted between the user's personal computer and the DMS servers using SSL.

2. What controls will be used to prevent unauthorized monitoring? (Note: Do not describe your controls and procedures in so much detail as to compromise system security.)

Access to the system is based on the rights and privileges established by the system owner and operations management. Authentication and access control is also supported by the operating system.

## **Section VI. Interface with Privacy Act Systems of Records.**

1. Does this system currently operate under an existing FLRA or Government- wide Privacy Act system of records?

No  (Go to Section VIII.)

Yes  (Continue.)

2. Provide the identifying number and name of each system.

3. If an existing FLRA Privacy Act system of records is being modified, will the system notice require amendment or alteration? (List all proposed changes. Consider the following: Will you be collecting new data elements not previously approved for collection; using the data for new internal procedures; sharing the data with new non-FLRA agencies; keeping the records longer; creating new locations of data, etc.?)

No

Yes  (Explain your changes.)

Not Applicable

4. If the system currently operates under an existing Government-wide Privacy Act system of records notice, are your proposed modifications in agreement with the existing notice?

No  (Explain your changes and continue.)

Yes  (Go to Section VIII.)  
Not Applicable

5. If you answered "no" to VII-4 above, have you consulted with the government agency that "owns" the government-wide system to determine if they approve of your modifications and intend to amend or alter the existing notice to accommodate your needs?

No --

Yes (provide the name and telephone number of the official with responsibility for the government-wide system.)

Not Applicable


### Section VIII. Certification

Certification: I have read and understand the purpose of this assessment. I have also accurately listed the personal data elements collected or accurately answered "no" to Question II-1.

Name: Fred Jacob  
Title: Solicitor and Senior Agency Official for Privacy  
Email address: [fjacob@flra.gov](mailto:fjacob@flra.gov)  
Telephone Number: (202) 218-7906

Signature:  \_\_\_\_\_ Date: 10/31/2018

Name: Michael W. Jeffries  
Title: Chief Information Officer  
Email address: [mjeffries@flra.gov](mailto:mjeffries@flra.gov)  
Telephone Number: (202) 218-7982

Signature:  \_\_\_\_\_ Date: 10/31/2018