FLRA eFILING 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 Noah Peters, 202- 218-7908 or npeters@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.

Federal Labor Relations eFiling System

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

The FLRA eFiling System is a web based software application that allows external parties to file cases electronically with the FLRA. In addition to the eFiling application the FLRA also accepts cases through other means (ex. Fax, Mail, Personal Delivery, etc.). The eFiling application was created to allow users greater flexibility in filing cases, streamline the case filing process, and to assist the FLRA in moving away from paper files and, ultimately, to an all-electronic case file.

Data is stored in the eFiling application in a Postgres database on a Amazon Web Services (AWS) instance.

Using Ruby on Rails and Quick Base APIs, data is transferred from the eFiling application to the Case Management application which is currently a Quick Base system

with data residing in off-site Quick Base 'cloud' servers. The agency is currently working to move all of the case management components from Quick Base to a standard Ruby on Rails and Postgres solution with all data being stored on Amazon Web Services (AWS) servers.

Information stored in the eFiling system is in a centralized off-site "cloud" location. Physical security, software and hardware updates of the "cloud" servers containing the eFiling data is controlled by Amazon Web Services. FLRA employees are granted access to the data on a need to know basis. External parties involved in filing cases with the agency have access to their filings and their user profile data.

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:

   Users enter personal data to create and profile and additional case specific data when filing a case. Data elements include:
   - Name
   - Address
   - Phone Number
   - eMail Address
   - Agency and/or Union involved in the filing
   - Case Type
   - Case Details

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

   __ 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.
   __x 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.]

x_____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.

_____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.
N/A.

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

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:

Parties filing cases are responsible for the accuracy of the information they provide. Additionally, the software does make some checks for correct formatting of email address, phone number, etc. Users also have the ability to enter the email address of a party and, if found, the relevant information for that party will auto populate on the form.

b. Completeness:

Parties are responsible for submitting complete filings. The software does check that required fields are populated and in the correct format. Users are unable to continue if they have not entered complete information.

c. Relevance:

Parties select the type of filing they wish to complete and the software controls the fields the user must enter. In this manner, only relevant data fields are presented to the user for data entry.

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).

The data resides on the AWS servers. AWS controls prevent non-authorized users from accessing data. Additionally, audit fields show additional information on when and by whom data was changed.

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 the FLRA eFiling system. Access is granted on a need-to-know basis and requires that users enter their account credentials in order to access the system.

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___X_(Explain).

After validating a file as correct, it is approved by an FLRA employee and moved to the FLRA case management system for further process. Data in the Case Management System is stored separately in a Quick Base instance. The FLRA is currently working towards moving away from Quick Base and storing all data in a Postgres database on AWS.

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 X (List each agency by name or type (e.g., law enforcement activities; Social Security Administration, etc.) and briefly provide the purpose of the access.

Potentially, any agency subject to the Federal Service Labor-Management Relations Statute, 5 U.S.C. *§* § 7101 *et seq.* will share data or have direct access to data in this system. They will need access to the information in order to participate in cases brought before the Authority, the Office of the General Counsel, and the Federal Service Impasses Panel.

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

The system does not have any automated measures to ensure that the agency is sent only the information needed to fulfill its official function. This function is performed through policies and staff.

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)
Yes__x_____

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

No X (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____x (Continue)
Yes (Identify the technology and describe how these technologies affect individual privacy.)

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 VII. 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___X_____(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 _____X

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 X (Go to Section VIII.)
   Not Applicable_____

5. If you answered "no" to VII-4 above, have you consulted with the government agencythat "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 _x___

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: Noah Peters
Title: Solicitor and Senior Agency Official for Privacy
Email Address: npeters@flra.gov
Telephone Number: (202) 218-7908

Signature: Noah Peters Digitally signed by Noah Peters DN: cn=Noah Peters, o=Federal Labor Relations Authority, ou=Office of the Solicitor, email=npeters@flra.gov, c=US Date: 2022.02.02 15:09:27 -05'00' Date: _____

Name: David Fontaine
Title: Chief Information Officer
Email Address: dfontaine@flra.gov
Telephone Number: (202) 218-7778

Signature: DAVID FONTAINE Digitally signed by DAVID FONTAINE Date: 2022.02.02 14:03:10 -05'00' Date: _____