

CASE MANAGEMENT E-FILING 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@flra.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:

1. 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.

Case Management e-Filing System.

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

The Case Management e-Filing System keeps track of the information about the cases received and processed by the Authority, the Office of Case Intake and Publication, the Office of the General Counsel (OGC), and the Federal Service Impasses Panel (FSIP). The types of cases received and processed are:

- Representation
- Arbitration
- Negotiability
- Unfair Labor Practice
- Impasse

Over the last several years, the Federal Labor Relations Authority (FLRA) **has** engaged in an initiative to make electronic filing or "e-Filing" available to parties in all cases before the FLRA. Making e-Filing available to its parties is another way in which the FLRA is using technology to improve the customer service experience. E-Filing is also expected to increase efficiencies by reducing procedural filing errors and resulting processing delays.

In the first stage of its e-Filing initiative, the FLRA enabled parties to use e-Filing to file requests for FSIP assistance in the resolution of negotiation impasses. The second stage of the FLRA's e-Filing initiative provided parties with an option to use the FLRA's e-Filing system to electronically file 11 types of documents in cases that are filed with the FLRA's three-Member adjudicatory body, the Authority. Parties may now e-File such documents. The third and last stage of the FLRA's e-Filing initiative provides parties with an option to use the FLRA's e-Filing system to file certain documents involved in representation and unfair labor practice proceedings.

3. Is the system in the development phase?

No. X

Yes

4. Is this system required by law or Executive Order?

No. X

Yes (List the law or Executive Order and the implementing FLRA policies and regulations).

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:

(a) Full name, address, telephone number, fax number, and e-mail address of contacts who are associated as participants in a case filed with the Federal Labor Relations Authority. Although most of these data elements are composed of work contact information, participants may also provide home addresses, telephone numbers, fax numbers, or e-mail addresses.

(b) Full name of FLRA employees who use the Case Management e-Filing System or who are assigned to cases or matters with information in the system.

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.

 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. Does the filer have an opportunity to decline to provide information or consent to particular uses of the information?

Yes. Participation in the Case Management E-Filing System is voluntary. Parties may still file documents via hard copy.

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:

Filers are responsible for the accuracy of the information they provide.

- b. Completeness:

Filers are responsible for the completeness of the information they provide. However, their submissions will be rejected if they do not contain all requested information.

- c. Relevance:

FLRA personnel review the information that is provided for relevance.

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 application and data reside on the Quick Base servers. Quick Base controls prevent non-authorized users from accessing data. If a user were to request access to the data the system owner would receive an email alert for the request.

Additionally: Application access is granted to users by the FLRA system owner on a need-to-know basis. Control of access to the data is then granted on a field level basis. The Quick Base system uses SSL, application tokens required for API Calls, and encryption technology to help protect 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 CMS. Access is granted on a need-to-know basis. Users are assigned a logon ID and password and may access only those cases (and data elements) in which they are participating.

2. Are criteria, procedures, controls, and responsibilities regarding access documented?

No. Quick Base users are assigned to the appropriate role(s) based on their job description (internal FLRA users) or a separate role if they are an external party filing a case. Access to the data is limited and based on the role that the user is assigned to.

3. Do other systems share data or have access to data in this system?

No X

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 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?

Like unions and individuals, agencies will have access only to the cases in which they are participating.

6. Who will be responsible for protecting the privacy rights of individuals and employees affected by the interface between agencies?

The agency receiving the information is responsible for adhering to lawful restrictions on use and dissemination of the information.

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 _____ (Continue)

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

The Case Management e-Filing System is a web-based application that the FLRA will use to receive public filings in proceedings conducted under Title 5, Chapter XIV, Subchapter C of the United States Code. These public filings will be submitted by parties to proceedings brought before the FLRA. Before the system was established, parties in these proceedings filed their petitions, complaints, responses, motions, memoranda, exhibits, and other submissions in paper form. The FLRA has, however, recently amended its rules of practice to provide for electronic filing of some of these documents.

The risk to privacy that e-filing creates is that a document filed via the system could contain sensitive personal information. That risk is mitigated by restricting access to the document to authorized parties, that is, the parties to the proceeding for which the document was filed. 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 filer's personal computer and the Quick Base servers using SSL. Additionally, all information stored on Quick Base servers is encrypted.

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.

N/A

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 _____ (Go to Section VIII.)

Not Applicable X

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 X

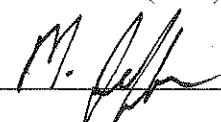
Section VIII. Certification

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

Signature:  Date: 2/10/15

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

Signature:  Date: 2/10/15