



**Federal Labor Relations Authority
Privacy Impact Assessment
General Support System Network
July 2020**

1. System Overview

1.1. The Federal Labor Relations Authority

The Federal Labor Relations Authority (“FLRA”) is an independent administrative federal agency created by Title VII of the Civil Service Reform Act of 1978 (also known as the Federal Service Labor-Management Relations Statute) (the Statute). Pub. L. 95-454, 5 U.S.C. §7101 *et seq.* The Statute allows certain non-postal federal employees to organize, bargain collectively, and participate through labor organizations of their choice in decisions affecting their working lives.

The Statute establishes distinct components within the FLRA, including the Authority, the Office of the General Counsel of the Authority, and the Federal Service Impasses Panel (Panel). Presidential appointees are included in each of these three components. The FLRA structure also includes an Office of Administrative Law Judges. These components are depicted below in the order in which cases generally process through the FLRA. The business of the FLRA, and thus the FLRA mission, is to carry out five (5) primary statutory responsibilities as efficiently as possible and in a manner that gives full effect to the rights afforded employees and agencies under the Statute. Those five primary responsibilities are:

1. Resolving complaints of unfair labor practices (ULPs)
2. Determining the appropriateness of units for labor organization representation (REP)
3. Adjudicating exceptions to arbitrators' awards (ARB)
4. Adjudicating legal issues relating to the duty to bargain (NEG)
5. Resolving impasses during negotiations (Impasse)

The FLRA components exercise statutory prosecutorial and adjudicative responsibilities, with different legal roles. The Statute, however, requires the President to designate one of the Authority Members to serve also as the FLRA Chairman, the head of the agency. As the FLRA's chief executive and administrative officer, the FLRA Chairman is responsible for decisions regarding agency-wide administrative functions, such as purchasing, human resources, budgeting, finance, information technology, leasing of office space, and agency performance management. The Chairman carries out these duties through the Office of the Executive Director. The Chairman has designated the FLRA's Solicitor to serve as Senior Agency Official for Privacy. The immediate staffs of the Authority Members, the Office of the General Counsel, and the Panel are under the general, day-to-day supervision of their respective Members or component heads. In addition, the Authority Members appoint Administrative Law Judges to hear and prepare decisions in cases involving alleged ULPs, as

well as decisions involving applications for attorney fees filed pursuant to the Back Pay Act or the Equal Access to Justice Act. The FLRA also provides full staff support to two other organizations - - the Foreign Service Impasse Disputes Panel and the Foreign Service Labor Relations Board. The Authority, Office of the General Counsel, and Panel maintain their respective headquarters offices at a common site in Washington, DC. The FLRA Office of the General Counsel also includes staff in seven regional offices (Atlanta, Chicago, Denver, San Francisco, Washington, D.C.).

The Agency’s Information Resources Management Division (IRMD), led by its Chief Information Officer (CIO), operates and maintains the necessary Information Technology (IT) services to support the mission, including the Agency’s network, servers, applications, databases, computers, and communication facilities.

1.2. General Support System (GSS) Network Architecture

The General Support System Network (GSS) is the primary IT infrastructure used by the FLRA to host information systems that collect, process, disseminate, and store information in support of the Agency’s mission. It supports the major administrative and mission functions of the Agency and provides for the internal and external transmission and storage of Agency data. It is the IT platform or host for several FLRA systems of records covered by the Privacy Act of 1974, 5 U.S.C. § 552a.¹ The GSS Network encompasses all permanent FLRA locations and approved remote connections. IRMD is the business owner for the GSS.

The GSS Network has dedicated connections with external (non-FLRA) entities as necessary to support the FLRA mission. At the time of this writing, those connections include:

Connection	Purpose
Department of Interior, National	Financial & Human Resources
DCNet CenturyLink MTIPS	Trusted Internet Connection Service

Information is stored in the GSS in centralized storage as well as local storage on servers and user-dedicated systems. Individual staff and managers are responsible for proper storage, handling, and use of Agency data residing in individually assigned network storage space, as well as compliance with FLRA privacy policies and related records retention, litigation, e-discovery, and information security procedures.

The design and proper operation of the GSS is accomplished using current technology including switches, routers, firewalls, monitors, and other equipment through which sensitive data may pass or be temporarily retained. Access to

¹ See section 8 of this PIA for further discussion. The GSS itself is not a Privacy Act system of records, even though it supports such systems.

these devices is restricted to network operations and operations assurance staff.

1.3. Systems of Records & Public Web Sites Hosted on the Datacenter GSS

The GSS hosts most of the Agency's databases and applications and its primary public web site. System and information owners or program managers are responsible for the proper handling, storage, and use of data in specific applications and databases in the GSS. Certain subsystems, applications, and databases hosted on the GSS are covered by their own separate Privacy Impact Assessments (PIAs). The following table lists the current components for which separate PIAs have been developed:²

Name	Function	System of Records ³	Minor Application ⁴
Case Management e-Filing System	Used to file and keep track of information about cases received and processed by the Authority, the office of Case Intake and Publication, the Office of the General Counsel, and the Panel.	No	Yes

² All current PIAs may be found here: <https://www.flra.gov/privacy-policy>

³ A "no" in this column indicates that the named IT function (like the Datacenter GSS) is not itself a "system of records" as defined by the Privacy Act, but may support or host other Privacy Act systems in whole or part, as described in the separate PIA for that IT function.

⁴ As defined by NIST SP 800-37.

2. Information Collected and Stored within the System

2.1. What information is to be collected, used, disseminated, or maintained by the system?

As the primary IT infrastructure used by the FLRA to host information systems that collect, process, disseminate, and store information in support of the Agency's mission, the GSS collects, stores, and transmits a large volume of sensitive information of many types, including both public and nonpublic Personally Identifiable Information (PII). Sensitive PII may relate to specific parties, legal representatives, witnesses, FOIA requestors, FLRA employees, FLRA contractors, and others. These data collections are described in SORNs or PIAs for systems housed in the Datacenter GSS, where necessary.

2.2. What are the sources of the information in the system?

Information in the GSS is obtained by FLRA staff in connection with the Agency's mission-related functions and other activities. In some instances, this information is provided voluntarily, such as when individuals file unfair labor practice charges, representation petitions, negotiability appeals, arbitration exceptions, or impasse cases. The FLRA sometimes obtains information in response to compulsory process, such as subpoenas and civil investigatory demands and via discovery in administrative and federal court litigation. Information in the GSS may also be obtained from other sources, such as public resources on the Internet and commercial databases such as Westlaw. In some instances, individuals – for example, third parties in investigations or witnesses in administrative and federal court matters—may provide information about other individuals.

2.3. Why is the information being collected, used, disseminated, or maintained?

Information in the GSS is collected, used, disseminated, and maintained for the FLRA to perform its mission-related functions and other activities. FLRA staff members collect and use the information to investigate unfair labor practices and representation petitions, resolve bargaining impasses and negotiability disputes, and review arbitration awards. FLRA staff also use the information to conduct general business operations, such as personnel matters, responses to FOIA requests, and contracts with private entities.

2.4. How is the information collected?

GSS information is obtained by the FLRA from a variety of sources, most often given to the FLRA voluntarily during the case handling process, as well as information obtained via compulsory process, discovery, or through other investigative sources. Typically, information is obtained from individuals and

entities with information that may be relevant to an FLRA investigation. Information is generally collected directly from whatever media is used to submit it. This may include copying information from paper-based sources or from removable media such as CDs, DVDs, and hard drives. It may also include copying information that is electronically submitted via email or some other electronic submission mechanism (e.g. through a website collection mechanism).

2.5. How will the information be checked for accuracy and timeliness (currency)?

Information in the GSS that is used by the FLRA as part of its mission-related activities will be reviewed for accuracy and timeliness as required by the particular activity, rather than as part of Datacenter GSS activities. For example, staff performing an investigation based upon an unfair labor practice charge may check the information that is obtained to ensure that it is timely and accurate.

Information in the GSS is also subject to appropriate information security controls, as further described below in this PIA. These controls will ensure that sensitive information is protected from any undue risk of loss and that the contents of materials remain unchanged from the point-in-time they are included in the GSS.

2.6. Is the system using technologies in ways that the FLRA has not previously employed (e.g., monitoring software, Smart Cards, etc.)? If so, how does the use of this technology affect individuals' privacy?

The GSS does not employ previously unused technologies, although the establishment of the GSS centralizes the IT functions for efficiency. The potential impact on individuals' privacy by the operation of the Datacenter GSS is discussed in this document below and in any related individual PIAs referenced in this document.

2.7. What law or regulation permits the collection of this information?

The Statute, the FLRA's Rules and Regulations, and other laws governing the FLRA's operations permit the collection of the information.

2.8. Considering the type of information collected and sources of collection, what privacy risks were identified and how were these risks mitigated?

The following privacy risks were considered during the development of the GSS:

a. Malicious Code

To address these risks, the FLRA employs a suite of tools and systems to detect, remove, and block malicious code and to minimize the risk of

network and user exposure.

b. Hackers

To address this risk, the FLRA implements a defense-in-depth strategy in the GSS.

c. Unauthorized Access to Data (Logical and Physical Access)

To address these risks, access to information is based on the least privilege security model. The most restrictive set of privileges are applied to Agency network user IDs upon creation. All network activity is closely audited and monitored, and unauthorized activity is referred to the appropriate official for action. Physical access to the GSS is controlled, logged, and monitored.

d. Data Leakage/Breach (unintentional release of sensitive PII to an untrusted environment)

i. Misconfigured information asset

To address this risk, the FLRA conducts regular reviews and audits of configurations on GSS IT assets. In addition configuration changes are strictly controlled within IRMD's Configuration Control Group.

ii. Unapproved Sensitive PII storage

To address this risk, FLRA policy states that electronic documents (including emails) containing Sensitive PII may be stored only on individually assigned FLRA network storage space or on a shared FLRA network storage service in a file folder to which access has been restricted to authorized individuals.

iii. Lost or misplaced tape backup media

This is not currently a risk as the FLRA keeps all backups in electronic format

iv. Information loss through IT asset decommissioning

To address this risk, all IT assets containing recoverable data are destroyed in accordance with NIST standards, in conjunction with the equipment excess process.

v. Personally Owned IT Equipment

To address this risk, no personally owned devices are allowed to be connected to any IT asset within the Datacenter GSS.

3. Use and Access to Data in the System

3.1. Describe how information in the system will or may be used.

Information in the GSS may be used to support the FLRA's mission-related functions and other activities, to include:

- Investigating potential or alleged violations of the Statute
- Investigating and processing representation petitions
- Processing exceptions to arbitration awards
- Resolving negotiability disputes and bargaining impasses

3.2. Which internal entities will have access to the information?

Agency staff and contractors who require information to support FLRA mission-related and system administrative activities and to respond to FOIA and other disclosure requests will have access to the information. Information also is used to carry out administrative functions related to human resources, security, financial management, and matter and resource management.

3.3. Which external entities will have access to the information?

The GSS may be accessed by FLRA authorized external contractors.

4. Notice and Access for Individuals

4.1. How will individuals be informed about what information is collected, and how this information is used and disclosed?

Wherever possible, the FLRA provides notice to individuals about its policies regarding the collection, use, and disclosure of information at the time the information is collected. For information that is collected pursuant to a request from the FLRA, notice is provided as part of that request (e.g., in a letter request or in the document outlining the compulsory process request). For those occasions where the FLRA cannot provide notice at the time the information is collected, the FLRA provides notice via its privacy policy, its Privacy Act system of records notices (SORNs), and its PIAs, including this one.

4.2. Do individuals have the opportunity and/or right to decline to provide information?

The opportunity or right depends on how the information is collected and the purpose for the collection. Those who provide information pursuant to compulsory process do not generally have a right to decline to provide the information. However, individuals who voluntarily file documents with the FLRA that may reside on the GSS Network do so voluntarily and could choose

to decline to provide such information.

4.3. What are the procedures that allow individuals to gain access to their own information?

An individual may make a request under the Privacy Act for access to information maintained about themselves in the Privacy Act systems that are hosted on GSS. Individuals must follow the FLRA's Privacy Act rules and procedures, which are published in the Code of Federal Regulations at 5 C.F.R. § 2412. Access to the information under the Privacy Act is subject to certain exemptions. In addition, there is public information in the GSS that also appears on the FLRA's website and is accessible to the public there or in paper format through the public reading room at FLRA Headquarters in Washington.

4.4. Discuss the privacy risks associated with the process of providing individuals access to their own records and how those risks are mitigated.

Individuals do not have direct access to the GSS so there are no associated privacy risks.

5. Web Site Privacy Issues

5.1. Describe any tracking technology used by the Web site and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, Web beacon). Currently, persistent tracking technology is not approved for use by the FLRA (see 5.2).

Not applicable (N/A). The GSS is not a website.

5.2. If a persistent tracking technology is used, ensure that the proper issues are addressed.

N/A

5.3. If personal information is collected through a Web site, page, or online form accessible through the Internet, is appropriate encryption used? If not, explain.

N/A

5.4. Explain how the public will be notified of the Privacy Policy.

N/A

5.5. Considering any Web site or Internet issues, please describe any

privacy risks identified and how they have been mitigated.

N/A

5.6. If the Web site will collect personal information from children under 13, or be directed at such children, explain how it will comply with the Children's Online Privacy Protection Act (COPPA).

N/A

6. Security of Information in the System

6.1. Are all IT security requirements and procedures required by federal law being followed to ensure that information is appropriately secured?

The FLRA follows all applicable Federal Information Security Management Act (FISMA) requirements, ensuring the GSS is appropriately secured. The GSS is categorized as moderate using Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems.

6.2. Has a Security Assessment and Authorization been completed for the system or systems supporting the program?

Yes.

6.3. Has a risk assessment been conducted on the system?

Yes, a risk assessment was completed as part of the Security Assessment and Authorization. An overall discussion of the privacy risks associated with the GSS and the steps that the FLRA has taken to mitigate those risks is provided in section 2.8, above.

6.4. Does the project employ any new technology that may raise privacy concerns? If so, please discuss its implementation.

No.

6.5. What procedures are in place to determine which users may access the system and are they documented?

All FLRA positions are assigned a risk designation and associated personnel screening criteria. All potential FLRA employees and contractors are subject to

background investigations and suitability reviews per OMB guidance.

Before any new employee, contractor, or volunteer can access any system in the GSS, their manager or supervisor must request the account outlining the necessary permissions the user needs. They must also successfully complete the FLRA's Privacy and Security Awareness training. All employees are granted basic network access to include email services, the Internet, the Intranet, and network-based applications.

Supervisors must identify and approve employee requests to access network applications and specify the appropriate access privileges. Network and application access is based on: (1) a valid access authorization, (2) intended system usage, and (3) other attributes based on the system's business function. All network and application access is based on least-privilege and need-to-know security models.

6.6. Describe what privacy training is provided to users either generally or specifically relevant to the program or system.

All FLRA staff members are required to complete a computer security and privacy awareness training annually. The interactive online training covers topics such as properly handling Sensitive PII and other data, online threats, social engineering, and the physical security of documents and electronics such as laptops and mobile devices. Individuals with significant security responsibilities are required to undergo additional training tailored to their respective responsibilities. Moreover, as stated above, all new employees receive privacy training when they join the FLRA.

6.7. What auditing measures and technical safeguards are in place to prevent the misuse of data?

Auditing measures and technical safeguards are in place commensurate with the National Institute of Standards and Technology (NIST) Recommended Security Controls for Federal Information Systems and Organizations Moderate-Impact Baseline Special Publication (SP) 800-53, Rev. 3.

6.8. Questions regarding the security of the system

Any questions regarding the security of the GSS should be directed to IRMD.

7. Data Retention

7.1. For what period of time will data collected by this system be maintained?

Information in the GSS, including information, if any, that may be incorporated

into or otherwise required to be preserved as Federal records, is retained and destroyed in accordance with applicable schedules and procedures issued or approved by the National Archives and Records Administration (NARA).

7.2. What are the plans for destruction or disposal of the information?

All information will be deleted/destroyed in accordance with OMB, NARA, and NIST regulations and guidelines.

7.3. Describe any privacy risks identified in the data retention and disposal of the information, and describe how these risks have been mitigated.

The privacy risks associated with the GSS and the steps that the FLRA takes to mitigate those risks are provided in section 2.8, above. Regarding risks identified in the disposal of information, all information will be destroyed in a manner that adheres to NIST guidelines, that makes it impossible to recover.

8. Privacy Act

8.1. Will the data in the system be retrieved by a personal identifier?

The GSS is a supporting infrastructure and as such will not retrieve information by a personal identifier. As noted earlier, however, the Datacenter GSS does support or host several of Privacy Act systems of records (i.e., containing information retrieved by name or other personal identifier of the subject individuals) in whole or part.

8.2. Is the system covered by an existing Privacy Act System of Records notice (SORN)?

As discussed earlier, the GSS hosted systems maintain data generated or compiled in the FLRA's mission-related activities, as well as human resources, security, financial management, and matter and resource management data necessary for internal agency administration. Such data, to the extent such data is about an individual and retrieved by that individual's name or other personal identifier, is covered by the Privacy Act of 1974, 5 U.S.C. 552a, under one or more applicable FLRA SORNs. A complete list and copies of these SORNs is available at: http://www.gpo.gov/fdsys/pkg/PAI-2005-FED_LAB/html/PAI-2005-FED_LAB.html.

9. Privacy Policy

9.1. Confirm that the collection, use, and disclosure of the information in this system have been reviewed to ensure consistency with the FLRA's privacy policy.

The collection, use, and disclosure of information in this system are consistent with the FLRA's Privacy Policy.

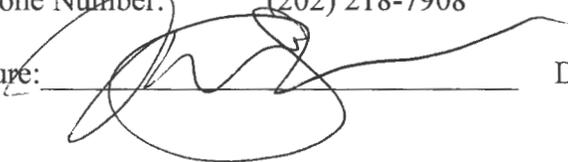
10. Scope of GSS PIA and Future Modifications

IRMD is constantly improving and expanding the technological capabilities of the GSS to enable the Agency to more effectively and efficiently carry out its mission. Consistent with the requirements of the E-Government Act of 2002, this PIA will be revised to reflect any significant changes to the GSS that impact the collection, storage, maintenance, or dissemination of PII. The PIA will not be modified to reflect routine application changes and modifications, version upgrades, feature patching, ongoing maintenance, new instances of existing products, or routine hardware upgrades such as the procurement of additional servers or additional memory or storage space. Changes to the GSS are closely managed by IRMD and the decision to update this PIA will be made on case-by-case basis in consultation with the SAOP.

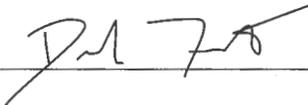
11. Approval and Signature Page

Certification: I have read and understand the purpose of this assessment. I have also accurately listed the personal data elements.

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

Signature:  Date: 07/22/2020

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

Signature:  Date: 22 July 2020