PRIVACY IMPACT ASSESSMENT— JANUARY 2024

Labor and Employee Relations System PIA v2

Does the CFPB use the information to benefit or make a determination about an individual?	Yes.
What is the purpose?	Manage and report labor and employee matters and grievances.
Are there controls to enforce accountability?	Yes, all standard CFPB privacy protections and security controls apply.
What opportunities do I have for participation?	Appropriate opportunities for notice, consent, access, and redress.

Consumer Financial Protection Bureau

Overview

The CFPB is committed to providing a fair, equitable, and timely review and resolution of employee concerns regarding employment-related matters subject to the control of CFPB management. The Employee and Labor Relations (ELR) team advises managers and is the main point of contact for questions concerning corrective and disciplinary actions related to employee misconduct, performance matters, and administrative grievances. The CFPB utilizes a digital file management system, the Labor and Employee Relations System (LER System), to effectively manage records pertaining to labor grievances and negotiations, or employee matters relating to conduct, performance, and disciplinary matters (herein collectively referred to as matters). The LER System collects personally identifiable information (PII) from CFPB employees, contractors, applicants, and detailees (CFPB staff).

The CFPB Office of Human Capital (OHC) ELR team operates the LER System and uses the PII to process and facilitate the adjudication of labor and employee relations matters. The LER System and subsequent collection of PII allows ELR to accurately identify individuals involved in the matters, document, track, manage, and efficiently report the status and outcomes of labor and employee relations matters.

The CFPB collects information based on the following statutory requirements:

- The Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 (No FEAR Act), Pub. L. No. 107-174;
- The Civil Rights Act of 1964, 42 U.S.C. § 2000d, et seq.;
- 5 U.S.C. Chapters 43 (performance appraisal), 71 (labor-management relations), and 75 (discipline);
- The Federal Labor-Management Relations Statute (FSLMRS), 5 U.S.C. §§ 7101-7135;
- The Alternative Dispute Resolution Act of 1998, 28 U.S.C. § 651;
- The Age Discrimination in Employment Act (ADEA), 29 U.S.C. § 621 (1967); and
- The Rehabilitation Act of, 29 U.S.C. § 790-94 (1973).

The CFPB also collects information under the labor-management agreement stipulated negotiated grievance process.

In practice, the ELR team collects information from individuals reporting a matter, individuals responding to these matters, or individuals who are knowledgeable about the details of a particular matter. The ELR team only uses the information collected to evaluate a matter, provide

guidance, process, and document the matter to support manager decisions on the employee matter. Once collected, information is stored in the LER System, and only accessed to manage or investigate an employee matter. The information remains in the system until it is required to be archived or destroyed according to National Archives and Records Administration (NARA) General Records Schedules (GRS) 2.3: Employee Relations Records.

This Privacy Impact Assessment (PIA) covers information collected specifically for evaluating and providing guidance on a labor or employee matter. The CFPB is updating this PIA to provide more details on additional information which may be collected by the ELR team, as well as several general updates. The publication of this updated PIA will replace the previously published Labor and Employee Relations System PIA (January 4, 2016). The information is collected pursuant to the system of records notice (SORN) CFPB.009, Employee Administrative Records[1].

The Paperwork Reduction Act (PRA) does not apply to the LER System. LER System does not ask "identical" questions of ten or more persons as defined in 5 CFR 1320.3(c).

Privacy Risk Analysis

The primary privacy risks associated with the use of the LER System are related to the following:

- Data Minimization
- Security
- Limits on Uses and Sharing of Information.

Data Minimization

The LER System contains information collected directly from (1) the individual who is filing a matter, which may also contain PII regarding the subject of the matter, (2) people responding to an individual's matter, and/or (3) people with knowledge of an individual's matter. There is a risk that more than the necessary information is collected from these individuals. This risk is mitigated by the general practice to train ELR staff to always seek the minimum amount of PII necessary to complete a task as it relates to responding to and resolving a matter. Moreover, CFPB personnel are supervised to ensure this training is followed.

[1] Employee Administrative Records SORN can be found at https://www.federalregister.gov/documents/2020/08/11/2020-16291/privacy-act-of-1974-system-of-records.

As the interactions that result in information collection are generally voluntary, the privacy risks associated with these collections are minimal. Individuals filing grievance or allegation choose what and how much information they share with the CFPB, and they have opportunities to change or update erroneous, inaccurate, or irrelevant information. Direct identifying PII is generally limited to information required in the matter (address, phone, date of birth, email, professional affiliation or employer).

Security

Given that the matters may contain sensitive and confidential information, there is a risk that the information may be a target for unauthorized access. The CFPB minimizes this risk by enforcing access controls to reduce the number of individuals who have access to the data and by storing data on systems that have been accredited as secure for this type of information. The OHC ELR team is also trained to handle potential breaches to minimize negative impacts.

Access to the LER System and the information within it is also limited. Access controls and other security measures are in place to limit information about a matter to federal ELR staff. Authorized access for ELR staff is based on their need to know and is restricted to the minimal amount of information required or appropriate to carry out their assigned job responsibilities. The CFPB terminates or reduces access as necessary should an ELR staff member no longer have a need to know the information, change job functions, be terminated, or resign. Information within the LER System is also subject to the appropriate technical, physical, and administrative controls implemented to address security risks such as data encryption. For example, the National Institute of Standards and Technology (NIST) control families are implemented to restrict access to information to authorized ELR staff. The technical, physical, and administrative controls also limit the uses of and sharing of PII, secure the system, and provide minimal information as is necessary and appropriate for purposes of the LER System.

Limits on Uses and Sharing of Information

Information within the LER System is used to manage and investigate employee matters. As a result, there is a risk that the information contained in the system may be misused or used for unauthorized purposes. Also, given the sensitive and confidential nature of the matters submitted and the ELR's role in processing these matters, in the event of a data breach, there is also a risk of embarrassment or loss of reputation to both individuals involved in claims and the CFPB.

The CFPB minimizes these risks by enforcing access controls limiting access to records regarding matters to very limited authorized ELR staff. Only ELR staff or certain, very limited individuals

inside the CFPB might have a need to know about a matter at different points in the process (e.g., witnesses who are interviewed, supervisors or other officials who may need to take disciplinary action if the CFPB ultimately is found to have violated the discrimination laws, etc.). ELR staff sign a Rules of Behavior (RoB) document and are trained on appropriate uses of the data within the application prior to being granted access to the application. Sensitive and confidential information is only stored in systems with the requisite security authorization to hold that type of information. Any information sharing can only happen under authorized circumstances (i.e., referral to another government agency).

The technical, physical, and administrative controls implemented to promote individual participation, minimization, and accountability are appropriate.

Privacy Risk Management

1. Describe what information the CFPB collects, how the information is collected, and the sources from which the information is collected.

The ELR team collects information to process and facilitate the adjudication of labor and employee relations matters.

PII collected by the system may include the following:

- Name of employee, manager, union representative, or other individuals with knowledge of the matter;
- Employee number;
- Date of birth (depending on the nature of the matter);
- Contact information;
- Phone numbers (work and personal);
- Employment information;
- Information about matters related to the matter. Some of these matters may contain sensitive PII related to gender identity, sexual orientation, race, disability status, religion, and/or national origin.

The ELR team directly collects PII from individuals submitting a matter, individuals responding to a matter, co-workers, former co-workers, supervisors, witnesses, union representatives, legal

representatives, OCR and/or other individuals with knowledge of the matter. Information is generally gathered via email, telephone, or virtual meeting. The ELR team schedules an intake call after receiving notification of the alleged misconduct to gather the initial necessary information from the reporting party to determine whether an investigation is appropriate. Personal identifiers are removed when the CFPB uses the information for reporting and statistical purposes[2].

The collection and intended use of PII supported by the LER System must first be reviewed and approved by the CFPB through data governance processes. This review ensures that proposed collections of PII is the minimum necessary for the intended purpose and the authorization to do so under CFPB's regulations prior to any collection of use of PII that is housed within this environment. The PII described above is the minimum amount necessary to appropriately manage and administer CFPB's Labor and Employee Relations matters.

There are currently no specific forms or surveys used in the collection of information for the system.

2. Describe CFPB's objective for the information.

The PII is used to identify individuals involved in matters, and in order to document, track, manage, and efficiently report the status and outcomes of labor and employee relations matters.

When an individual files a matter, the CFPB initiates an information intake process and may conduct an investigation of the matter, which may involve interviewing witnesses or others with knowledge of the matter. The amount and specific type of information collected varies based on the particulars of the matter, but the investigator or specialist strives to collect only the necessary information to address the particulars of that matter. When the information is used by the CFPB for reporting and for statistical purposes, personal identifiers are removed.

3. Describe how CFPB shares any of the information with third parties with whom the CFPB shares the information for

[2] As an example, CFPB must regularly and publicly report the number of individuals disciplined for violations of employment discrimination and whistleblower laws, as well as the types of discipline administered.

compatible purposes, e.g., federal or state agencies, the general public, etc.

Information related to matters may be shared with other federal and state authorities when necessary or required, such as the Office of Personnel Management (OPM), Equal Employment Opportunity Commission (EEOC), Federal Labor Relations Authority (FLRA), arbitrators, courts and other tribunals, and Congress. Unless required to be provided, all identifying information is redacted from data before it is shared externally. Information shared externally for reporting and statistical purposes is stripped of all PII.

The CFPB only shares PII if legally required and only in accordance with the routine uses published in CFPB.009 - Employee Administrative Records SORN.

4. Describe what opportunities, if any, individuals to whom the information pertains have to (a) receive notice regarding the CFPB's use of the information; (b) consent to such use; (c) access the information that pertains to them; or (d) obtain redress.

The CFPB provides notice to individuals through Privacy Act Statements, the publication of this PIA, CFPB.009 Employee Administrative Records SORN.

Individuals agree to voluntarily submit information in support of their matter. Individuals with knowledge of information pertinent to the matter are requested to provide their information in support of the investigation. While witnesses are required to provide information in matters of misconduct, this information is minimized to that which is necessary to support the investigation.

Where applicable, the CFPB allows individuals to request access and amend their PII per the Privacy Act and CFPB's Privacy Act regulations at 12 C.F.R. § 1070.50 *et seq*. Information about Privacy Act requests is published in the associated SORNs and on the CFPB's website. Individuals may also file a request for information under the Freedom of Information Act.

5. Explain the standards and relevant controls that govern the CFPB's—or any third-party contractor(s) acting on behalf of the CFPB—collection, use, disclosure, retention, or disposal of information.

The CFPB manages risks to privacy by complying with the Privacy Act of 1974, the Right to Financial Privacy Act, and the E-Government Act of 2002. To further compliance, the CFPB

voluntarily adopts Office of Management and Budget (OMB's) privacy-related guidance as a best practice;[3] and applies the NIST risk management processes for privacy.

The CFPB uses the following technical and administrative controls to secure the information and create accountability for the CFPB's appropriate collection, use, disclosure, and retention of the information:

- Audit logs and reviews are in place to identify, review, and assess unauthorized access to the LER System and the data that resides within the system.
- Data quality and integrity checks are performed to continually validate that PII within the system is accurate and relevant for the purposes it was collected for.
- Extract logging and reviews to ensure that data within the system is only accessed and used by authorized CFPB staff.
- CFPB general and role-based privacy trainings are required prior to granting access to the LER System. Role-based trainings include guidance on data handling procedures, incident and breach response procedures, and the CFPB's authority to collect and use PII in accordance with its regulations.
- CFPB incident response procedures and breach response procedures are in place to address incidents involving data residing in the LER System.
- Compliance with the CFPB's cybersecurity and privacy policies and standard operating procedures are documented within the security and privacy implementation plans.
- Role-based Access Controls: The LER System is not accessible to the public. The following internal users have access to information collected and maintained by the application:
    - ELR staff members assigned to assist with managing and reporting labor and employee matters have access to the collected information, including any PII, to update the status of the matter.
    - System administrators, who are federal employees that directly support the ELR Office, are considered privileged users and, as such, have access to all data in the system, including PII associated with all records, to ensure the systemic

[3] Although pursuant to Section 1017(a)(4)(E) of the Consumer Financial Protection Act, Pub. L. No. 111-203, the CFPB is not required to comply with OMB-issued privacy guidance. The CFPB follows OMB privacy-related guidance as a best practice and to facilitate cooperation and collaboration with other agencies.

functionality of the LER System and other administrative application functions.

- The LER System is subject to the records schedule: GRS 2.3: Employee Relations Records.
- Security logging and monitoring tools are used to ensure authorized access to both the environment and to monitor system access within the system.
- Personnel Security, including completing background checks for all employees, contractors, or other individuals authorized to conduct CFPB activities in the LER System.

Contractors are not currently provided access to the system. The CFPB may, however, use contractors to help support the collection, use, disclosure, or retention of information covered by this PIA, and those contractors are subject to the same controls described herein. When contractors are granted access to direct identifying PII, they are required to report suspected or confirmed privacy incidents to the CFPB immediately and no later than one hour after discovery. Other requirements placed on contractors may include training on privacy and compliance with federal privacy requirements and privacy requirements found within Federal Acquisition Regulations (FAR).

In addition, the PII collected for employee and labor relations matter is only accessed by federal employees, not contractors. The LER System is not accessible to the public or anyone outside of the CFPB that does not have prior authorization.

The CFPB has updated this PIA as a result of its privacy continuous monitoring (PCM) processes. The system has also been assessed to determine how it provides a more secure and automated approach to business operations. Further, due to this PIA, the CFPB Privacy team is part of governance and project working groups to assess privacy implications related to the use of PII within the LER System.

6. Discuss the role of third party(ies) that collaborate or partner with the CFPB, if any. Identify any controls used to protect against inappropriate collection, use, disclosure, or retention of information. (This does not include third parties acting on behalf of the CFPB, e.g., government contractors discussed in Question 5.)

Not applicable.

Document control

7. Approval

CHRISTOPHER CHILBERT
Digitally signed by CHRISTOPHER CHILBERT
Date: 2024.01.24 13:22:02 -05'00'

Chris Chilbert

Chief Information Officer

Date

KATHRYN FONG
Digitally signed by KATHRYN FONG
Date: 2024.01.24 13:36:06 -05'00'

Kathryn Fong

Chief Privacy Officer

Date

ARI TARAGIN
Digitally signed by ARI TARAGIN
Date: 2024.01.23 19:11:25 -05'00'

Ari Taragin

Director of Employee and Labor Relations

Date

Change control

Version	Summary of material changes	Pages affected	Date of change
1.0	Original approval	All	January 2016
2.0	Update to provide more details on other information which may be collected by the ELR team, as well as several general updates.	All	January 2024