National Labor Relations Board

Privacy Impact Assessment
for the
Backpay Management System (BMS)
August 2019

Background

Background: Rapid advancements in computer technology make it possible to store and retrieve vast amounts of data 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. The collection, use, maintenance, and dissemination of information on individuals by the National Labor Relations Board (NLRB) requires a thorough collaborative analysis of legal, technical, security and privacy teams. Whether a system is automated, manual, or both, integration of privacy protections is a primary element in the development of the system.

Purpose

The purpose of the privacy compliance documentation, the Privacy Threshold Analysis (PTA) and Privacy Impact Assessment (PIA) is to determine if the proposed plan to collect, maintain, and use data in an automated system will impact the Privacy rights of U. S. Citizens and lawfully admitted aliens.

Agency Process

NLRB's privacy compliance process is comprised of two phases. Phase 1, the *initial* assessment known as a Privacy Threshold Analysis (PTA), determines whether a formal PIA is necessary for the system. Following a review of the PTA, the IT Security Officer along with the Privacy Officer will determine if a more detailed PIA is necessary. If a more detailed PIA is necessary, the system will undergo Phase 2, a *detailed* assessment. Both phases require the gathering of system information on technical, legal, security, and privacy issues, along with identification and mitigation of privacy risks. PIA's are published to the public facing website, as NLRB's commitment to fostering transparency, regarding how the agency uses personally identifiable information (PII) to fulfill its mission.

Applicable laws and regulations affecting Privacy Act Data

- Privacy Act of 1974, as Amended (5 USC 552a) which affords individuals the right to privacy in records that are maintained and used by Federal agencies.
- Computer Security Act of 1987 (Public Law 100-235) establishing minimum-security practices for Federal IT systems.
- Matching and Privacy Act of 1988 (Public Law 100-503).
- OMB Circular A-130, Management of Federal Information Resources and A-130 revised, "Managing Information as a Strategic Resource". Appendix III to OMB Circular No. A-130, Appendix III establishes:
    - A minimum set of controls to be included in Federal automated information security programs;

  - Assigns Federal agency responsibilities for the security of automated information; and
  - Links agency automated information security programs and agency management control systems established in accordance with OMB Circular No. A-123.

- The Appendix revises procedures formerly contained in Appendix III to OMB Circular No. A-130 (50 FR 52730; December 24, 1985), and incorporates requirements of the Computer Security Act of 1987 (P.L. 100-235) and responsibilities assigned in applicable national security directives. Furthermore, the aforementioned provides uniform government-wide information to Federal agencies on compliance of fair information practices, security and reporting requirements. Appendix III and makes minor technical revisions to the Circular to reflect the Paperwork Reduction Act of 1995 (P.L. 104-13).
- Freedom of Information Act (FOIA), as Amended (5 USC 552) which provides for the disclosure of information maintained by Federal agencies to the public while allowing limited protections for privacy.

Privacy Impact Assessment

<u>Section I Nature of the System:</u>

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 parentheses after the name.

   Backpay Management System (BMS)

2. In five sentences or less, provide a generalized description of the system and its purpose. Provide an explanation of how the system functions and what agency-based mission(s) the system fulfills.

   The Backpay Management System (BMS) is used in cases where NLRB is actively involved in the financial management (e.g., recording and receiving funds and making disbursements) of awards given to discriminatees. The system also facilitates the efforts and responsibility of the agency to properly report and pay the employer share of taxes to IRS, Social Security, and Medicare. Typically, the employer issues the award. In a fraction of the cases, the agency steps in to issue the awards. The Backpay system is used where the agency has taken the responsibility to manage funds for awarding to the discriminatee. Once the agency receives the funds on behalf of discriminatees, they are deposited into a deposit fund with the U.S. Department of the Treasury and tracked. Upon finalization of the awards, discriminates are issued the proceeds.

3. Describe the stage of development the system is currently:

   ☐ A new system which is --

      ☐ Still in the planning stages.

      ☐ Mid-way to launch.

      ☐ Ready for launch. Anticipated Launch Date:

☐ Proposals to change an existing system, the changes are:

☐ Still in the planning stages.

☐ Mid-way to launch.

☐ Ready for launch. Anticipated Launch Date:

☒ Other or Maintenance

This is an existing system that is in the maintenance stage. There are periodic releases that require a System Development Life Cycle (SDLC) approach, however, the overall system remains operational.

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

☒ No

☐ Yes (Provide the law, Executive Order and NLRB policies and regulation)

Section II Data in the System:

1. Will this system contain personal data elements? (See Definitions for a list of common data elements considered personal.)

☐ No (See Section IX)

☒ Yes (Continue)

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

- Name and/or other names *i.e.* maiden name
- Social Security Number
- Home Address – Current and History
- Bank Account
- Telephone Contact Information

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

☒ NLRB files or databases.

Regional offices maintain addresses and contacts of discriminatees.

☒ Non- NLRB files or databases. The discriminate list provided by the employers.

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

☐ State and local agencies.

☐ The record subject himself/herself.

☐ 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/form and attach a copy.

Yes, the Regional Office Accounting Manual

5. Review the list of personal data elements you currently collect. Is each data element essential to perform some official function? *[This question only pertains to data elements you specifically solicit. Provide explanation in the additional information section as 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.

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

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

Section III Verifying Data:

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

   a. Accuracy:
   b. Completeness:
   c. Relevance:
   d. Timeliness:

   Data collected and verified for Accuracy, Completeness, Relevancy and Timeliness by the regional compliance officer from the employers.

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

   The application resides on existing NLRB platforms that are protected by the NLRB firewall and intrusion detection systems. The data and system files are restricted to user's personal computers and access to local area network file locations.

Section IV Access to the Data:

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

   Regional compliance officers, regional directors, and the Finance Branch

2. How is right of access to the data by a user determined?

   The Finance Director determines who needs access to the system and based upon the functions assigned to the employee.

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

   No, but access to the system and data is based upon the Finance Director designating the access for the user.

4. What controls are in place to prevent the misuse (e.g. browsing) of data by those individuals having access? Do not go into so much detail as to compromise system security.

   The access control is implemented by user role authorization, and data encryption.

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

   ☒ No

   ☐ Yes (Explain)

6. Will other non-NLRB 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.)

7. How will the system ensure that agencies only get the needed information to fulfill their official functions?

   Not Applicable

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

   NLRB Finance personnel, in conjunction the CIO and CISO.

9. Who is responsible for assuring proper use of the data? Provide name, title, mailing address and current telephone number.)

   Isabel McConnell
   Chief Financial Officer
   Isabel.McConnell@nlrb.gov
   Phone: 202-273-3726

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 designed?

   ☐ No (Explain)

   ☒ 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/database.)

☒ Not Applicable

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

☐ No

☐ Yes (Explain)

☒ Not Applicable

2c. Will the data be retrieved by personal identifier (name, SSN, employee number, computer ID number, etc.)? The data can be retrieved by name, but data relating to individuals are not disclosed to the public.

☐ No (Go to Section VI.)

☐ Yes (List retrieval fields)

☒ Not Applicable

2d. Are there potential effects on the due process rights of citizens and lawfully admitted aliens?

2d-l. Consolidation and linkage of files and systems?

☐ No ☐ Yes ☒ Not Applicable

2d-2. Derivation of data?

☐ No ☐ Yes ☒ Not Applicable

2d-3. Accelerated information processing anddecision-making?

☐ No ☐ Yes ☒ Not Applicable

2d-4. Use ofnew technologies?

☐ No ☐ Yes ☒ Not Applicable

2e. How are any effects discussed in 2d-1 through 2d-4 to be mitigated?

Not Applicable

<u>Section VI Maintenance of Administrative Controls:</u>

1. Describe how the system and its use will ensure equitable treatment of individuals. If the system is operated in more than one site, also include a discussion of how consistent use of the system and data will be maintained in all sites.

   The system is designed to facilitate NLRB's fiduciary obligation to manage the funds related to the accurate and timely issuance of monetary awards to discriminatees.

2. Explain the possibility of disparate treatment of individuals or groups.

   The remotest possibility of disparate treatment might occur when the occasional discriminatee does not provide a timely residential address or fails to cash an award check within the time specified by the U.S. Department of the Treasury.

3. What are the retention periods for the data in this system?

   All BMS data is kept in Azure SQL, there is no plan to delete/archive any data.

3a. Does your retention period agree with that listed in Appendix I, of the NLRB Files? Management and Records Disposition Handbook?

☐ No (Provide Explanation)

☒ Yes (List disposal rule from the Appendix I of NLRB Files Management & Records Disposition Handbook)

NLRB Files Management and Records Disposition Handbook Chapter 8, Standard Number 802-13, crosswalk to 802-02. Disposition Permanent, Transfer to NARA 30 years after cutoff.

3b. What are the procedures for eliminating the data at the end of the retention period?

Not applicable.

3c. Where are the elimination of data procedures documented as discussed in Question 3b above?

There is no plan to delete any BMS data.

3d. Is the system using technologies in ways that the NLRB has not previously? employed (e.g. Caller-ID, surveillance, etc.)?

☒ No (Continue.)

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

3e. Will this system provide the capability to identify, locate, and monitor individuals?

☒ No

☐ Yes (Provide Explanation)

3f. Will this system provide the capability to identify, locate, and monitor groups of people?

☒ No

☐ Yes (Provide Explanation)

3g. What controls will be used to prevent unauthorized monitoring? Do not describe your controls and procedures in so much detail as to compromise system security.

OCIO IT Security scheme

Section VII Interface with Privacy Act Systems of Records:

1. Does this system currently operate under an existing NLRB or Government-Wide Privacy Act system of records? NLRB and Government Wide systems are described at: *http://www.access.gpo.gov/su_docs/aces/PrivacyAct.shtml* and https://www.whitehouse.gov/omb/memoranda_m99-05-c/

   ☐ No (Go to Section VIII)
   ☒ Yes (Continue)

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

3. If an existing NLRB Privacy Act system of records is being modified, will the system notice require amendment or alteration? Provide a list all proposed changes. Consider the following, will you be collecting new data elements not previously approved forcollection; using the data for new internal purposes; sharing the data with new non-NLRB agencies; keeping the records longer; creating new locations of data, etc.?)

   ☐ No
   ☐ Yes (Explanation of 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 (Explanation of changes)
   ☐ Yes (Go to Section VIII)
   ☒ Not Applicable

5. If you answered "no" to **Section VII- Number 4** above, have you consulted with the government agency that "owns" the government-wide system in determining 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 contact information of the official with responsibility for the government-wide system)
   ☒ Not Applicable

6. Is there a Authority to Operate of record within OCIO's FISMA tracking system?

   ☐ Unknown
   ☐ No
   ☒ Yes (Please provide the determination of Low/Moderate/High/Undefined for each of the following:)

   Confidentiality - Moderate

   Integrity - Moderate

   Availability - Moderate

Section VIII. Certification: Personnel Security Files

I have read and understand the purpose of this assessment. I have reviewed the definition of "personal data" and have accurately listed the personal data elements collected or accurately answered all questions contained in this Privacy Impact Assessment.

System Owner Name	Kimberly Jackson signing on behalf of Isabel McConnell
System Owner Title	Chief Financial Officer
System Owner E-mail Address	Isabel.McConnell@nlrb.gov
System Owner Telephone & Fax Number	(202) 273-3726
System Owner's Signature/Date	KIMBERLY JACKSON Digitally signed by KIMBERLY JACKSON Date: 2019.08.12 10:45:44 -04'00'

IT Security Officer’s Name	Tremell Warren
IT Security Officer Title	Associate Chief Information Officer, Information Assurance
IT Security Officer’s E-mail Address	Tremell.Warren@nlrb.gov
I`T Security Officer’s Telephone	(202) 273-0766
Records Management Officer’s Signature/Date	TREMELL WARREN Digitally signed by TREMELL WARREN Date: 2019.08.12 11:05:27 -04'00'

Records Management Officer’s Name	Kenneth Williams
Records Management Officer Title	Supervisory Records and Information Management Specialist
Records Management Officer’s E-mail Address	Kenneth.Williams@nlrb.gov
Records Management Officer’s	(202)273-2833
Records Management Officer’s Signature/Date	KENNETH WILLIAMS Digitally signed by KENNETH WILLIAMS Date: 2019.08.09 12:42:23 -04'00'

Privacy Officer’s Name	Virginia Ephraim
Privacy Officer Title	Information Security, Compliance and Privacy Specialist
Privacy Officer’s E-mail Address	Virginia.Ephraim@nlrb.gov
Privacy Officer’s Telephone	(202) 273 -0010
Privacy Officer’s Signature/Date	VIRGINIA EPHRAIM Digitally signed by VIRGINIA EPHRAIM Date: 2019.08.09 12:12:14 -04'00'

OCIO Deputy OCIO Name	Eric Marks
OCIO Deputy OCIO Title	Deputy Chief Information Officer
Deputy CIO’s E-mail Address	Eric.Marks@nlrb.gov
OCIO Deputy OCIO Telephone	(202) 273-4131
OCIO Deputy OCIO Signature/Date	CHARLES MARKS Digitally signed by CHARLES MARKS DN: c=US, o=U.S. Government, ou=National Labor Relations Board, cn=CHARLES MARKS, 0.9.2342.19200300.100.1.1=63001000009755 Date: 2019.08.12 10:00:00 -04'00'

OCIO CIO Name	Prem Aburvasamy
OCIO CIO Title	Chief Information Officer
OCIO CIO’s E-mail Address	Prem.aburvasamy@nlrb.gov
OCIO CIO Telephone	(202) 273-3925
OCIO CIO Signature/Date	PREM ABURVASAMY Digitally signed by PREM ABURVASAMY Date: 2019.08.09 13:13:11 -04'00'

Definitions

Accounting of Disclosures – a record showing all third party disclosures made from a system. The disclosure accounting shows the date, recipient name, recipient address, purpose, and the data elements disclosed. You need not account for disclosures made to NLRB employees who require access to the data to perform official duties.

Accuracy – within sufficient tolerance for error to assure the quality of the record in terms of its use in making a determination.

Completeness – all elements necessary for making a determination are present before such determination is made.

Determination – **any** decision affecting an individual which, in whole or in part, is based on information contained in the record and which is made by any person or agency.

Disclosure – the transfer of any personal information from a system of records by any means of communication (oral, written, electronic, mechanical, or actual review) to any person, private entity, or government agency, other than the subject of the record, the subject's designated agent, or the subject's legal guardian.

Necessary – a threshold of need for an element of information greater than mere relevance and utility. A data element is "necessary" if the program cannot function properly or efficiently without it.

Personal Data – data about an individual that is personal in nature. Personal data may consist of home address; home email address; home telephone numbers; date and place of birth; marital status; names of spouse and children; financial, credit, and medical data; SSN; take home pay; credit card account numbers; mother's maiden name; other names used; government life and health insurance options elected; criminal history; for individuals assigned to (or about to be assigned to) overseas, sensitive, or routinely duty stations, their names, duty stations, duty addresses, and duty telephone numbers; performance ratings; race and national origin data; citizenship; religion; annual and sick leave use and balances; security clearance information; drug test results; and the fact of participation in rehabilitation or employee assistance programs. The following data elements are **NOT** normally considered personal: U.S. based work addresses and work telephone numbers; position data; performance elements; date of rank; source of commission; education level; education and training paid for by the government; job related certifications; current and past annual salary rates (but not take home pay); position titles; occupational series; and current and past grades. **NOTE: If you are not sure if the data elements you plan to collect are considered "personal," contact NLRB Privacy Officer.**

Record – **any** item, collection or grouping of information about an individual and identifiable to that individual that is maintained by an agency.

Relevance – limitation to only those elements of information which clearly bear on the determination(s) for which the records are intended. A data element is "relevant" if you cannot make a determination without it.

Routine Use – the disclosure of a record outside the National Labor Relations Board for a use that is compatible with the purpose for which the information was collected and maintained. The "Routine Users" that have been authorized access to each NLRB data system are listed in the governing NLRB or government-wide Privacy Act system notice. *The NLRB and Government Wide systems are described* *at: http://www.access.gpo.gov/su_docs/aces/PrivacyAct.shtml and http://www.whitehouse.gov/omb/memoranda/m99-05-c.html*

System of Records – a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. Each Federal agency is required to publish in the Federal Register full descriptions of its systems of records. Some systems of records are "owned" by one agency but maintained at another agency. The "owning" agency is responsible for publishing a system notice for all Federal agencies to follow. These are referred to as "Government Wide" system notices. Example 1: Civilian Official Personnel Files are "owned" by the Office of Personnel Management but maintained at the employing agency. OPM publishes the system notice. Example 2: Workers Compensation Case files are "owned" by the Department of Labor but maintained at the employing agency. Thus, Labor publishes the system notice. *The NLRB and Government Wide systems are described at: http://www.access.gpo.gov/su_docs/aces/PrivacyAct.shtml and http://www.whitehouse.gov/omb/memoranda/m99-05-c.html*

Third Party – an organization, entity, or individual other than the record subject himself, his designated agent, or his legal guardian. For purposes of disclosure accountings, a NLRB employee is not considered a "third party" when performing officially assigned duties.