

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 National Labor Relations Board (NLRB) appropriately considers privacy issues from the earliest stages of design.

Purpose: The purpose of this Privacy Impact Assessment is to determine if your proposed plans to collect, maintain, and use data in an automated system will impact on the Privacy rights of U. S. Citizens and lawfully admitted aliens. Depending on your answers, we may be required to seek additional details from you to comply with certain publication requirements of the Privacy Act (5 U.S.C. 552a). Please direct questions to Steven Coney, 202-273-2833.

Authorities: 5 U.S.C. 552a, The Privacy Act of 1974, as implemented by OMB Circular A-130.

Other Requirements: You may be required to conduct a NLRB Security Certification and Accreditation Process as required by OMB Circular A-130. Contact NLRB-ITB or your local information technology office for details.

Definitions: Some terms in this assessment have unique or specific meanings. Therefore, please review the "Definitions" section before completing this assessment.

Returning Assessments: Return this completed assessment to National Labor Relations Board (NLRB-LASB), 1099 14th Street, NW, Room 7620, Washington, DC 20570-0001.

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 parentheses after the name.

National Labor Relations Board (NLRB) Office of Inspector General Investigative Files (OIG Investigations Data Base)

2. In five sentences or less, provide a generalized broad description of the system and its purpose. (*What does this system do; what function does it fulfill.*)

OIG Investigations Data Base is an information storage and retrieval system that utilizes Microsoft Access to electronically record actions that initiate, change, or complete activities within the lifecycle of an OIG investigation. This system is designed to collect, process, and maintain case handling data; track active data and compile performance measurement data.

3. Describe the stage of development of this system:

This is a new system which is --
 Still in the planning stages.
 Mid-way to launch.
 Ready for launch.
Anticipated Launch Date: _____

We propose to change an existing system, the changes of which are:
 Still in the planning stages.
 Mid-way to launch.
 Ready for launch.
Anticipated Launch Date: _____

Other (Explain, providing the data required above for new or existing systems.)

The OIG Investigations Data Base was created prior to this reporting requirement.

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

No.

_____ Yes. (*List the law or Executive Order and the implementing NLRB regulations.*)

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 _____ *(Go to Section IX.)*

Yes X *(Continue.)*

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

First and last names of individual involved in the OIG investigation to include the subject, source of the allegation, witnesses, and investigators. Additionally, the system has a "Notes" section for the recording of other information that may be needed during the course of the investigation. This information often includes addresses and telephone numbers of subjects and witnesses.

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

X NLRB or other agency files or databases.

X Other agencies. *(List.)*

_____ State and local agencies. *(List.)*

X The record subject himself.

X Supervisors.

X Other third party sources. *(List.)*

Witnesses, the Internet, or other publicly available source.

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 and attach a copy.

No name, See attached copy

5. Review the list of personal data elements you currently collect. Is each data element essential to perform some official function? *[Note: This question only pertains to data elements 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 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 or the record subject himself, describe how the data will be verified for --

a. Accuracy:

The nature of an investigation is the determination of the accuracy, completeness, and relevance of the data. Once an investigation is completed, a report is made regarding these issues.

b. Completeness:

The nature of an investigation is the determination of the accuracy, completeness, and relevance of the data. Once an investigation is completed, a report is made regarding these issues.

c. Relevance:

The nature of an investigation is the determination of the accuracy, completeness, and relevance of the data. Once an investigation is completed, a report is made regarding these issues.

d. Timeliness:

All cases are monitored by the Inspector General to ensure timeliness. Additionally, cases are reported in OIG the Semi-annual Report to Congress.

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

Hard copies of the information are maintained in the case file once the case is closed. While the case is open, the information is reviewed on a regular basis. Access to the system is limited to OIG employees in the OIG office suite.

Section IV. Access to the Data.

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

Users, Managers, and Technical Support — on an as needed basis.

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

All users have the same right of access to data. Users are limit to OIG managers in the OIG office suite.

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

Users are limited to OIG managers in the OIG office suite. The system is located on the OIG portion of a server. Passwords are required to access the server and user rights are required to access the OIG portion of the server. A second password is required to access the electronic database. Hardcopy files are maintained in controlled OIG office space.

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

The potential for misuse is controlled by limiting access to the database to only those OIG managers with a need to know the data. Other OIG personnel have not been provided the access password.

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

No _____

Yes X

The system is located with a tracking system for OIG audits.

6. Will other agencies share data or have direct access to data in this system (International, Federal, State, Local, Other)?

No X *(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 information they need to fulfill their official functions?

N/A

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

N/A

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

David Berry
Counsel to the Inspector General
Office of Inspector General, National Labor Relations Board
1099 14th Street NW, Suite 9820
Washington, DC 20570

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 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.)

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.)

2d. What are the potential effects on the due process rights of citizens and lawfully admitted aliens of-

2d-1. Consolidation and linkage of files and systems?

Not Applicable X

2d-2. Derivation of data?

Not Applicable X

2d-3. Accelerated information processing and decision making?

Not Applicable X

2d-4. Use of new technologies?

Not Applicable X

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

Section VI. Maintenance of Administrative Controls.

1. Explain how the system and its use will ensure equitable treatment of individuals. (NOTE: 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 requires the same information for each subject and case.

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

None.

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

The following retention periods are applied to this system, depending upon the type of data: (a) Destroy/delete when dissemination, revision, or updating is completed; (b) Destroy/delete within 180 days after the recordkeeping copy has been produced; (c) Cut off closed cases at the end of each fiscal year and destroy 5 years after cutoff; (d) Cut off closed cases at the end of each fiscal year and destroy 10 years after cutoff, and (e) *Permanent*, cut off closed cases at the end of each fiscal year and transfer to the National Archives of the United States 25 years after cutoff.

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

No ___ X ___ (*Explain.*)

The system is part of the investigative file which has its own records disposition criteria that was approved by NARA and will be incorporated in the next revision on the NLRB Files Management and Records Disposition Handbook

Yes _____ (*List disposal rule from NLRB Files Management and Records Disposition Handbook*)

(See the response to Item Number 3)

3b. What are the procedures for eliminating the data at the end of the retention period?
(See the response to Item Number #3)

3c. Where are the procedures discussed in Question 3b above documented?

The NARA approved records disposition authority. The system also has a field that indicates when elimination or permanent retention is required.

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

No ___ X ___

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 ___ X ___

Yes _____ (*Explain.*)

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

No ___ X ___

Yes _____ (*Explain.*)

3g. 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.*)

No monitoring is possible with this system.

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? (*Note: The NLRB and Government Wide systems are described at: <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi> and <http://www.whitehouse.gov/omb/memoranda/m99-05-c.html>*)

No _____ (*Go to Section VIII.*)

Yes X (*Continue.*)

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

NLRB – 18 Office of Inspector General Investigative Files

3. If an existing NLRB 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 purposes; sharing the data with other agencies; keeping the records longer; creating new locations of data, etc?*)

No _____

Yes _____ (*Explain your changes.*)

Not Applicable X

3. 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

4. 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. Accounting of Disclosures: When data is disclosed to any individual outside of the Agency, NLRB is required to record the date of the disclosure, the recipient's name and address, the purpose of the disclosure, and the actual data elements disclosed. This record of the disclosure is referred to as an "Accounting of Disclosures."

1. What steps have been taken to insure that the Accounting of Disclosures is maintained as required by 5 U.S.C. 552a?

 The system software has the capability to generate a list of all disclosures that includes recipient name, address, date, data elements disclosed, and the purpose.

 X The accounting of disclosures will be kept manually. Identify the person who will be responsible for maintaining the accounting. (*List the person's name, title, address, and telephone number.*)

Jennifer Kovachic

Counsel to the Inspector General 202- 273-1960

2. How will the system account for mass disclosures (such as time and attendance, payroll, and similar types of data)?

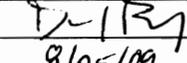
No mass disclosures are allowed.

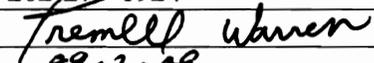
3. What procedures are in place to ensure that the Accounting of Disclosures is maintained for 5 years or the life of the record, whichever is longer?

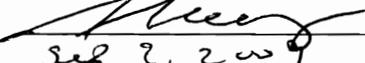
NARA approved records disposition authority for investigative files.

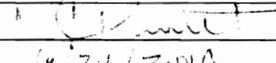
Section IX. Certification:

Certification: I have read and understand the purpose of this assessment. I have also reviewed the definition of "personal data" and have accurately listed the personal data elements collected or accurately answered "no" to Question II-1.

Name: David Berry
 Title: Systems/Program Manager
 Email Address: David.Berry@nlrb.gov
 Telephone Number: 202-273-1964
 FAX Number: 202-273-2344
 (Signature) 
 (Date) 8/25/09

Name: Tremell Warren
 Title: Chief, IT Security
 Email Address: tremell.warren@nlrb.gov
 Telephone Number: 202-273-0766
 FAX Number: 202-273-1924
 (Signature) 
 (Date) 09-2-09

Name: Steven Coney
 Title: Privacy Act Officer
 Email Address: steven.coney@nlrb.gov
 Telephone Number: 202-273-2833
 FAX Number: 202-273-4286
 (Signature) 
 (Date) sep 2, 2009

Name: Bryan Burnett
 Title: Acting, Chief Information Officer
 Email Address: bryan.burnett@nlrb.gov
 Telephone Number: 202-273-2555
 FAX Number: 202-273-1924
 (Signature) 
 (Date) 9/24/2009

Microsoft Access [Investigations] [X] [X]

File Edit View Insert Format Records Tools Window Help

Case Number: OIG-1 [] Org Unit: [] Main Menu

Date OIG notified: [] Sub Unit: []

Date Opened: [] Joint Investigation: Allegation Type: []

Subject Last Name: [] First Name: [] Type of Violation: Criminal

Assigned To: [] Allegation Summary: []

Referred to for investigation: [] IG Findings: []

Date Referred for investigation: []

Source Type: [] Source: []

18 USC 289: Date of OIG Report: []

Referred for Personnel Action: Referred to DOJ Criminal: Date Referred to DOJ: []

Referred to: [] Referred to DOJ Civil: []

Adverse Personnel Action: Criminal Conviction: Statute(s): []

Type of Personnel Action: [] Restitution: \$0.00

Date of Personnel Action: []

Investigative Recovery: [] Witness Confidentiality:

Source Notified:

Record: 14 | 90 of 90

Form View 10:29 AM

