National Labor Relations Board
Security Branch

iTrak
Privacy Impact
Assessment
Prepared: April 2026

The Office of the Chief Information Officer

Introduction:

This Privacy Impact Assessment (PIA) is necessary for iTrak. This PIA is primarily based on the Office of Management and Budget (OMB) privacy guidance and the National Labor Relations Board (NLRB) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PIA, please contact NLRB's Privacy Officer.

Abstract/Overview: iTrak Incident & Security Management software is a SaaS (Software as a Service) product used to store incidents and information concerning threats made against NLRB employees or operating locations. iTrak Incident & Security Management Software (TMD) provides a repository of information for all reported Regional specific or veiled threats directed towards the agency. Secondly TMD acts as a repository for reports of any terminated (for cause) employee who may pose a future problem. Once reports and information regarding subjects are obtained and finalized, the data is available for search and retrieval by Security Branch personnel, Regional Directors and select agency leadership personnel.

Section 1 Reason for the PIA:

1.1. Is the Agency developing or procuring an IT system or project that collects, maintains, or disseminates information in identifiable form from or about members of the public?

- No, the system is already in production. iTrak does store PII from members of the public.

1.2 If a current IT system or project is undergoing a significant change, please describe. [For examples of significant changes, please see OMB Memorandum M-03-22 (Sept. 26, 2003).]

- No

1.3 Is the Agency initiating a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities, or employees of the federal government)?

- No

Section 2 Authorities and Other Requirements:

2.1. What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

- **Privacy Act of 1974, 5 U.S.C. § 552a**
- **5 U.S.C. § 552(h) (FOIA / OGIS authority)**
- **28 U.S.C. § 1746 (unsworn declarations)**
- **40 U.S.C. § 1315 (Federal facility security authority)**
- **44 U.S.C. Chapters 21 and 33 (Federal records management)**

- **Executive Order 12958, as amended by Executive Order 13292 (National security classification)**
- **41 C.F.R. §§ 102-81.10 and 102-81.15 (Federal building security)**
- **29 C.F.R. § 102.119 (a), (b), (c), (d) (NLRB Privacy Act regulations)**

2.2. Does a current Privacy Act System of Records Notice(s) (SORN(s)) apply to the information? (*If the answer is no, then ensure that Section 10 below is addressed based on the analysis in this PIA.*)

- Yes - NLRB-34 NLRB iTrak and Banned Entry List

2.3. Has a system security plan been completed for the information system(s) supporting the project?

- iTrak is a minor application with the SBIS boundary.

2.4. Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

- GRS 5.6, Item 100, Security Records, Accident and Incident records.

2.5. If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

- N/A

Section 3 Characterization of the Information:

3.1. Identify the information the project collects, uses, disseminates, or maintains.

- iTrak collects, uses, and maintains personally identifiable information necessary for assessing and managing threats against NLRB personnel and facilities, including Social Security numbers, dates and places of birth, home and work contact information, personal and work email addresses, driver's license numbers, and security clearance details, as well as incident narratives, threat reports, law-enforcement-derived data, interviews, and subject information gathered from NLRB systems, federal and state agencies, the record subject, and third-party sources such as police and CLEAR reports; all of this information is stored to support security investigations, monitor individuals who may pose risks, and provide a searchable repository for authorized Security Branch personnel.

3.2. What are the sources of the information and how is the information collected for the project?

- iTrak stores information from multiple authoritative sources to support threat assessment and security operations. iTrak collects data directly from NLRB records and databases as well as from non-NLRB federal systems, including OPM Federal Investigative Service files, and from state and local agencies involved in law enforcement activities. Information is also collected directly from the record subject during interviews, along with additional details gathered from third-party sources such as police reports, CLEAR reports, driver's license records, and records from other federal agencies.

3.3. Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

- Yes, the system does use information from commercial sources and publicly available data, and this information is incorporated to support accurate threat assessments and security investigations. Specifically, iTrak receives information from commercial investigative tools such as CLEAR reports, as well as publicly available records including driver's license records and state or local law-enforcement documentation. These sources are used to verify identities, validate incident details, supplement investigative findings, and ensure that the information entered into iTrak is accurate, complete, and up-to-date.

3.4. Discuss how accuracy of the data is ensured.

- iTrak ensures the accuracy, completeness, and timeliness of data through a multilayered verification process involving trained law-enforcement and security personnel. Information obtained from external sources such as state, federal, and county agencies, police reports, CLEAR reports, and other investigative records is validated by Department of Homeland Security Police Officers and NLRB physical security specialists, who confirm accuracy during subject interviews and through official records checks.

3.5. Privacy Impact Analysis: Related to Characterization of the Information

3.5.1. Privacy Risk: None.

3.5.2. Mitigation: None.

Section 4 Uses of the Information

4.1. Describe how and why the project uses the information.

- iTrak uses the information it stores to support the NLRB's mission of protecting employees and agency facilities by enabling effective identification, assessment, and management of security threats. The system serves as a centralized repository for incident reports, subject information, and investigative findings, allowing Security Branch personnel, Regional Directors, and select leadership to retrieve and analyze information related to threats against staff or operating locations. This information is used to evaluate risk levels, guide protective actions, and maintain awareness of individuals such as terminated employees or external subjects who may pose ongoing security concerns.

4.2. Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how NLRB plans to use such results.

- No, the project does not use technology to perform electronic searches, queries, or analytical processes to identify predictive patterns or anomalies. The system functions as a repository for storing, retrieving, and managing information related to threats against NLRB personnel or facilities.

4.3. Are there other components with assigned roles and responsibilities within the system?

Several components within the agency have assigned rolesand responsibilities in operating and overseeing the system. The Security Branch's Physical Security Section and the Chief Security Officer are the primary users with access to the system, responsible for entering, reviewing, and managing incident and subject data. Additionally, the Office of the Chief Information Officer (OCIO) serves as the system administrator, maintaining the technical environment, managing system performance, and enforcing access controls. These roles ensure that operational, security, and administrative responsibilities are clearly divided so that iTrak functions effectively while safeguarding the sensitive information it contains.

4.4. Privacy Impact Analysis: Related to the Uses of Information

4.4.1. Privacy Risk: None.

4.4.2. Mitigation: None.

Section 5 Notice

5.1. How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

- Individuals are not provided notice prior to the collection of information, because the system is used for security and threat-assessment purposes where advance notice could compromise the agency's ability to investigate, verify, and respond to potential risks. The information maintained in iTrak is gathered as part of law-enforcement activities, security interviews, and incident reporting processes conducted by DHS Police Officers, NLRB Physical Security Specialists, and other authorized personnel.

5.2. What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

- Data is gathered from official records, law-enforcement sources, interviews, and third-party reports to ensure the NLRB can identify, evaluate, and respond to threats against its personnel and facilities. As a result, individuals who are the subjects of security incidents do not have the ability to opt out or restrict the collection or use of information required for these legally authorized security purposes.

5.3. Privacy Impact Analysis: Related to Notice

5.3.1. Privacy Risk: None.

5.3.2. Mitigation: None.

Section 6 Data Retention by the Project

6.1. Explain how long and for what reason the information is retained.

- GRS 5.6, Item 100, Security Records, Accident and Incident records. Destroy three (3) years after final investigation or reporting action or when three (3) years old, whichever is later, but longer retention is authorized for business use.

6.2. Is the record retention compatible with any applicable SORN? (See Question 2.2, "*WY*

- Yes, NLRB-34 NLRB iTrak and Banned Entry List

6.3. Privacy Impact Analysis: Related to Retention

6.3.1. Privacy Risk: None.

6.3.2. Mitigation: None.

Section 7 Information Sharing

7.1. Is information shared outside of NLRB as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

- iTrak receives data from external law-enforcement agencies, but NLRB does not share iTrak data with those agencies as part of normal operations.

7.2. Describe how the external sharing noted in 7.1 is compatible with any applicable SORN? (See Question 2.2, "*What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?*")

- The external sharing noted in 7.1 is compatible with the applicable SORN because the NLRB does not disclose iTrak information to external agencies as part of normal operations. The system only receives information from external law enforcement, and this intake supports the system's authorized purpose.

7.3. Does the project place limitations on re-dissemination?

- Yes. iTrak does place limitations on re-dissemination of the information it contains. Access to the system is strictly limited to the NLRB Security Branch's Physical Security Section, the Chief Security Officer, and OCIO system administrators, and no external agencies are given direct access to iTrak data as part of normal operations.

7.4. Describe how the project maintains a record of any disclosures outside of the agency?

- Although iTrak does not share information externally, any permitted disclosure such as those made under the routine uses of SORN NLRB-34 for law-enforcement or security purposes must be logged in accordance with these policies to ensure transparency, compliance, and auditability.

7.5. Privacy Impact Analysis: Related to Information Sharing

7.5.1. Privacy Risk: None.

7.5.2. Mitigation: None.

Section 8 Redress

8.1. What are the procedures that allow individuals to access their information?

- Individuals may request access to any information about themselves maintained in iTrak through the Privacy Act and Freedom of Information Act (FOIA) processes applicable to NLRB Privacy Act systems of records. Because iTrak operates under SORN NLRB-34 (I-Trak and Banned Entry List), individuals seeking access must submit a Privacy Act request identifying the relevant system, after which the agency evaluates the request in accordance with statutory requirements and applicable exemptions.

8.2. What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

8.3. How does the project notify individuals about the procedures for correcting their information?

8.4. Privacy Impact Analysis: Related to Redress

8.4.1. Privacy Risk: None.

8.4.2. Mitigation: None.

Section 9 Auditing and Accountability

9.1. How does the project ensure that the information is used in accordance with stated practices in this PIA?

- Individuals may request correction of inaccurate or erroneous information maintained in iTrak through the Privacy Act amendment process, which applies to all NLRB Privacy Act systems, including those covered by SORN NLRB-34.

9.2. Describe what privacy training is provided to users either generally or specifically relevant to the project.

- Users of iTrak receive privacy training as part of the NLRB's mandatory annual IT Awareness Training program, which includes modules on Cybersecurity, Privacy, Insider Threat, and Handling Sensitive Information. These trainings are required for all employees, contractors, and individuals with network access in compliance with OMB A-130, FISMA,

and NIST requirements, ensuring users understand how to properly handle, safeguard, and use personally identifiable information within systems like iTrak.

9.3. What procedures are in place to determine which users may access the information and how does the project determine who has access?

- Access to information in iTrak is strictly controlled and granted only to users who have a demonstrated need-to-know in support of NLRB security operations. The Chief Security Officer determines which staff members within the Security Branch's Physical Security Section are authorized to use the system.

9.4. How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within NLRB and outside?

- The project reviews and approves information-sharing agreements, MOUs, new uses of information, and any new access requests through a structured governance process consistent with NLRB privacy and security policy.

9.5. Privacy Impact Analysis: Related to the Accountability and Integrity of the Information.

9.5.1. Privacy Risk: None.

9.5.2. Mitigation: None.

Section 10 Privacy Act System of Records (SORN)

10.1. If the answer to question 2.2 above ("Does a current Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?") is no, then based on the information in this PIA, is a new SORN required? If a current SORN applies but requires modification based on the information in this PIA, please explain.

- N/A - NLRB-34 NLRB iTrak and Banned Entry List

Section 11 Certification

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: Raymond Hankins
Title: Chief Security Officer
E-mail Address: Raymond.Hankins@nlrb.gov
Telephone: (202) 273-3790
Signature: RAYMOND HANKINS
Date: Digitally signed by RAYMOND HANKINS Date: 2026.05.05 07:24:06 -04'00'

Name: Fitz Raymond
Title: ACIO Information Assurance / Acting CISO
E-mail Address: Fitz.Raymond@nlrb.gov
Telephone: 202-273-1084
Signature: FITZ RAYMOND
Date: Digitally signed by FITZ RAYMOND DN: c=US, o=U.S. Government, ou=National Labor Relations Board, cn=FITZ RAYMOND, 0.9.2342.19200300.100.1.1=63001002928583 Date: 2026.05.08 14:05:56 -04'00'

Name: Kenneth Williams
Title: Records Management Officer
E-mail Address: Kenneth.Williams@nlrb.gov
Telephone: 202-273-2833
Signature: KENNETH WILLIAMS
Date: Digitally signed by KENNETH WILLIAMS Date: 2026.05.05 12:19:38 -04'00'

Name: Ibrahim M. Ibrahim
Title: Sr. Privacy Analyst
E-mail Address: Ibrahim.Ibrahim@nlrb.gov
Telephone: 202-273-4259
Signature: IBRAHIM IBRAHIM
Date: Digitally signed by IBRAHIM IBRAHIM Date: 2026.05.05 11:32:00 -04'00'

Name: Prem Aburvasamy
Title: Chief Information Officer
E-mail Address: Prem.Aburvasamy@nlrb.gov
Telephone: 202-273-3925
Signature: PREM ABURVASAMY
Date: Digitally signed by PREM ABURVASAMY Date: 2026.05.14 09:19:37 -04'00'