Privacy Act of 1974; System of Records

This Notice document was issued by the National Labor Relations Board

---

NATIONAL LABOR RELATIONS BOARD

Privacy Act of 1974; System of Records

AGENCY:

National Labor Relations Board (NLRB).

ACTION:

Notice of a New Privacy Act System of Records.

SUMMARY:

In accordance with the Privacy Act of 1974, the National Labor Relations Board proposes to issue a National Labor Relations Board system of records notice titled "NLRB iTrak and Banned Entry List" (NLRB-34) to support the protection of employees, contractors, and property leased, or occupied, by the National Labor Relations Board. This system of records includes the NLRB's iTrak Incident & Security Management Software System ("iTrak"), which is used to manage information on individuals who have been reported to present a threat or potential threat to NLRB employees, contractors, and property, as well as a Banned Entry List, which is a list of individuals banned from entering NLRB facilities based on information in iTrak. The system allows the National Labor Relations Board to collect and maintain records on the results of law enforcement activities concerning individuals maintaining a presence at or who have access to property leased or occupied by the NLRB and who have been reported to present a threat as described above. The NLRB is issuing this system of records notice in compliance with the Privacy Act of 1974, 5 U.S.C. 552a. This issued system notice will be included in the NLRB inventory of record systems.

All persons are advised that, in the absence of submitted comments considered by the Agency as warranting modification of the notice as here proposed, it is the intention of the Agency that the notice shall be effective upon expiration of the comment period without further action.

DATES:

Written comments on the system's routine uses must be submitted on or before [30 days after publication]. This system will be effective upon publication. The routine uses in this action will become effective on [30 days after publication] unless written comments are received that require a contrary determination.

ADDRESSES:

All persons who desire to submit written comments for consideration by the Agency in connection with this proposed notice of the amended system of records shall mail them to the Agency's Senior Agency Official for Privacy, National Labor Relations Board, 1015 Half Street S.E., Third Floor, Washington, DC 20570-0001, or submit them electronically to privacy@nlrb.gov. Comments may also be submitted electronically through http://www.regulations.gov, which contains a copy of this proposed notice and any submitted comments.

FOR FURTHER INFORMATION CONTACT:

For general questions and privacy issues please contact: Privacy and Information Security Specialist, Office of the Chief Information Officer, National Labor Relations Board, 1015 Half Street S.E., Third Floor, Washington, DC 20570-0001, (202) 273-3733, or at privacy@nlrb.gov.

SUPPLEMENTARY INFORMATION:

The Agency exempts a new system of records, NLRB-34, NLRB iTrak and Banned Entry List, from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f). The Agency is claiming exemptions

pursuant to Section 5 U.S.C. 552a(k)(1), (2), and (5) of that Act. The Agency's Direct Final Rule setting forth these exemptions appears elsewhere in today's issue of the Federal Register.

In accordance with 5 U.S.C. 552a(r), the NLRB has provided a report of this system of records to Congress and to the Office of Management and Budget.

NLRB-34

SYSTEM NAME:

NLRB iTrak and Banned Entry List

SECURITY CLASSIFICATION:

Most of the iTrak and Banned Entry List records are not classified. However, limited records of individuals, or portions of records, may be classified in the interest of national security.

SYSTEM LOCATION:

Records are maintained at the National Labor Relations Board Headquarters in Washington, DC and in NLRB field locations, which are available at https://www.nlrb.gov/who-we-are/regional-offices.

SYSTEM MANAGER:

For all locations: Chief Security Officer, Security Branch, (202) 273-1990, 1015 Half Street S.E., Washington, DC 20570-0001.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Executive Order 12958, as amended by Executive Order 13292; Title 5 U.S.C. 552a(e)(10); Title 44 U.S.C. chapters 21 and 33. These statutes and Executive Orders are directed toward security of United States Government records maintained by

federal agencies. Title 40 U.S.C. section 1315, and Title 41 C.F.R. section 102-81.10 and 81.15. This statute and the federal regulations are directed toward security of United States Government buildings and the people working at and visiting such buildings.

PURPOSES OF THE SYSTEM:

The purpose of this system is to maintain and record the results of law enforcement activities in support of the protection of NLRB employees and contractors and of property leased or occupied by the National Labor Relations Board and its Regional Offices. It will also be used to pursue criminal prosecution or civil penalty actions against individuals or entities suspected of offenses that may have been committed against property owned, occupied, or secured by the NLRB or persons on the property.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Categories of individuals covered by this system include:

Individuals or entities involved in, suspected of being involved in, or who the Agency believes may become involved in criminal acts against the buildings, grounds, and property that are leased or occupied by the National Labor Relations Board, or against persons who are in or on such buildings, grounds, or property.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records in the system may include the following types of information about individuals:

- Individual's or entity's name;
- Alias;
- Digital video recordings and Closed Circuit Television (CCTV) recordings;
- Audio recordings;
- Date of birth, place of birth, and age;
- Social Security number;

- Alien File Number (A-Number);
- Duty/work address and telephone number;
- Race and ethnicity;
- Citizenship;
- Sex;
- Marital status;
- Identifying marks (e.g., tattoos, scars);
- Height and weight;
- Eye and hair color;
- Biometric data (e.g., photograph, fingerprints);
- Home address, telephone number, and other contact information;
- Driver's license information and citations issued;
- Vehicle information;
- Date, location, nature and details of the incident/offense;
- Alcohol, drugs, or weapons involvement;
- Bias against any particular group;
- Confinement information to include location of correctional facility;
- Gang/cult affiliation, if applicable;
- Release/parole/clemency eligibility dates;
- Foreign travel notices and reports including briefings and debriefings;
- Notices and reports with foreign contacts;
- Reports of investigation;
- Statements of individuals, affidavits, and correspondence;
- Documentation pertaining to criminal activities;
- Investigative surveys;
- Certifications pertaining to qualifications for employment, including but not limited to education, firearms, first aid, and CPR;
- Technical, forensic, polygraph, and other investigative support to criminal investigations to include source control documentation and regional information;
- Data on individuals to include victims, witnesses, complainants, offenders, and suspects;

- Records of possible espionage, foreign intelligence service elicitation activities, and terrorist collection efforts directed at the U.S. Government or its staff, contractors, or visitors;
- Records of close coordination with the intelligence and law enforcement community.

RECORD SOURCE CATEGORIES:

Records are obtained from sources contacted during investigations; NLRB employees; state, tribal, international, and local law enforcement; and federal departments and agencies.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b), all or a portion of the records or information contained in this system may be disclosed outside the NLRB as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

1. To the Department of Justice for use in litigation when either (a) the Agency or any component thereof, (b) any employee of the Agency in his or her official capacity, (c) any employee of the Agency in his or her individual capacity where the Department of Justice has agreed to represent the employee, or (d) the United States Government is a party to litigation or has an interest in such litigation, and the Agency determines that the records are both relevant and necessary to the litigation.

2. To a court or other adjudicative body before which the Agency is authorized to appear, when either (a) the Agency or any component thereof, (b) any employee of the Agency in his or her official capacity, (c) any employee of the Agency in his or her individual capacity, where the Agency has agreed to represent the employee, or (d) the United States Government is a party to litigation or has an interest in such litigation, and the Agency determines that the records are both relevant and necessary to the litigation.

3. To a Member of Congress or to a Congressional staff member in response to an inquiry of the Congressional office made at the written request of the constituent about whom the record is maintained. However, the investigative file, or parts thereof, will only be released to a Congressional office if the Agency receives a signed statement under 28 U.S.C. 1746 from the subject of the investigation.

4. To the National Archives and Records Administration (NARA) pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

5. To the National Archives and Records Administration, Office of Government Information Services (OGIS), to the extent necessary to fulfill its responsibilities in 5 U.S.C. 552(h), to review administrative agency policies, procedures and compliance with the Freedom of Information Act (FOIA), and to facilitate OGIS's offering of mediation services to resolve disputes between persons making FOIA requests and administrative agencies.

6. To appropriate agencies, entities, and persons when:

a. the National Labor Relations Board determines that the use of information from this system of records is reasonably necessary and otherwise compatible with the purpose of collection to assist another federal recipient agency or entity in (a) responding to a suspected or confirmed breach of private information, or (b) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security resulting from a suspected or confirmed breach; or

b. the National Labor Relations Board suspects or has confirmed there has been a breach of this system of records; and (a) the NLRB has determined that as a result of the suspected or confirmed breach, there is a risk of harm to individuals, harm to the NLRB (including its information systems, programs, and operations), the Federal Government, or national security; and (b) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the NLRB's

efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

7. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for NLRB, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to NLRB employees.

8. To an appropriate federal, state, tribal, or local law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations, and such disclosure is proper and consistent with the official duties of the person making the disclosure.

9. To a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations or in connection with criminal law proceedings or pursuant to the order of a court of competent jurisdiction.

10. To third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation, provided disclosure is appropriate to the proper performance of the official duties of the officer making the disclosure.

11. To a federal, state, local agency, or other appropriate entities or individuals, or through established liaison channels to selected foreign governments, in order to provide intelligence, counterintelligence, or other information for the purposes of intelligence, counterintelligence, or antiterrorism activities authorized by United States law, Executive Order, or other applicable national security directive.

12. To a public or professional licensing organization when such information indicates, either by itself or in combination with other information, a violation or potential violation of professional standards, or reflects on the moral, educational, or professional qualifications of an individual who is licensed or who is seeking to become licensed.

13. To individuals involved in incidents occurring on federal facilities, their insurance companies, and their attorneys for the purpose of adjudicating a claim, such as personal injury, traffic accident, or other damage to property. The release of personal information is limited to that required to adjudicate a claim.

14. To the news media and the public, with the approval of the Senior Agency Official for Privacy in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information, when disclosure is necessary to preserve confidence in the integrity of the NLRB, or when disclosure is necessary to demonstrate the accountability of the NLRB's employees or individuals covered by the system, except to the extent the Senior Agency Official for Privacy determines that release of the specific information in the context of a particular case would constitute a clearly unwarranted invasion of personal privacy.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records are maintained in paper format in file folders, on digital images, and in electronic databases. Any classified information is maintained in a storage container that meets classification requirements.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records may be retrieved by individual name or other personal identifier listed in "Categories of Records," when applicable.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are maintained in accordance with NARA General Records Schedule 5.6, Security Records, Item 010 Security Administrative Records, which generally requires destruction after three years, but which also permits longer retention as required for business use. Disposition Authority: DAA-GRS-2017-0006-0001.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Paper—Paper files are stored in a locked file cabinet or a secure facility with an intrusion alarm system at NLRB Headquarters in the Security Branch. Access is limited to security specialists and their duly authorized representatives who have a need to know the information for the performance of their official duties. The U.S. Postal Service and other postal providers are used to transmit hard copy records sent to and from field offices, other agencies, and designated individuals.

Electronic—Comprehensive electronic records are maintained in the Security Branch and on the NLRB network. Electronic records are maintained in computer databases in a secure room accessible only by a personal identity verification card reader which is limited to Office of Chief Information Officer designated employees. Information that is transmitted electronically from field offices is encrypted. Access to the records is restricted to security staff with a specific role in creating and maintaining the Banned Entry List.

NOTIFICATION PROCEDURES:

For records not exempted under 5 U.S.C. 552a(k)(1), (2), and (5), an individual may inquire as to whether this system contains a record pertaining to such individual by sending a request in writing, signed, to the System Manager at the address above, in accordance with the procedures set forth in 29 CFR 102.119(a).

An individual requesting notification of records in person must provide identity documents sufficient to satisfy the custodian of the records that the requester is entitled to such notification, such as a government-issued photo ID. Individuals

requesting notification via mail must furnish, at minimum, name, date of birth, and home address in order to establish identity.

RECORD ACCESS PROCEDURES:

For records not exempted under 5 U.S.C. 552a(k)(1), (2), and (5), an individual seeking to gain access to records in this system pertaining to him or her should contact the System Manager at the address above, in accordance with the procedures set forth in 29 CFR 102.119(b) and (c).

An individual requesting access in person must provide identity documents sufficient to satisfy the custodian of the records that the requester is entitled to such access, such as a government-issued photo ID. Individuals requesting access via mail must furnish, at minimum, name, date of birth, and home address in order to establish identity. Requesters should also reasonably specify the record contents being sought. Investigative information created by other agencies remains the property of those agencies and requests regarding such material must be directed to them.

CONTESTING RECORD PROCEDURES:

For records not exempted under 5 U.S.C. 552a(k)(1), (2), and (5), an individual may request amendment of a record pertaining to such individual maintained in this system by directing a request to the System Manager at the address above, in accordance with the procedures set forth in 29 CFR 102.119(d).

An individual seeking to contest records in person must provide identity documents sufficient to satisfy the custodian of the records that the requester is entitled to contest such records, such as a government-issued photo ID. Individuals seeking to contest records via mail must furnish, at minimum, name, date of birth, and home address in order to establish identity. Requesters should also reasonably identify the record, specify the information they are contesting, state the corrective action sought and the reasons for the correction along with supporting justification showing why the record is not accurate, timely, relevant, or complete. Investigative information created

by other agencies remains the property of those agencies and requests regarding such material must be directed to them.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

Pursuant to 5 U.S.C. 552a(k)(1), (2), and (5), the Agency has exempted portions of this system that relate to providing an accounting of disclosures to the data subject, and access to and amendment of records (5 U.S.C. 552a(c)(3),(d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f)). This system may contain the following types of information:

1. Properly classified information subject to the provisions of section 552(b)(1), which describes matters that are: (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) in fact properly classified pursuant to such Executive order.

2. Investigatory material compiled for law enforcement purposes, other than material within the scope of 5 U.S.C. 552a(j)(2): provided, however, that if any individual is denied any right, privilege, or benefit to which he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence.

3. Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment and Federal contracts or access to classified information. Materials may be exempted to the extent that release of the material to the individual whom the information is about would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to

September 27, 1975, furnished information to the Government under an implied promise that the identity of the source would be held in confidence.

When this system receives a record from another system exempted in that source system under 5 U.S.C. 552a(j)(2), the NLRB will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claim any additional exemptions set forth here.

HISTORY:

None.

Dated:
Washington, DC
By direction of the Board
Roxanne Rothschild, Executive Secretary
National Labor Relations Board