National Labor Relations Board
Security Branch

Personnel Security Case Management System (PSCMS)
Privacy Impact
Assessment
Prepared: April 2026

The Office of the Chief Information Officer

Introduction:

This Privacy Impact Assessment (PIA) is necessary for Personnel Security Case Management System (PSCMS). 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: PSCMS is a case management system that records when the Security Branch initiates, receives, stores, and adjudicates background information. Additionally, the PSCMS facilitates the eDelivery and management/tracking of background checks performed on employees, contractors, interns and volunteers by the NLRB Security Branch in conjunction with the Department of Defense Defense Counterintelligence and Security Agency. Information is entered into the system manually as well as importing files from eDelivery.

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. PSCMS 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?

- **Executive Order 10450** – Security Requirements for Government Employment
- **Executive Order 10865** – Safeguarding Classified Information within Industry
- **Executive Order 12333 (amended)** – United States Intelligence Activities

- **Executive Order 12356** – National Security Information
- **Title 5 U.S.C. § 3301** – Civil Service—Generally
- **Title 5 U.S.C. § 9101** – Access to Criminal History Records for National Security and Other Purposes
- **Title 5 U.S.C. Parts 1400** – National Security Positions
- **Title 5 U.S.C. Parts 736** – Personnel Investigations
- **Title 42 U.S.C. § 2165** – Security Restrictions
- **Title 42 U.S.C. § 2201** – General Duties of Commission
- **Title 50 U.S.C. §§ 781–858** – Internal Security
- **Title 50 U.S.C. §§ 881–887** – National Defense Facilities

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-17 Personnel Security Files

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

- PSCMS 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 181, Personnel Security Clearance Files, Index to the Personnel Security Case Files. Destroy with related case file.

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

3 Characterization of the Information:

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

- PSCMS stores, uses, disseminates, and maintains personally identifiable information and background investigation data for NLRB employees, contractors, interns, and volunteers. This includes identity data (such as name, date/place of birth, SSN, address, contact information), background investigation forms and reports from OPM and other agencies (including criminal, financial, employment, and education history), suitability and clearance adjudication records, case processing milestones, and security-related documentation. PSCMS maintains this information to support the personnel security

process, clearance determinations, reinvestigations, and documentation of security actions.

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

- Information in PSCMS is collected from individuals undergoing personnel security investigations; from OPM and other federal investigative bodies such as the FBI, DHS, and DoD; and from internal NLRB Security Branch adjudication activities. Data is collected through electronic eDelivery from OPM, secure transfers from partner agencies, standard federal background investigation forms (SF-85/85P/86/87), and manual data entry by NLRB Security Branch staff.

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

- No

3.4 Discuss how accuracy of the data is ensured.

- PSCMS ensures the accuracy of personnel security data by relying on authoritative investigative sources such as OPM and other federal agencies; using standardized federal forms that require legal attestation; conducting Security Branch review and adjudication checks; enforcing role-based data entry controls; applying privacy compliance oversight; and maintaining audit trails to monitor data integrity.

3.5 Privacy Impact Analysis: Related to Characterization of the Information

3.5.1 Privacy Risk: None.

3.5.2 Mitigation: None.

4 Uses of the Information

4.1 Describe how and why the project uses the information.

- The Personnel Security Case Management System (PSCMS) uses the information it stores to facilitate the secure processing, tracking, and adjudication of background investigations for NLRB employees, contractors, interns, and volunteers. It enables the Security Branch to receive electronic investigation data from the U.S. Office of Personnel Management (OPM), record case milestones, and manage suitability and clearance determinations in a consistent and efficient manner. By centralizing personnel-security information, PSCMS ensures accurate vetting, supports decisions related to access to

facilities and systems, and maintains an authoritative repository of investigation and adjudication records necessary for safeguarding agency operations.

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.

- N/A

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

- Yes. Several NLRB components have defined roles and responsibilities within PSCMS. The primary users are members of the NLRB Security Branch, who manage personnel security investigations, adjudications, and case processing. The Office of the Chief Information Officer (OCIO) supports system administration, maintenance, and security functions, while Information Assurance (IA) personnel oversee compliance, auditing, and continuous monitoring activities. Additionally, authorized NLRB program offices may interact with PSCMS information as part of onboarding, suitability, or access-management workflows, but only within the scope of their assigned duties and access privileges.

4.4 Privacy Impact Analysis: Related to the Uses of Information

4.4.1 Privacy Risk: None.

4.4.2 Mitigation: None.

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.

- Yes, Privacy Act Statement is provided.

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

- Individuals undergoing personnel security vetting for employment, contracting, or internship positions with the NLRB do not have the ability to opt out of providing the information required for a background investigation, as this information is mandated under federal personnel-security laws and suitability requirements. The information collected and used within PSCMS is necessary to determine eligibility for federal service, access to facilities, and issuance of credentials. Individuals provide implicit consent when

completing required security forms such as the SF-85, SF-85P, SF-86, or SF-87, which include federally mandated Privacy Act notices outlining the purpose and use of the information. However, individuals may decline to provide certain information, understanding that doing so may delay or prevent completion of the background investigation and may disqualify them from employment or continued access.

5.3 Privacy Impact Analysis: Related to Notice

5.3.1 Privacy Risk: None.

5.3.2 Mitigation: None.

6 Data Retention by the Project

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

- Destroy five (5) years after employee or contractor relationship ends, but longer retention is authorized if required for business use.

6.2 Is the record retention compatible with any applicable SORN? (See Question 2.2, "*What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?*")

- NLRB-17 Personnel Security Files

6.3 Privacy Impact Analysis: Related to Retention

6.3.1 Privacy Risk None.

6.3.2 Mitigation: None.

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.

- Yes. As part of normal agency operations, the NLRB Security Branch shares information with the Department of Defense Counterintelligence and Security Agency along with the Office of Personnel Management, which conducts and manages federal background investigations. PSCMS transmits and receives investigation records through OPM's secure electronic systems to facilitate personnel vetting, case updates, and adjudication activities. Additionally, information may be shared with other authorized federal investigative or security agencies, as required under federal personnel-security regulations, to validate criminal history, verify identity, or support security-clearance

determinations. These external organizations access the information through secure, encrypted channels and use it solely for the purpose of conducting background investigations, performing suitability assessments, verifying credentials, and ensuring individuals meet federal security requirements necessary for employment or access to government systems and facilities.

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 described in Section 7.1 is fully compatible with the system's applicable System of Records Notice (SORN), NLRB-17 Personnel Security Files, which governs the maintenance and disclosure of personnel-security related records. The SORN explicitly authorizes sharing personnel security information with other federal agencies including the U.S. Office of Personnel Management (OPM) and other investigative or adjudicative bodies—for purposes such as evaluating suitability, verifying identity and credentials, and conducting background investigations. PSCMS sends and receives information through secure channels and uses that information strictly for authorized personnel-security purposes, these activities fall squarely within the SORN's permitted "routine uses," which allow disclosures to other agencies with a need to evaluate qualifications, determine eligibility for access, or support lawful investigations. The system's sharing practices therefore align directly with the disclosures and purposes outlined in NLRB-17, ensuring full Privacy Act compatibility.

7.3 Does the project place limitations on re-dissemination?

- Yes. PSCMS places explicit limitations on the re-dissemination of information shared with external agencies. Any information disclosed outside the NLRB Security Branch such as to the Department of Defense Counterintelligence and Security Agency, U.S. Office of Personnel Management (OPM) or other authorized federal investigative bodies is shared solely for the purposes permitted under the applicable SORN (NLRB-17) and only within the scope necessary to conduct personnel security investigations and suitability determinations. Receiving agencies are required to handle the information in accordance with the Privacy Act and may not further disseminate it unless authorized by law, regulation, or a published routine use. PSCMS also transmits information through secure channels and limits disclosures to only those entities with a demonstrated investigatory or adjudicative need, ensuring that all re-dissemination is controlled, lawful, and consistent with federal privacy requirements.

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

- PSCMS maintains a record of disclosures outside the agency through audit logging and controlled access mechanisms built into the system and overseen by the NLRB Security Branch and OCIO. Any transmission of personnel-security information to external entities such as the U.S. Office of Personnel Management (OPM) is conducted through secure, encrypted channels.

7.5 Privacy Impact Analysis: Related to Information Sharing

7.5.1 Privacy Risk: None.

7.5.2 Mitigation: None.

8 Redress

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

Individuals may access their personnel-security information maintained in PSCMS by submitting a Privacy Act request.

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

Individuals may request correction of inaccurate or erroneous personnel-security information contained in PSCMS by submitting a formal amendment request under the Privacy Act.

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

PSCMS notifies individuals of the procedures for correcting their information through the Privacy Act Statements. On all OPM related federal background investigation forms such as the SF-85, SF-85P, SF-86, and SF-87 explain individuals' rights to access and amend their records, as well as the process for doing so.

8.4 Privacy Impact Analysis: Related to Redress

8.4.1 Privacy Risk: None.

8.4.2 Mitigation: None.

9 Auditing and Accountability

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

- Role-based access controls restrict users to only the information needed for their specific duties, and all system activity is subject to continuous monitoring and audit logging to detect unauthorized or improper use. PSCMS adheres to NLRB's IT security/privacy policy, ensuring that handling, storage, sharing, and retention of personnel security information is consistent with the uses described in this PIA.

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

- All PSCMS users are required to complete the NLRB's mandatory annual privacy and security training, which covers the proper handling of personally identifiable information (PII), Privacy Act obligations, secure data access practices, incident reporting procedures, and rules governing authorized use of federal information systems. In addition to this agency-wide training, personnel within the NLRB Security Branch and OCIO Information Assurance receive role-specific instruction on safeguarding sensitive background-investigation data, applying least-privilege principles, and complying with the procedures outlined in the PSCMS PIA and privacy compliance framework. These training requirements ensure all PSCMS users understand their responsibilities for protecting the sensitive personnel-security information they access.

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

- PSCMS determines which users may access personnel-security information through formal account provisioning and access-control procedures established by the NLRB Security Branch and OCIO Information Assurance. Access is granted only after a validated access authorization request, documented approval by system owners or designated account managers, and verification that the user's job duties require access to PSCMS in accordance with the principle of least privilege. The NLRB Annual Privileged User Account Management Process and Procedure document outlines how PSCMS accounts are created, modified, reviewed, and disabled, including requirements for role assignment and recertification. The AC-1 Information Security Access Control Policy further requires that authorized users, role memberships, and privileges be explicitly documented, approved, and periodically reviewed to ensure continued need-to-know. It also mandates monitoring of account usage, immediate notification and removal of access when roles change, and alignment of PSCMS account management with personnel onboarding, transfer, and separation processes.

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?

- PSCMS follows a formal governance and review process coordinated by the NLRB Security Branch and OCIO to ensure that any proposed sharing of personnel-security information is lawful, necessary, and consistent with the uses described in the PSCMS PIA and the NLRB-17 SORN.

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

9.4.1 Privacy Risk: None.

9.4.2 Mitigation: None.

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-17 Personnel Security Files currently applies.

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 07:26:48 -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 14:09:34 -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 12:18:31 -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 11:30:47 -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 09:18:48 -04'00'