



NATIONAL MEDIATION BOARD

APPLICATIONS

Version: 2.2

System Acronym: NMB APPS

Document Title: Privacy Impact Assessment (PIA)

Date: 10/15/2026

Prepared by: Softthink Solution Inc.

DISTRIBUTION IS LIMITED TO AUTHORIZED U.S. GOVERNMENT AGENCIES AND THEIR CONTRACTORS. OTHER REQUESTS FOR THIS DOCUMENT MUST BE REFERRED TO: NMB CHIEF INFORMATION OFFICER OR OTHER AUTHORIZED NMB PERSONNEL

Document Change History

The following table is used to annotate changes to the NMB APPS Privacy Impact Assessment (PIA) document.

Table 1: Document Change History

Document Version	Change Description	Change POC	Change Date
1.0	Initial Document	Kareem Adham	06/18/2020
2.0	Update to include changes to NMB APPS ATO Boundary	Nathan Jones	02/01/2023
2.1	Minor Updates and removal of ZoomGov from the ATO Boundary.	Chris Lambeth	3/23/2026
2.2	Updated SAOP and minor updates.	Chris Lambeth	10/9/2026

Document Review History

The following table is used to annotate any reviews of the NMB APPS Privacy Impact Assessment (PIA) document.

Table 2: Document Review History

Document Version	Change Description	Change POC	Position	Change Date
1.0	Initial Review	Kareem Adham	ISSO	06/18/2020
2.0	Review to ensure changes to NMB APPS ATO boundary are incorporated	Nathan Jones	ISSO	02/01/2023
2.1	Reviewed document to ensure accurate and updated ATO boundary.	Chris Lambeth	ISSO	3/23/2026
2.2	Reviewed document to ensure accurate and updated ATO boundary.	Chris Lambeth	ISSO	10/9/2026

FOR OFFICIAL USE ONLY

System Acronym: NMB APPS

Document Title: Privacy Impact Assessment (PIA)

10/9/2026

APPROVAL PAGE

This document must be signed by the System Owner or designated appointee to be considered authoritative. This document can be signed physically (wet signature) or digitally using PKI enabled digital signature (non-repudiation).

Taha Sadeghi

NMB System Owner / Senior Agency Official for Privacy

Table of Contents

Document Change History	2
<i>Table 1: Document Change History</i>	2
Document Review History	3
<i>Table 2: Document Review History</i>	3
APPROVAL PAGE	4
Table of Contents	5
References	7
1. Introduction	1
2. Overview	1
2.1 NMB Organizational Background	1
2.1.1 NMB Organizational Structure	1
2.2 NMB APPS System Description	2
2.3 NMB APPS PII Collection and Uses	2
2.3.1 C.2 Rationale and Factors for Services Delivery Support Information	3
2.3.2 C.3 Rationale and Factors for Government Resource Management Information	3
2.3.3 D.11 Transportation	3
2.3.4 D.13 Work Force	3
2.4 NMB Organizational Usage of PII	3
<i>Table 3: Typical NMB Organizational NMB APPS Usage of PII</i>	3
2.5 NMB APPS PII Protections	4
<i>Table 4: Critical PII Protection Controls</i>	4
3. Legal Authority to Process PII	5
4. NMB APPS System of Record Notice (SORN) Requirement	5
5 NMB APPS System Security Plan (SSP)	5
6 Privacy Impact Analysis of Characterization of Information	6
7 Individual Opportunities to Consent to Use or Decline Use of PII	6
8 Retention of Collected PII	6
NMB APPS ISSO PII Program Recommendations	6

List of Tables

FOR OFFICIAL USE ONLY

System Acronym: NMB APPS

Document Title: Privacy Impact Assessment (PIA)

10/9/2026

<u>Table 1: Document Change History</u>	1
<u>Table 2: Document Review History</u>	2
<u>Table 3: Typical NMB Organizational NMB APPS Usage of PII</u>	3
<u>Table 4: Critical PII Protection Controls</u>	4

References

The following reference material was used in the development of this document:

- a) **NIST SP 800-30 Revision 1**, *“Risk Management Guide for Information Technology Systems”*
- b) **NIST SP 800-37 Revision 2**, *“Risk Management Framework for Information Systems and Organizations”*
- c) **NIST SP 800-53 Revision 5**, *“Security and Privacy Controls for Federal Information Systems and Organizations”*
- d) **NIST SP 800-60 Volume II Revision 1**, *“Guide for Mapping Types of Information and Information Systems to Security Categories”*
- e) **NIST SP 800-60 Volume II Revision 1**, *“Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories”*
- f) **NIST SP 800-122**, *“Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)”*
- g) **NIST SP 800-144**, *“Guidelines on Security and Privacy in Public Cloud Computing”*
- h) **NISTIR 8062**, *“An Introduction to Privacy Engineering and Risk Management in Federal Systems”*
- i) **5 U.S.C. § 552, Freedom of Information Act of 1996**, As Amended by Public Law No. 104-231, 110 Stat. 3048
- j) **5 U.S.C. § 552a, Privacy Act of 1974**, As Amended
- k) **Public Law 100-503, Computer Matching and Privacy Act of 1988**
- l) **E-Government Act of 2002 § 208**
- m) **Federal Trade Commission Act § 5**
- n) **44 U.S.C. Federal Records Act**, Chapters 21, 29, 31, 33
- o) **Title 35, Code of Federal Regulations, Chapter XII, Subchapter B**
- p) **OMB Circular A-130**, *“Management of Federal Information Resources”*, Updated in 2016
- q) **OMB Memo M-10-23**, *“Guidance for Agency Use of Third-Party Websites”*
- r) **OMB Memo M-17-12**, *“Preparing and Responding to a Breach of Personally Identifiable Information”*
- s) **The Health Insurance Portability and Accountability Act of 1996 (HIPAA)**
- t) **NMB Policy # 8200**, *“Privacy Policy”*, 2017
- u) **NIST SP 800-70 Revision 5**, *“National Checklist Program for IT Products—Guidelines for Checklist Users and Developers”*

1. Introduction

The National Mediation Board (NMB) is completing this Privacy Impact Assessment (PIA) for NMB Applications (NMB APPS). The NMB APPS Major Application provides critical Information Technology (IT) infrastructure/capabilities to the organization. The Privacy Threshold Analysis (PTA) indicated that the NMB APPS Major Application is a “Privacy Sensitive System”.

2. Overview

This PIA is designed to demonstrate NMB’s structured processes for identifying and mitigating privacy risks to the NMB APPS Major Application. Special consideration was given to the confidentiality of the information and major application along with its subsystems in the development of the PIA. The NMB APPS PIA is designed to achieve the following objectives throughout the system’s lifecycle:

- a. Ensure the NMB APP’s handling of PII information conforms to all applicable legal, regulatory, and policy requirements
- b. Determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic (IS)
- c. Identify and evaluate protections and alternative processes for handling information to mitigate potential privacy risks

2.1 NMB Organizational Background

NMB was established by the Railway Labor Act of 1926, as an independent U.S. Federal government agency. NMB’s mission is to facilitate labor management relations within the nation’s railroad and airline industries by providing dispute resolution processes for the railroad and airline industries.

2.1.1 NMB Organizational Structure

The NMB organizational structure has three sections: **NMB Board Members**, **NMB Mission Areas**, and **NMB Mission Support Areas**.

- **NMB Board Members:** Are directly responsible for the strategic, operational, and managerial oversight of the Designated Agency Ethics Official (DAEO), Ombudsmen (OMB), and Designated EEO Official (DEEOO). The NMB Mission and Mission Support Areas report to the NMB Board Members. NMB Board Members are not typically given administrator access to NMB Mission and Mission Support files, work products, or IT assets.
- **NMB Mission Area Personnel:** Are directly responsible for the strategic, operational, and managerial oversight of the Office of Legal Affairs (OLA), Office of Mediation Services (OMS), and Office of Arbitration Services (OAS). The NMB Mission Area

personnel are not typically given administrator access to NMB Board Members or Mission Support files, work products, or IT assets.

- **NMB Mission Support Area Personnel:** Are directly responsible for strategic, operational, and managerial oversight of the Office of Administration (OA), Office of Fiscal Services (OFS), and Office of Information Services (OIS). The NMB Mission Support Area personnel are not typically given administrator access to NMB Board Members or Mission Area files, work products, or IT assets, with exception of OIS personnel. The OIS personnel that are assigned as administrators are typically given rights to access IT assets from the NMB Board Members, Mission Area, and Mission Support Areas.

2.2 NMB APPS System Description

NMB APPS Major Application provides personnel with the IT infrastructure/capabilities to perform their assigned tasks. The NMB APPS Major Application comprises the following six subsystems: **NMB.gov**, **AWS** (Arbitration Workspace), **MCMS** (Mediation Case Management System), **KnowledgeStore**, **KnowBe4**, and **GitHub**. The subsystems act in concert to provide NMB personnel with the following IT capabilities:

- Access to all publicly available agency data, rules, railway and airline acts, information on representation, arbitration, notices, case load information, outcome of cases.
- Create cases, submit bills, schedule arbitration cases, set up new cases and future cases
- Data storage and retrieval
- Data receiving and transfer
- File repository
- Access to application resources via the Internet
- Sending out bulk emails on a predetermined time schedule
- Performing search functions of NMB documents from a repository of information
- Employee security awareness training
- Document version and source code management

2.3 NMB APPS PII Collection and Uses

NMB APPS Major Application typically collects and utilizes Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (S-PII) during the execution of mission related tasks utilizing information types that fall under the C.2 Rationale and Factors for Services Delivery Support Information, C.3 Rationale and Factors for Government Resource Management Information, C.5 Information and Technology Management Rationale, D.11 Transportation, and D.13 Workforce Management, which are described in NIST SP 800-60 Volume II Revision 1 “Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories”, as follows:

2.3.1 C.2 Rationale and Factors for Services Delivery Support Information

“Resource management functions are the back-office support activities that enable the government to operate effectively. Security objectives and impacts for resource management functions are determined by the direct service missions and constituencies ultimately being supported. It is likely that all Federal government information systems store, process, and operate under the control of IT infrastructure maintenance information (e.g., password files and file and network access settings). A basic set of security controls will apply to this information and processes to combat potential corruption, misuse, or abuse of system information and processes.”

2.3.2 C.3 Rationale and Factors for Government Resource Management Information

“IT management involves the coordination of IT resources and systems required to support or enable a citizen service. Impacts to information associated with the operation of IT systems generally need to be considered even when all mission-related information processed by the system is intended to be available to the general public. The relevant issues may be different for integrity and availability than for confidentiality. Information that has been made public, by definition, requires no confidentiality protection. In contrast, integrity and availability protection cannot be maintained for copies of information that have been distributed to the public. Integrity and availability assurance can only be maintained by maintaining copies of information in organization-controlled information systems.”

2.3.3 D.11 Transportation

“Transportation involves all federally supported activities related to the safe passage, conveyance, or transportation of goods and/or people. Note that impacts to some information and many information systems associated with transportation activities may affect the security of, not only the transportation infrastructure, but also to a broad range of other critical infrastructures and key national assets.”

2.3.4 D.13 Work Force

“Workforce Management includes those activities that promote the welfare and effectiveness of the Nation’s workforce by improving their proficiency, working conditions, advancing opportunities for profitable employment, and strengthening free collective bargaining.”

2.4 NMB Organizational Usage of PII

The following table highlights the typical organization usage of PII for each subsystem in the NMB APPS Major Application.

Table 3: Typical NMB Organizational NMB APPS Usage of PII

NMB APPS Subsystem	Information Types Utilized	Typical PII Usage
NMB.gov	D.11.1 Ground Transportation, D.11.3 Air Transportation, D.13.2 Labor Rights Management, C.2.6.1 Customer Services, C.2.6.2 Official Information Dissemination, C.3.5.6 Record Retention Information Type	PII is displayed in the Arbitrator resumes. However, this information is intended to be public.
AWS (Arbitration Workspace)	D.11.1 Ground Transportation, D.11.3 Air Transportation, D.13.2 Labor Rights Management, C.2.6.1 Customer Services, C.3.5.6 Record Retention Information Type	PII is in the form of arbitrator information incidentally stored in

FOR OFFICIAL USE ONLY

System Acronym: NMB APPS

Document Title: Privacy Impact Assessment (PIA)

10/9/2026

		contact information of files.
MCMS (Mediation Case Management System)	D.11.1 Ground Transportation, D.11.3 Air Transportation, D.13.2 Labor Rights Management, C.2.6.1 Customer Services, C.3.5.6 Record Retention Information Type	PII can have mediation case participants names and contact information.
Knowledge Store	D.13.2 Labor Rights Management, C.3.5.6 Record Retention, D.11.1 Ground Transportation, D.11.3 Air Transportation	PII can have some individual's contact information incidentally included in file notes.
KnowBe4	C.3.5.6 Record Retention	PII is collected to verify users and document completed security, section 508 and privacy training.
GitHub	C.3.5.6 Record Retention, C.3.5.4 IT Infrastructure Maintenance Information Type	No PII is maintained or intended to be maintained in GitHub.

2.5 NMB APPS PII Protections

The NMB APPS Major Application has been developed with an emphasis placed on the protection of PII and S-PII information. NMB APPS Major Application System Security Plan (SSP) incorporates the guidelines for the implementation of the Risk Management Framework (RMF) Assessment and Authorization (A&A) process as outlined in NIST SP 800-37 Revision 2 *“Risk Management Framework for Information Systems and Organizations”*. NMB APPS incorporates the appropriate baseline security controls to protect the confidentiality, integrity, and availability (CIA) of the system. NMB APPS utilizes “Low” level baseline security controls, as outlined in the NIST SP 800-53 Revision 5, *“Security and Privacy Controls for Federal Information Systems and Organizations”*.

NMB is committed to protecting the PII information contained in the NMB APPS Major Application by emphasizing the following security controls listed in **Table 2: Critical PII Protection Controls**.

Table 4: Critical PII Protection Controls

Control Description	Control Description Objective
Technical Controls	
Multifactor Authentication	Admins must use Multifactor 2FA enabled for authentication.
Encryption	Data used in the NMB applications are encrypted in transit and stored at rest.
Unique Admin User ID	Each admin account will have its unique log-in ID to aid in tracking system configuration changes.

FOR OFFICIAL USE ONLY

System Acronym: NMB APPS

Document Title: Privacy Impact Assessment (PIA)

10/9/2026

Admin Activity Logs Generated	All admin changes to NMB applications are generated and captured in the system audit logs.
Administrative Controls	
Periodic Security Audits	The NMB ISSO and SCA will make annual security audits/assessments for each NMB system with authority to operate (ATO).
Rules of Behavior	Each NMB employee has to read and accept the NMB Rules of Behavior to ensure they familiarize themselves with information security and privacy best practices
Role-Based Admin Training	Each NMB Admin is required to take annual role-based training to keep current with information security and privacy best practices
Annual Mandatory Security and Privacy Training	Each NMB IT user, must take annual security awareness training to keep current with information security and privacy best practices.
Weekly Review of Admin Audit Logs	The NMB ISSO reviews admin/privilege user audit logs weekly to identify malicious anomalies or abuse of privilege by system administrators.

3. Legal Authority to Process PII

NMB is authorized to collect PII based on the following statute:

- **Privacy Act of 1974:** Allows for the collection of information about a U.S. Citizen that aligns with the mission objectives of federal agencies. NMB collects information about personnel relevant to employment, performance reviews, arbitrations, and other mission related tasks.

4. NMB APPS System of Record Notice (SORN) Requirement

The NMB APPS Major Application is **NOT** required to have a SORN. An information system is required to have a SORN, if it meets all the criteria listed below.

- Records maintained by a federal agency.
- Records contain information about an individual.
- Records are retrieved by a personal identifier.

NMB APPS Major Application is not considered a system of record (SOR) because the individual PII information is not grouped together nor is it retrieved by a personal identifier.

5 NMB APPS System Security Plan (SSP)

The NMB APPS SSP has been developed in-accordance-with (IAW) the Risk Management Framework process.

6 Privacy Impact Analysis of Characterization of Information

Primary risks for the NMB APPS Major Application as it relates to the characterization of information are a data breach of the NMB APPS subsystems and malicious (intentional or unintentional) activity from NMB personnel.

The collected PII and S-PII is stored primarily on a third-party cloud system (G-Suite/GCP). Subsequently, NMB APPS Major Application relies on the performance of Google administrators to properly implement the appropriate information security controls and disclose breaches to NMB. NMB OIS has to ensure that the applications that are utilized remain hardened against attacks by ensuring secure software engineering practices are maintained throughout the lifecycle of the application. Particular attention should be paid to those applications whose security is managed by a third-party such as KnowBe4, and any subsequently added applications.

Malicious (intentional or unintentional) activity from NMB personnel could compromise PII information. Proper implementation of least privilege principles, separation of duties, proper account management practices, and user training are used to reduce the risk of PII/S-PII being compromised through this threat vector.

7 Individual Opportunities to Consent to Use or Decline Use of PII

Individuals have the right to decline usage of their PII in NMB operations, but it will restrict their ability to gain or maintain employment at NMB. Individuals are notified that the information they are providing is subject to applicable statutes regarding PII and how the information will be used. NMB documentation that uses PII is marked and/or labeled with the appropriate statute (i.e. Privacy Act statement).

8 Retention of Collected PII

Formally requested and/or provided PII from individuals are retained according to the NMB's Director of OA records management program.

NMB APPS ISSO PII Program Recommendations

- Utilize enhanced privacy controls as outlined in NIST SP 800-53 Revision 5, "*Security and Privacy Controls for Federal Information Systems and Organizations*"
- Conduct annual privacy control reviews to help ensure effectiveness of implemented privacy controls
- Continue to conduct annual privacy trainers for standard users and administrators
- Monitor the cloud provider's implementation of privacy controls
- Continue to make improvements to NMB APPS access controls processes