



NATIONAL MEDIATION BOARD GENERAL SUPPORT SYSTEM

Version: 2.4
System Acronym: NMB GSS
Document Title: Privacy Impact Assessment
(PIA) Date: 10/9/2026

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**

FOR OFFICIAL USE ONLY

Document Change History

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

Table 1: Document Change History

Document Version	Change Description	Change POC	Change Date
1.0	Initial Document	Kareem Adham	5/25/2020
1.1	Removed Prey Subsystem from document	Kareem Adham	9/18/2020
2.0	Update to reflect the changes in the NMB GSS ATO boundary	Nathan Jones	2/23/2023
2.1	Update to include addition of BeyondTrust	Patrick Manley	07/03/2025
2.2	Update to include addition of MobileIron	Solomon Gebretensai	08/14/2025
2.3	Update to include addition of FedRAMP version of Webex and Cisco Meraki	Chris Lambeth	07/09/2026
2.4	Removed PACS and minor reference updates.	Chris Lambeth	10/9/2026

Document Review History

The following table is used to annotate any reviews of the NMB GSS 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	5/25/2020
2.0	Review to ensure changes to the NMB GSS ATO boundary are incorporated	Nathan Jones	Acting ISSO	2/08/2023
2.1	Review	Patrick Manley	ISSO	07/03/2025
2.2	Review	Solomon Gebretensai	Acting ISSO	08/14/2025
2.3	Review	Chris Lambeth	ISSO	07/09/2026
2.4	Review	Chris Lambeth	ISSO	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

$$\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \frac{1}{6}, \frac{1}{7}, \frac{1}{8}, \frac{1}{9}, \frac{1}{10}, \frac{1}{11}, \frac{1}{12}, \frac{1}{13}, \frac{1}{14}, \frac{1}{15}, \frac{1}{16}, \frac{1}{17}, \frac{1}{18}, \frac{1}{19}, \frac{1}{20}$$

FOR OFFICIAL USE ONLY

Table of Contents

Document Change History	1
Table 1: Document Change History	1
Document Review History	2
Table 2: Document Review History	2
APPROVAL PAGE	3
References	5
1. Introduction	6
2. Overview	6
2.1 NMB Organizational Background	6
2.1.1 NMB Organizational Structure	6
2.2 NMB GSS System Description	7
2.3 NMB GSS PII Collection and Uses	7
2.3.1 C.2 Rationale and Factors for Services Delivery Support Information	8
2.3.3 D.13 Workforce Management	8
2.3.4 D.20 Knowledge Creation and Management	8
2.4 NMB Organizational Usage of PII	8
Table 3: Typical NMB Organizational NMB GSS Usage of PII	8
2.5 NMB GSS PII Protections	10
Table 4: Critical PII Protection Controls	10
3. Legal Authority to Process PII	11
4. NMB GSS System of Record Notice (SORN) Requirement	12
5. NMB GSS System Security Plan (SSP)	12
6. NMB GSS Characterization of Information	12
Table 5: NMB GSS Collected PII Information	12
7. Privacy Impact Analysis of Characterization of Information	13
8. Individual Opportunities to Consent to Use or Decline Use of PII	13
9. Retention of Collected PII	13
10. NMB GSS ISSO PII Program Recommendations	13

References

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

- a) **NIST SP 800-30 Revision 1**, “Guide for Conducting Risk Assessments”
- 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 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 1974**, 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 Protection 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 36, Code of Federal Regulations**, Chapter XII, Subchapter B
- p) **OMB Circular A-130**, “Managing Information as a Strategic Resource”, 2016
- q) **OMB Memo M-10-23**, “Guidance for Agency Use of Third-Party Websites and Applications”
- r) **OMB Memo M-99-18**, “Privacy Policies on Federal Web Sites”
- s) **OMB Memo M-03-22**, “OMB Guidance for Implementing the Privacy Provisions”
- t) **OMB Memo M-17-12**, “Preparing for and Responding to a Breach of Personally Identifiable Information”
- u) **The Health Insurance Portability and Accountability Act of 1996 (HIPAA)**
- v) **NMB Policy # 8200**, “Privacy Policy”, 2017
- w) **NIST SP 800-70 Revision 4**, “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 the NMB General Support System (NMB GSS). The NMB GSS provides critical Information Technology (IT) infrastructure/capabilities to the organization. The Privacy Threshold Assessment (PTA) indicated that the NMB GSS 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 GSS. Special consideration was given to the confidentiality of the information and information system in the development of the PIA. The NMB GSS PIA is designed to ensure the GSS will meet the following objectives throughout the system’s lifecycle:

- a. Ensure the GSS and its subsystems that process PII fully comply with all applicable legal, regulatory, and policy requirements.
- b. Determine the risks and impacts of collecting, maintaining, and disseminating information in an identifiable form in the GSS and its subsystems.
- 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 GSS System Description

The NMB GSS and its subsystems provide NMB personnel with the IT infrastructure/capabilities to perform their assigned tasks. The NMB GSS is comprised of the following nine (9) subsystems: G-Suite/GCP, Zscaler, Qualys, Endpoints, Duo, BeyondTrust, MobileIron, Webex, and Cisco Meraki. The subsystems act in concert to provide NMB personnel with the following IT capabilities:

- Data storage and retrieval
- Data receiving and transfer
- File repository
- Local Network and Internet access
- Telecommunications services
- E-mail services
- Vulnerability management solution including configuration and patch management
- Document creation, modification, and deletion
- Network printer services
- Remote support services
- Privileged remote access services
- Endpoint management services

2.3 NMB GSS PII Collection and Uses

NMB GSS 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, D.13 Workforce Management, and D.20 Knowledge Creation and 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

*“Services delivery support functions provide the critical policy, programmatic, and managerial foundation to support Federal government operations. Security objectives and impact levels for service delivery support information and systems are generally determined by the natures of the supported direct services and constituencies being supported. If a system stores, processes, or communicates national security information, it is defined as national security system, and is outside the scope of this guideline.”*C.3 Rationale and Factors for Government Resource Management Information

“Resource management functions are the back-office support activities that enable the government to operate effectively. Security objectives and impact 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.”

2.3.3 D.13 Workforce Management

“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.”

2.3.4 D.20 Knowledge Creation and Management

“Knowledge Creation and Management involves the programs and activities in which the Federal Government creates or develops a body or set of knowledge, the manipulation and analysis of which can provide inherent benefits for both the Federal and private sector.”

2.4 NMB Organizational Usage of PII

The following table highlights the typical organization usage of PII for each subsystem in the NMB GSS information system.

Table 3: Typical NMB Organizational NMB GSS Usage of PII

NMB GSS Subsystem	Information Categories Utilized	Typical PII Usage
G-Suite and Google Cloud Platform (GCP)	C.2 Rationale and Factors for Services Delivery Support Information, C.3 Rationale and Factors for Government Resource Management Information, and D.13 Workforce Management	PII is typically utilized to process HR actions.
Zscaler	C.2 Rationale and Factors for Services Delivery Support Information, C.3 Rationale and Factors for Government Resource Management Information, and D.20 Knowledge Creation and Management	PII is transferred and received utilizing the network infrastructure.
Qualys	C.3 Rationale and Factors for Government Resource Management Information	Qualys does not use PII to perform its vulnerability management functions
Endpoints	C.2 Rationale and Factors for Services Delivery Support Information, C.3 Rationale and Factors for Government Resource Management Information, and D.13 Workforce Management Resource Management	PII is typically used to perform HR and personnel security actions. PII can be transferred verbally utilizing the telecommunications system.
Duo	C.3 Rationale and Factors for Government Resource Management Information	PII is typically utilized to create user accounts and validate those accounts. The types of PII used are names, e-mail, phone numbers, and IP addresses.
BeyondTrust	C.3 Rationale and Factors for Government Resource Management Information	BeyondTrust does not use PII to perform its remote support or remote access functions
MobileIron	C.3 Rationale and Factors for Government Resource Management Information	PII is utilized to create user accounts and validate devices through identifiers such as phone number, and email.
Webex	C.3 Rationale and Factors for Government Resource Management Information	PII can be transferred verbally utilizing the telecommunications.
Cisco Meraki	C.3 Rationale and Factors for Government Resource Management Information	PII is transferred and received utilizing the network infrastructure.

2.5 NMB GSS PII Protections

The NMB GSS has been developed with an emphasis placed on the protection of PII and S-PII information. The NMB GSS 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*.” The NMB GSS incorporates the appropriate baseline security controls to protect the confidentiality, integrity, and availability (CIA) of the system.

The NMB GSS utilizes “Moderate” level baseline security controls (except Avaya Phone System which incorporates the low baseline as a categorized low system per the FIPS 199), as outlined in the NIST SP 800-53 Revision 5, “*Security and Privacy Controls for Information Systems and Organizations*”. NMB is committed to protecting the PII information contained in the NMB GSS and its subsystems by emphasizing the following security controls listed in **Table 4: Critical PII Protection Controls**.

Table 4: Critical PII Protection Controls

Control Description:	Control Objective
Multifactor Authentication	Admins must know a [REDACTED] password and have 2FA enabled for authentication.
Encryption	Data used in the NMB GSS is encrypted in transit and at rest.
Unique Admin User ID	Each admin account will have its unique log-in ID to aid in tracking system configuration changes.
Admin Activity Logs Generated	All admin changes to NMB GSS subsystems are generated and captured in the system audit logs.
Periodic Security Audits	The NMB ISSO and SCA will conduct annual security audits/assessments for each NMB system with an 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 GSS System of Record Notice (SORN) Requirement

The NMB GSS 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 GSS 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 GSS System Security Plan (SSP)

The NMB GSS SSP has been developed and is updated in accordance with the RMF process.

6. NMB GSS Characterization of Information

The NMB GSS collects, uses, disseminates, or maintains PII information from three categories: prospective employees, current employees, terminated employees.

Table 5: NMB GSS Collected PII Information

Category of Individual	Type of PII Collected	Collection Source	PII NMB GSS Storage Locations
Prospective Employees	Criminal history, Medical information, Bank account numbers, Mother's maiden name, Employment information, Account passwords, Financial account numbers (i.e. credit card number), Social Security numbers, Truncated SSN (such as last four digits), Passport numbers, Citizenship or immigration status, Education information	Individual	G-Suite and GCP, NMB Endpoints (laptops, workstations, peripheral devices, etc.)
Current Employees	Criminal history, Medical information, Bank account numbers, Mother's maiden name, Employment information, Account passwords, Financial account numbers (i.e. credit card number), Social Security numbers, Truncated SSN (such as last four digits), Passport numbers, Citizenship or immigration status, Education information	Individual	G-Suite and GCP, NMB Endpoints (laptops, workstations, peripheral devices, etc.)
Terminated Employees	Criminal history, Medical information, Bank account numbers, Mother's maiden name, Employment information, Account passwords, Financial account numbers (i.e. credit card number), Social Security numbers, Truncated SSN (such as last four digits), Passport numbers, Citizenship or immigration status, Education information	Individual	G-Suite and GCP, NMB Endpoints (laptops, workstations, peripheral devices, etc.)

7. Privacy Impact Analysis of Characterization of Information

Primary risks for the NMB GSS as it relates to the characterization of information are a data breach of the G-Suite/GCP subsystem, loss of an NMB Endpoints (printers, laptops, workstations, etc.), and malicious (intentional or unintentional) activity from NMB personnel.

Employment at NMB requires the collection of PII/S-PII to determine the prospective employee's eligibility for employment, performance monitoring of current employees, and completion of various work tasks. The collected PII and S-PII is stored primarily on a third-party cloud system (G-Suite/GCP). Subsequently, NMB GSS relies on the performance of Google administrators to properly implement the appropriate information security controls and disclose breaches to NMB.

PII and S-PII information that is stored on an NMB Endpoint subsystem (laptops, printers, workstations, etc.) could become compromised if the asset is lost or stolen.

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.

8. 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).

9. Retention of Collected PII

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

10. NMB GSS ISSO PII Program Recommendations

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