INSPECTOR GENERAL

MEMORANDUM

May 29, 2026

TO: Julie Kitka
Federal Co-Chair, Denali Commission

FROM: Roderick Fillinger
Inspector General

SUBJECT: Denali Commission - Privacy and Data Protection Audit (Report No. 2026-AUD-007)

I am pleased to provide you with the attached audit report in which Premier Group Services (PG), an independent public accounting firm, presented an audit of the Denali Commission's implementation of privacy and data protection policies, procedures and practices as directed in 42 U.S.C. § 2000ee-2.

The objective of the audit was to assess the Commission's implementation of its privacy and data security program in accordance with federal law, regulation, and policy. Specifically, the audit was designed to determine whether the Commission implemented effective privacy and data protection policies and procedures in accordance with 42 U.S.C. § 2000ee-2.

In PG's opinion, the Commission has implemented privacy and data protection policies and procedures that are consistent with applicable federal requirements. The Commission’s privacy policy documentation, website practices, and Section 522 compliance posture are adequate. Nine NIST Privacy Framework control subcategories were assessed as not addressed in the Commission’s policy documentation; however, as explained further in the Objectives, Scope and Methodology section and Appendix A, these observations are directly attributable to the Commission’s shared service operating model and do not represent substantive deficiencies. The prior year finding regarding privacy program weaknesses has been reviewed and is addressed under the Status of Prior Year Findings and Recommendations section of this report.

In connection with the contract, we reviewed PG's report and related documentation and inquired of its representatives. Our review, as differentiated from an examination in accordance with generally accepted government auditing standards, was not intended to enable us to express, and we do not express, an opinion on PG's description of the Commission's controls, the suitability of

the design of these controls and the operating effectiveness of controls tested. PG is solely responsible for the attached report, dated May 28, 2026, and the conclusions expressed in it. However, our review disclosed no instances where PG did not comply, in all material respects, with U.S. generally accepted government auditing standards.

We appreciate the cooperation and courtesies the Denali Commission extended to both PG and my office during the audit. If you wish to discuss the contents of this report, please call me at (907) 271-3500.

Attachment

cc: Judy Herrick
John Whittington, General Counsel

DENALI COMMISSION
OFFICE OF INSPECTOR GENERAL
ANCHORAGE, AK 99501

PRIVACY AND DATA PROTECTION AUDIT REPORT
CONTRACT NUMBER: 20342925Q00003
PERIOD: OCTOBER 1, 2024, TO SEPTEMBER 30, 2025

Table of Contents

Premier Group
Trust. That's our bottom line!

Report of Independent Public Accountants

To the Office of Inspector General of Denali Commission:

This report presents the results of our audit of the Denali Commission's (the Commission) privacy and data protection policies, procedures, and practices for compliance with the Consolidated Appropriations Act of 2005 (Public Law 108-447), Division H, Section 522, as amended; Section 208 of the E-Government Act of 2002 (Public Law 107-347); the Privacy Act of 1974; and applicable OMB Memorandums.

The audit included an assessment of applicable federal privacy laws, regulations, and standards to the Commission's privacy policy. The privacy requirements were mapped to applicable privacy controls listed under the National Institute of Standards and Technology (NIST) Privacy Framework.

The audit was performed in accordance with *Generally Accepted Government Auditing Standards*. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives.

Based on the results of our audit procedures, we concluded that the Commission has implemented effective privacy and data protection policies and procedures and was in compliance with all applicable federal privacy laws, regulations, and standards identified above. Nine controls within the NIST Privacy Framework Gap Analysis were assessed as not addressed; however, these gaps do not constitute substantive deficiencies in the Commission's privacy program because the Commission does not collect, use, share, disclose, transfer, or store privacy data. Systems containing privacy data are maintained by the Department of the Treasury and the Department of the Interior under applicable Interagency Support Agreements and are outside the scope of this audit. Observations and related context are presented in Appendix A.

Premier Group

Premier Group Services, Inc.

May 28, 2026

Landover, MD

Executive Summary

Premier Group (PG) was engaged by the Denali Commission Office of Inspector General (OIG) to conduct a Privacy and Data Protection Audit of the Denali Commission (the Commission) for the period October 1, 2024, through September 30, 2025. The audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) and evaluated the Commission's compliance with the Consolidated Appropriations Act of 2005 (Public Law 108-447), Division H, Section 522, as amended; Section 208 of the E-Government Act of 2002 (Public Law 107-347); the Privacy Act of 1974; and applicable Office of Management and Budget (OMB) Memorandums. Privacy requirements were mapped to applicable controls under the National Institute of Standards and Technology (NIST) Privacy Framework.

A key determinative factor in this audit is that the Commission does not collect, use, share, disclose, transfer, or store privacy data. Systems containing privacy data used by Commission employees are owned and maintained by the Department of the Treasury and the Department of the Interior under applicable Interagency Support Agreements and are outside the scope of this engagement. Given this operating model, the Commission's privacy risk profile is inherently limited; privacy obligations at the Commission level relate principally to governance, policy documentation, workforce awareness, and coordination with shared service providers rather than to direct data handling.

Based on audit procedures performed, PG concluded that the Commission has implemented privacy and data protection policies and procedures that are consistent with applicable federal requirements. The Commission's privacy policy documentation, website practices, and Section 522 compliance posture are adequate. Nine NIST Privacy Framework control subcategories were assessed as not addressed in the Commission's policy documentation; however, as explained further in the Objectives, Scope and Methodology section and Appendix A, these observations are directly attributable to the Commission's shared service operating model and do not represent substantive deficiencies. The prior year finding regarding privacy program weaknesses has been reviewed and is addressed under the Status of Prior Year Findings and Recommendations section of this report.

Objectives, Scope and Methodology

Objectives

The overall objectives of the Privacy and Data Protection audit are to:

- Review the Commission's compliance with section 522 of the Consolidated Appropriations Act of 2005, as amended
- Evaluate the Commission's technology, practices, and procedures regarding collection, use, sharing, disclosure, transfer, and storage of information in identifiable form
- Review stated privacy and data protection procedures relating to agency employees and the public
- Conduct detailed analysis of agency intranet, network, and websites for privacy vulnerabilities
- Assess compliance with Federal privacy and data security laws and regulations, including:
- Consolidated Appropriations Act of 2005 (Public Law 108-447), Division H, Section 522, as amended
- Section 208 of the 2002 E-Government Act (Privacy Provisions)
- Privacy Act of 1974
- Office of Management and Budget Memorandums.

Scope and Methodology

The scope of this audit encompassed the Commission's privacy and data security policies and procedures for the fiscal year ended September 30, 2025. To accomplish the audit objectives, PG performed the following procedures within each area of scope:

1. Planning and Risk Assessment

PG reviewed applicable Federal laws, regulations, and OMB guidance governing privacy and data protection, including the Privacy Act of 1974, Section 208 of the E-Government Act of 2002, the Consolidated Appropriations Act of 2005 (Section 522, as amended), and relevant OMB memorandums (e.g., OMB M-03-22, OMB M-07-16). We reviewed the Commission's organizational structure, mission, programs, and information technology (IT) environment to identify the universe of systems, applications, and processes that collect, use, or maintain privacy data. We also reviewed the prior Privacy and Data Protection Audit report and open recommendations to focus testing on previously identified risk areas and assess the status of corrective actions.

2. Collection, Use, Sharing, Disclosure, Transfer, and Storage of Privacy Data

To assess the Commission's technology environment and operational practices governing privacy data, PG:

- Reviewed policies, procedures, and internal controls over the collection, use, sharing, disclosure, transfer, and storage of privacy data relating to agency employees and the public;
- Evaluated whether data handling practices are consistent with the Commission's published privacy notices and applicable Federal requirements; and

- Assessed the Commission's data retention and disposal procedures for privacy data, including whether records are maintained or destroyed in accordance with approved records schedules and applicable law.

3. Privacy and Data Protection Policies and Procedures

To evaluate the Commission's stated privacy and data protection policies, PG:

- Obtained and reviewed the Commission's privacy program documentation, including Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), Privacy Act notices, IT security policies, acceptable use policies, and data breach response procedures;
- Assessed the completeness and currency of privacy program documentation against applicable Federal requirements; and
- Conducted interviews with Commission management and key personnel responsible for privacy program oversight, IT systems administration, and records management to obtain an understanding of how privacy and data protection responsibilities are assigned, communicated, and monitored.

4. Intranet, Network, and Website Privacy Vulnerability Analysis

To identify privacy vulnerabilities within the Commission's technology environment, PG performed a detailed analysis of the Commission's intranet, network, and public-facing websites. Specifically, PG:

- Assessed compliance between published privacy practices, policies, and procedures and actual operational practices, identifying instances of noncompliance;
- Reviewed public-facing websites for required privacy notices, privacy policy statements, and machine-readable privacy metadata consistent with OMB and agency requirements; and
- Evaluated access controls, data handling configurations, and transmission security measures for risks of inadvertent release of privacy data.

5. Compliance with the Consolidated Appropriations Act of 2005

To evaluate the Commission's compliance with Section 522 of the Consolidated Appropriations Act of 2005, as amended, PG:

- Verified whether required privacy reviews, reports, and notifications were completed within the required timeframes;
- Evaluated whether PIAs were conducted for applicable IT systems and updated following significant system changes; and
- Assessed whether SORNs were published for applicable systems of records and accurately describe the Commission's data practices.

6. Follow-Up on Prior Audit Recommendations

To evaluate the Commission's progress in addressing previously identified weaknesses, PG:

- Identified all open recommendations from the prior Privacy and Data Protection Audit report;

- Evaluated management's proposed corrective action plan (CAP) for each open recommendation to determine whether planned actions are sufficient to remediate the identified weaknesses; and
- Documented the current implementation status of each prior recommendation as of the fieldwork period.

Summary of Findings and Recommendations

PG's assessment of the Commission's privacy and data protection program identified nine NIST Privacy Framework control subcategories that were not addressed in the Commission's policy documentation. These observations are noted as findings in Appendix A and reflect areas where the Commission's documentation does not explicitly address the applicable control requirement. However, each of these control gaps is directly attributable to the Commission's shared service operating model: because the Commission does not collect, use, share, disclose, transfer, or store privacy data, and all privacy data-bearing systems are owned and operated by the Department of the Treasury and the Department of the Interior under applicable Interagency Support Agreements, the underlying activities to which these controls apply do not occur at the Commission level. Accordingly, the findings do not represent substantive deficiencies in the Commission's privacy and data protection program. Outside of these nine framework observations, no additional findings or recommendations were identified.

Status of Prior Year Findings and Recommendations

Prior Year Finding: Privacy Program Weakness

While the Commission has further enhanced its privacy policy, there are still areas that need to be enhanced to comply with the requirements of the NIST Privacy Framework.

Recommendation:

Review the data asset inventory to ensure that all data assets owned by the Commission are identified and enhance the Commission's Privacy Policies and Procedures to address the gaps that were identified in the current Privacy Policy.

Current Status

PG reviewed documentation provided by the Commission and interviewed Denali Commission personnel to assess the status of the prior year recommendation. Based on procedures performed, the Commission has taken steps to strengthen its privacy program, including the issuance of an updated internal privacy policy and improved documentation of its shared service provider framework. The nine NIST Privacy Framework control subcategories identified as not addressed in this year's gap analysis (Appendix A) are attributable to the Commission's operational model and do not reflect a failure to act on the prior year recommendation. The prior year finding is considered resolved to the extent practicable given the Commission's shared service structure.

Appendix A – NIST Privacy Framework Gap Analysis

The following table presents PG's independent assessment of the Commission's privacy program against the NIST Privacy Framework.

Legend: Yes = Control is addressed. **No** = Control is not addressed or insufficient. Where noted as a Finding, the control gap is attributable to the Commission's operational model; the Commission does not collect, use, share, disclose, transfer, or store privacy data.

FUNCTION	CATEGORY	SUBCATEGORY	ADDRESSED IN THE COMMISSION'S POLICY
IDENTIFY-P (ID-P): Develop the organizational understanding to manage privacy risk for individuals arising from data processing.	**Inventory and Mapping (ID.IM-P):** Data processing by systems, products, or services is understood and informs the management of privacy risk.	**ID.IM-P1:** Systems/products/services that process data are inventoried.	Yes
		ID.IM-P2: Owners or operators (e.g., the organization or third parties such as service providers, partners, customers, and developers) and their roles with respect to the systems/products/services and components (e.g., internal or external) that process data are inventoried.	Yes
		ID.IM-P3: Categories of individuals (e.g., customers, employees or prospective employees, consumers) whose data are being processed are inventoried.	Yes
		ID.IM-P4: Data actions of the systems/products/services are inventoried.	No (Commission does not collect, use, share, disclose, transfer, or store privacy data)
		ID.IM-P5: The purposes for the data actions are inventoried.	No (Commission does not collect, use, share, disclose, transfer, or store privacy data)
		ID.IM-P6: Data elements within the data actions are inventoried.	No (Commission does not collect, use, share, disclose, transfer,

		or store privacy data)
	ID.IM-P7: The data processing environment is identified (e.g., geographic location, internal, cloud, third parties).	Yes
	ID.IM-P8: Data processing is mapped, illustrating the data actions and associated data elements for systems/products/services, including components; roles of the component owners/operators; and interactions of individuals or third parties with the systems/products/services.	Yes
Business Environment (ID.BE-P): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform privacy roles, responsibilities, and risk management decisions.	**ID.BE-P1:** The organization's role(s) in the data processing ecosystem are identified and communicated.	Yes
	ID.BE-P2: Priorities for organizational mission, objectives, and activities are established and communicated.	Yes
	ID.BE-P3: Systems/products/services that support organizational priorities are identified and key requirements communicated.	Yes
Risk Assessment (ID.RA-P): The organization understands the privacy risks to individuals and how such privacy risks may create follow-on impacts on organizational operations, including mission, functions, other risk management priorities (e.g., compliance, financial), reputation, workforce, and culture.	**ID.RA-P1:** Contextual factors related to the systems/products/services and the data actions are identified (e.g., individuals' demographics and privacy interests or perceptions, data sensitivity and/or types, visibility of data processing to individuals and third parties).	Yes
	ID.RA-P2: Data analytic inputs and outputs are identified and evaluated for bias.	Yes
	ID.RA-P3: Potential problematic data actions and	Yes

		associated problems are identified.	
		ID.RA-P4: Problematic data actions, likelihoods, and impacts are used to determine and prioritize risk.	Yes
		ID.RA-P5: Risk responses are identified, prioritized, and implemented.	Yes
	Data Processing Ecosystem Risk Management (ID.DE-P): The organization's priorities, constraints, risk tolerance, and assumptions are established and used to support risk decisions associated with managing privacy risk and third parties within the data processing ecosystem. The organization has established and implemented the processes to identify, assess, and manage privacy risks within the data processing ecosystem.	**ID.DE-P1:** Data processing ecosystem risk management policies, processes, and procedures are identified, established, assessed, managed, and agreed to by organizational stakeholders.	Yes
		ID.DE-P2: Data processing ecosystem parties (e.g., service providers, customers, partners, product manufacturers, application developers) are identified, prioritized, and assessed using a privacy risk assessment process.	Yes
		ID.DE-P3: Contracts with data processing ecosystem parties are used to implement appropriate measures designed to meet the objectives of an organization's privacy program.	Yes
		ID.DE-P4: Interoperability frameworks or similar multi-party approaches are used to manage data processing ecosystem privacy risks.	Yes
		ID.DE-P5: Data processing ecosystem parties are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual, interoperability framework, or other obligations.	Yes

GOVERN-P (GV-P): Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.	**Governance Policies, Processes, and Procedures (GV.PO-P):** The policies, processes, and procedures to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of privacy risk.	**GV.PO-P1:** Organizational privacy values and policies (e.g., conditions on data processing such as data uses or retention periods, individuals' prerogatives with respect to data processing) are established and communicated.	Yes
		GV.PO-P2: Processes to instill organizational privacy values within system/product/service development and operations are established and in place.	Yes
		GV.PO-P3: Roles and responsibilities for the workforce are established with respect to privacy.	Yes
		GV.PO-P4: Privacy roles and responsibilities are coordinated and aligned with third-party stakeholders (e.g., service providers, customers, partners).	Yes
		GV.PO-P5: Legal, regulatory, and contractual requirements regarding privacy are understood and managed.	Yes
		GV.PO-P6: Governance and risk management policies, processes, and procedures address privacy risks.	Yes
	Risk Management Strategy (GV.RM-P): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**GV.RM-P1:** Risk management processes are established, managed, and agreed to by organizational stakeholders.	Yes
		GV.RM-P2: Organizational risk tolerance is determined and clearly expressed.	Yes
		GV.RM-P3: The organization's determination of risk tolerance is informed by its role(s) in the data processing ecosystem.	Yes
	Awareness and Training (GV.AT-P): The organization's	**GV.AT-P1:** The workforce is informed and trained on its roles and responsibilities.	Yes

	workforce and third parties engaged in data processing are provided privacy awareness education and are trained to perform their privacy-related duties and responsibilities consistent with related policies, processes, procedures, and agreements and organizational privacy values.	**GV.AT-P2:** Senior executives understand their roles and responsibilities.	Yes
		GV.AT-P3: Privacy personnel understand their roles and responsibilities.	Yes
		GV.AT-P4: Third parties (e.g., service providers, customers, partners) understand their roles and responsibilities.	Yes
	Monitoring and Review (GV.MT-P): The policies, processes, and procedures for ongoing review of the organization's privacy posture are understood and inform the management of privacy risk.	**GV.MT-P1:** Privacy risk is re-evaluated on an ongoing basis and as key factors, including the organization's business environment (e.g., introduction of new technologies), governance (e.g., legal obligations, risk tolerance), data processing, and systems/products/services change.	Yes
		GV.MT-P2: Privacy values, policies, and training are reviewed and any updates are communicated.	Yes
		GV.MT-P3: Policies, processes, and procedures for assessing compliance with legal requirements and privacy policies are established and in place.	Yes
		GV.MT-P4: Policies, processes, and procedures for communicating progress on managing privacy risks are established and in place.	Yes
		GV.MT-P5: Policies, processes, and procedures are established and in place to receive, analyze, and respond to problematic data actions disclosed to the organization from internal and external sources (e.g., internal discovery, privacy researchers, professional events).	Yes

		GV.MT-P6: Policies, processes, and procedures incorporate lessons learned from problematic data actions.	Yes
		GV.MT-P7: Policies, processes, and procedures for receiving, tracking, and responding to complaints, concerns, and questions from individuals about organizational privacy practices are established and in place.	Yes
CONTROL-P (CT-P): Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.	**Data Processing Policies, Processes, and Procedures (CT.PO-P):** Policies, processes, and procedures are maintained and used to manage data processing (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) consistent with the organization's risk strategy to protect individuals' privacy.	**CT.PO-P1:** Policies, processes, and procedures for authorizing data processing (e.g., organizational decisions, individual consent), revoking authorizations, and maintaining authorizations are established and in place.	Yes
		CT.PO-P2: Policies, processes, and procedures for enabling data review, transfer, sharing or disclosure, alteration, and deletion are established and in place (e.g., to maintain data quality, manage data retention).	Yes
		CT.PO-P3: Policies, processes, and procedures for enabling individuals' data processing preferences and requests are established and in place.	Yes
		CT.PO-P4: A data life cycle to manage data is aligned and implemented with the system development life cycle to manage systems.	Yes
	Data Processing Management (CT.DM-P): Data are managed consistent with the organization's risk strategy to protect individuals' privacy, increase manageability, and enable the	**CT.DM-P1:** Data elements can be accessed for review.	Yes
		CT.DM-P2: Data elements can be accessed for transmission or disclosure.	Yes
		CT.DM-P3: Data elements can be accessed for alteration.	Yes
		CT.DM-P4: Data elements can be accessed for deletion.	Yes

	implementation of privacy principles (e.g., individual participation, data quality, data minimization).	**CT.DM-P5:** Data are destroyed according to policy.	Yes
		CT.DM-P6: Data are transmitted using standardized formats.	Yes
		CT.DM-P7: Mechanisms for transmitting processing permissions and related data values with data elements are established and in place.	Yes
		CT.DM-P8: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization.	Yes
		CT.DM-P9: Technical measures implemented to manage data processing are tested and assessed.	Yes
		CT.DM-P10: Stakeholder privacy preferences are included in algorithmic design objectives and outputs are evaluated against these preferences.	No (Commission does not collect, use, share, disclose, transfer, or store privacy data)
	Disassociated Processing (CT.DP-P): Data processing solutions increase disassociability consistent with the organization's risk strategy to protect individuals' privacy and enable implementation of privacy principles (e.g., data minimization).	**CT.DP-P1:** Data are processed to limit observability and linkability (e.g., data actions take place on local devices, privacy-preserving cryptography).	Yes
		CT.DP-P2: Data are processed to limit the identification of individuals (e.g., de-identification privacy techniques, tokenization).	Yes
		CT.DP-P3: Data are processed to limit the formulation of inferences about individuals' behavior or activities (e.g., data processing is decentralized, distributed architectures).	Yes
		CT.DP-P4: System or device configurations permit selective collection or disclosure of data elements.	Yes

		CT.DP-P5: Attribute references are substituted for attribute values.	Yes
COMMUNICATE-P (CM-P): Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding and engage in a dialogue about how data are processed and associated privacy risks.	**Communication Policies, Processes, and Procedures (CM.PO-P):** Policies, processes, and procedures are maintained and used to increase transparency of the organization's data processing practices (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) and associated privacy risks.	**CM.PO-P1:** Transparency policies, processes, and procedures for communicating data processing purposes, practices, and associated privacy risks are established and in place.	Yes
		CM.PO-P2: Roles and responsibilities (e.g., public relations) for communicating data processing purposes, practices, and associated privacy risks are established.	Yes
	Data Processing Awareness (CM.AW-P): Individuals and organizations have reliable knowledge about data processing practices and associated privacy risks, and effective mechanisms are used and maintained to increase predictability consistent with the organization's risk strategy to protect individuals' privacy.	**CM.AW-P1:** Mechanisms (e.g., notices, internal or public reports) for communicating data processing purposes, practices, associated privacy risks, and options for enabling individuals' data processing preferences and requests are established and in place.	Yes
		CM.AW-P2: Mechanisms for obtaining feedback from individuals (e.g., surveys or focus groups) about data processing and associated privacy risks are established and in place.	No (Commission does not collect, use, share, disclose, transfer, or store privacy data)
		CM.AW-P3: System/product/service design enables data processing visibility.	Yes
		CM.AW-P4: Records of data disclosures and sharing are maintained and can be accessed for review or transmission/disclosure.	Yes

		CM.AW-P5: Data corrections or deletions can be communicated to individuals or organizations (e.g., data sources) in the data processing ecosystem.	Yes
		CM.AW-P6: Data provenance and lineage are maintained and can be accessed for review or transmission/disclosure.	Yes
		CM.AW-P7: Impacted individuals and organizations are notified about a privacy breach or event.	Yes
		CM.AW-P8: Individuals are provided with mitigation mechanisms (e.g., credit monitoring, consent withdrawal, data alteration or deletion) to address impacts of problematic data actions.	Yes
PROTECT-P (PR-P): Develop and implement appropriate data processing safeguards.	**Data Protection Policies, Processes, and Procedures (PR.PO-P)**: Security and privacy policies (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment), processes, and procedures are maintained and used to manage the protection of data.	**PR.PO-P1:** A baseline configuration of information technology is created and maintained incorporating security principles (e.g., concept of least functionality).	Yes
		PR.PO-P2: Configuration change control processes are established and in place.	Yes
		PR.PO-P3: Backups of information are conducted, maintained, and tested.	Yes
		PR.PO-P4: Policy and regulations regarding the physical operating environment for organizational assets are met.	Yes
		PR.PO-P5: Protection processes are improved.	Yes
		PR.PO-P6: Effectiveness of protection technologies is shared.	No (Commission does not collect, use, share, disclose, transfer, or store privacy data)

		PR.PO-P7: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed.	Yes
		PR.PO-P8: Response and recovery plans are tested.	Yes
		PR.PO-P9: Privacy procedures are included in human resources practices (e.g., deprovisioning, personnel screening).	Yes
		PR.PO-P10: A vulnerability management plan is developed and implemented.	Yes
	Identity Management, Authentication, and Access Control (PR.AC-P): Access to data and devices is limited to authorized individuals, processes, and devices, and is managed consistent with the assessed risk of unauthorized access.	**PR.AC-P1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.	Yes
		PR.AC-P2: Physical access to data and devices is managed.	Yes
		PR.AC-P3: Remote access is managed.	Yes
		PR.AC-P4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	Yes
		PR.AC-P5: Network integrity is protected (e.g., network segregation, network segmentation).	Yes
		PR.AC-P6: Individuals and devices are proofed and bound to credentials, and authenticated commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).	Yes
	Data Security (PR.DS-P): Data are managed consistent with the organization's risk	**PR.DS-P1:** Data-at-rest are protected.	Yes
		PR.DS-P2: Data-in-transit are protected.	Yes

	strategy to protect individuals' privacy and maintain data confidentiality, integrity, and availability.	**PR.DS-P3:** Systems/products/services and associated data are formally managed throughout removal, transfers, and disposition.	Yes
		PR.DS-P4: Adequate capacity to ensure availability is maintained.	Yes
		PR.DS-P5: Protections against data leaks are implemented.	Yes
		PR.DS-P6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	Yes
		PR.DS-P7: The development and testing environment(s) are separate from the production environment.	Yes
		PR.DS-P8: Integrity checking mechanisms are used to verify hardware integrity.	Yes
	Maintenance (PR.MA-P): System maintenance and repairs are performed consistent with policies, processes, and procedures.	**PR.MA-P1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.	No (Commission does not collect, use, share, disclose, transfer, or store privacy data)
		PR.MA-P2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	No (Commission does not collect, use, share, disclose, transfer, or store privacy data)
	Protective Technology (PR.PT-P): Technical security solutions are managed to ensure the security and resilience of systems/products/services and associated data, consistent with related policies, processes, procedures, and agreements.	**PR.PT-P1:** Removable media is protected and its use restricted according to policy.	No (Commission does not collect, use, share, disclose, transfer, or store privacy data)
		PR.PT-P2: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	Yes

	PR.PT-P3: Communications and control networks are protected.	Yes
	PR.PT-P4: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.	Yes

Denali Commission
550 W. 7th Street, Suite 1230
Anchorage, AK 99501

907.271.1414 (P)
888.480.4321(TF)
www.denali.gov

May 19, 2026

To: Premier Group Services, Inc.

Subject: Response to Privacy and Data Protection Act Audit

Thank you for conducting a thorough review and providing the results of the Denali Commission's (the Commission) privacy and data protection policies, procedures, and practices for the fiscal year October 1, 2024, through September 30, 2025.

The Commission appreciates the acknowledgment that as a small agency, the Commission does not collect, use, share, disclose, transfer, or store privacy data. Systems containing privacy data used by staff are owned and maintained by the Department of the Treasury and the Department of the Interior under applicable Interagency Support Agreements and are outside the scope of this engagement.

The Commission will continue its diligence to adhere to the current standards, adjust to changes and ensure that our shared service providers meet the standards required on an annual basis.

Thank you,

Julie Kitka
Denali Commission
Federal Co-Chair

Judy Herrick
Denali Commission
Privacy Officer