INSPECTOR GENERAL

MEMORANDUM

August 16, 2024

TO: Jocelyn Fenton
Interim Federal Co-Chair, Denali Commission

FROM: Roderick Fillinger
Inspector General

SUBJECT: Report of Findings and Recommendations for the Review of the Denali Commission's Privacy Program (Report No. OIG-AR-24-006)

I am pleased to provide you with the attached audit report in which SB & Company, LLC (SBC), 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 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 SBC's opinion, the Denali Commission has implemented effective privacy and data protection policies and procedures because it has implemented a majority of the NIST Privacy Framework to achieve effective privacy and data protection policies and procedures. In the fiscal year 2022 audit the privacy program was determined to be ineffective. This audit reflects the improvement made in the Commission's privacy program. Two recommendations have been made to continue improving the effectiveness of the privacy program.

In connection with the contract, we reviewed SBC'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 SBC's description of the Commission's controls, the suitability of the design of these controls and the operating effectiveness of controls tested. SBC is solely responsible for the attached report, dated August 15, 2024, and the conclusions expressed in it. However, our review disclosed no instances where SBC 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 SBC 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: Denali Commissioners
John Whittington, General Counsel

Report of Findings and Recommendations for the Review of the Denali Commission's Privacy Program

Certified Public Accountants & Business Advisors
SBC

August 15, 2024
The Honorable Roderick Fillinger
Inspector General
The Denali Commission
510 L Street, Suite 410
Anchorage, Alaska 99501

Dear Inspector General Fillinger:

SB & Company LLC is pleased to present our Audit of the Denali Commission's Privacy Program, which details the results of our performance audit of the Denali's Commission's implementation of privacy and data protection policies, procedures and practices as directed in 42 United States Code (U.S.C.) § 2000ee-2. We performed the audit under the contract with the Denali Commission Office of Inspector General.

We have reviewed the Denali Commission's response to the draft of this report and have included our evaluation of management's comments within this final report.

We appreciate the assistance received from the Denali Commission and appreciate the opportunity to serve you. We will be pleased to discuss any questions that you may have.

Very truly yours,

SB & Company, LLC

SB & Company, LLC

Certified Public Accountants & Business Advisors

Inspector General
The Denali Commission (Commission)

SB & Company LLC (SBC) conducted a performance audit of the Denali Commission's (the Commission) implementation of privacy and data protection, policies, procedures, and practices in 42 United States Code (U.SC.) § 2000ee-2. The objective of the audit was to assess the Commission's implementation of its privacy 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 United States Code (U.SC.) § 2000ee-2.

The Audit included an assessment of applicable federal privacy laws, regulations, and standards to the Commissions privacy policy. The privacy requirements were mapped to applicable privacy controls listed under the National Institute of Standards and Technology (NIST) Special Publications (SP) includes the Privacy Framework and (SP) 800-53 Revision 5 Security and Privacy Controls for Federal Information Systems and Organizations and the NIST Privacy Framework. The NIST Privacy Framework provides information on components that should be included in the Agency Privacy Program. The Privacy Framework is composed of three parts: Cores, Profiles, and Implementation Tiers. Each component reinforces privacy risk management through the connections between business and mission drivers, organizational roles and responsibilities, and privacy protection activities.

Our audit was performed in accordance with the performance audit standards specified in the *Government Auditing Standards*, issued by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide reasonable basis for our findings and conclusions based on our audit objectives.

We concluded the Commission had implemented effective privacy and data protection policies and procedures because it has implemented a majority of the NIST Privacy Framework to achieve effective privacy and data protection policies and procedures. While the Commission has implemented a majority of the framework, we recommend that a data asset inventory be completed to identify the data assets owned by the Commission. In addition, the Commission should perform a gap assessment to the Privacy Framework and NIST 800-53 to determine where the Privacy Policy can be enhanced. We identified opportunities to put in place or enhance privacy policies related to Identify, and Protect to inventory data actions, prevent data exfiltration, and maintenance of organizational assets.

Certified Public Accountants & Business Advisors
SBC

Additional information on our findings and recommendations are included in the accompanying report.

SB and Company LLC
Washington, DC
August 15, 2024

Certified Public Accountants & Business Advisors
SBC

Table of Contents **Page #**

Section I – Executive Summary ---------- 6

Section II – Findings and Recommendations ---------- 8

Appendix A - NIST Privacy Framework ----------11

Certified Public Accountants & Business Advisors
SBC

Section I

Executive Summary

The Denali Commission Act of 1998 established the Denali Commission (Commission) to deliver services of the federal government in the most cost-effective manner by reducing administrative and overhead costs. As part of the act, the Commission's mission of providing job training and other economic development services in rural communities was established with a specific focus on promoting rural development, and providing power generation, transition facilities, modern communication systems, water and sewer systems and other infrastructure needs in rural Alaska.

Since its inception, the Denali Commission Act of 1998 has been updated several times expanding its mission to include the planning and construction of health care facilities and the establishment of the Denali Access System Program for surface transportation infrastructure and waterfront transportation projects. Most recently, the Denali Commission Act was again expanded to include the authority for the Commission to accept funding from other federal agencies as well as gifts or donations for the purpose of carrying out the act.

The Privacy Act of 1974 defines the requirements of federal agencies for maintaining a Privacy Program. Federal government agencies are required to maintain a Data Privacy Program in accordance with the established Government-wide privacy standards. The National Institute of Standards and Technology (NIST) Special Publications (SP) includes the Privacy Framework and (SP) 800-53 Revision 5 Security and Privacy Controls for Federal Information Systems. These provide the information on components that should be included in the Agency Privacy Program. The Privacy Framework is composed of three parts: Cores, Profiles, and Implementation Tiers. Each component reinforces privacy risk management through the connections between business and mission drivers, organizational roles and responsibilities, and privacy protection activities.

The objective of the audit was to assess the Commission's implementation of its privacy program in accordance with federal law, regulation, and policy. Specifically, the audit was to determine whether the Commission implemented comprehensive privacy and data protection policies and procedures governing the Agency's collection, use, sharing, disclosure, transfer, storage, and security of information in an identifiable form relating to Agency employees and the public.

The audit was performed in accordance with the performance audit standards specified in *Government Auditing Standards*, issued by the Comptroller General of the United States. 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. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Certified Public Accountants & Business Advisors
SBC

Denali Commission
Summary of Results:

Privacy Program Weaknesses	**Recommendation**
1. While the Commission has further enhanced their privacy policy, there are still areas that need to be enhanced to comply with the requirements of the NIST Privacy Framework	**Recommendation 1:** 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.

Denali Commission

Section II - Status of Prior Year Findings and Recommendations

1. The Commission needs to enhance the Privacy Policy to comply with the requirements of the NIST Privacy Framework

Using the NIST Privacy Framework, SBC evaluated the policies, procedures, and controls in place to support the Denali Privacy Program. While the Commission has formalized their Privacy Policy and addressed many of the exceptions from the Prior Year's audit, exceptions remain to be addressed in three of the five domains – Identify, Communicate, and Protect. The exceptions identified related to enhancing the Commission's Policy such that all the privacy procedural requirements have been addressed. To complete this process, the Commission should verify inventory of the current data assets and then determine based on these assets how the remaining gaps in the Privacy Policy should be addressed. Appendix A of this report identifies the areas of gaps in the current Privacy Policy.

Recommendations

- Review the data asset inventory to verify that all the data assets owned by the Commission are identified.

- Enhance the Commission's Privacy Policies and Procedures to address the gaps that have been identified in the current Privacy Policy.

The Denali Commission's Response

This is in response to the *Audit of the Denali Commission's Privacy Program*. The report made two recommendations and the agencies' response includes a summary of services provided by Administration Resource Center (ARC) via Inter Agency Agreement (IAA) in four service areas that include Procurement, HR, Travel and Financial Management Servies.

For the purposes of this memo the Financial Management Services Summary is provided to show support that ARC adheres to the (along with all other services provided by ARC) six FISMA, NIST and OMB Circular A-130 and FISCAM bullets below.

Overview/Summary of Services/Denali/ARC-25-0013

ARC Financial Management Services provides a full range of accounting services including financial management system platform, budget processing, vendor and employee record maintenance/reporting, accounts payable (AP), accounts receivable (AR) and debt collections, receivable reporting, purchase and fleet card, payroll accounting, cash, accounting and reporting. Additional services that are optionally offered to ARC's full-service accounting

customers depending on need and/or preference include: investment accounting, budget reporting (MAX), Intra-governmental reporting & analysis, payroll projections, budget analysis, extended record retention services, and budget formulation and performance management.

The customer authorizes ARC to input and store information in electronic systems used by ARC. Access to these systems is controlled by a user's Personal Identity Verification Card (PIV) credentials or other Multi Factor Authentication service, such as ID.me in accordance with relevant laws, regulations, security requirements, privacy act and policies, such as:

- Coordination of Federal Information Policy [44 USC Ch. 35] which includes Federal Information Security Modernization Act (FISMA) of 2014 [PL 113-283]
- Recommended Security Controls for Federal Information Systems and Organizations [NIST SP 800-53, Revision 5]
- Guide for Developing Security Plans for Federal Information Systems [NIST SP 800-18, Revision1]
- Managing the Security of Information Exchanges [NIST SP 800-47, Revision 1]
- Office of Management and Budget (OMB) Circular A-130, Appendix III: Security of Federal Automated Information Systems
- Federal Information System Controls Audit Manual (FISCAM) ARC will maintain the supporting documentation related to transactions processed and reconciliations or reports prepared, including electronic and/or paper records, in accordance with the current Fiscal Service File Plan. Records retained are available for review and audit as needed. Records will be destroyed at the end of their retention period.

The findings in the Audit Report identifies areas that the Commission can improve upon:

- CM.AW-P2: Mechanisms for obtaining feedback.
  Response: ARC sends surveys requesting feedback to IAA customers on a basis. Feedback or issues can be made at any time via email or phone should the need arise.
- PR.PO-P6: Effectiveness of protection technologies.
  Response: The Commission can only access Commission-owned data through the server and if the position warrants access. Example only the HR specialist may access the HR site.
- PR.DS-P5: Protections against leaks are implemented.
  Response: The Commission staff is adequately trained on handling PII, PHI or Sensitive but unclassified. Staff can only access sites that relate to their position or personal data.
- PR.MA-P1: Maintenance and repair of organizational assets are performed and logged with approved controlled tools.
  Response: IT contract requires logging and tracking of tickets, reports provided to COR.
- PR.MA-P2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.

Response: Same as above. Additionally, IT contractor is vetted through DOI and granted access based on IT duties. Security background checks are more stringent for systems and tasks that have a higher risk association.

Certified Public Accountants & Business Advisors
SBC

Denali Commission
Appendix A - NIST Privacy Framework

Function	Category	Subcategory	Addressed in Denali's Privacy Policy	
			CY	PY
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	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	Yes
		ID.IM-P3: Categories of individuals (e.g., customers, employees or prospective employees, consumers) whose data are being processed are inventoried.	Yes	Yes
		ID.IM-P4: Data actions of the systems/products/ services are inventoried.	No	No
		ID.IM-P5: The purposes for the data actions are inventoried.	No	No
		ID.IM-P6: Data elements within the data actions are inventoried.	No	No
		ID.IM-P7: The data processing environment is	Yes	Yes

Function	Category	Subcategory	Addressed in Denali's Privacy Policy	
			CY	PY
		identified (e.g., geographic location, internal, cloud, third parties).		
		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	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	Yes
		D.BE-P2: Priorities for organizational mission, objectives, and activities are established and communicated.	Yes	Yes
		ID.BE-P3: Systems/products/services that support organizational priorities are identified and key requirements are communicated.	Yes	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	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	Yes	No

Function	Category	Subcategory	Addressed in Denali's Privacy Policy	
			CY	PY
	operations, including mission, functions, other risk management priorities (e.g., compliance, financial), reputation, workforce, and culture.	perceptions, data sensitivity and/or types, visibility of data processing to individuals and third parties).		
		ID.RA-P2: Data analytic inputs and outputs are identified and evaluated for bias.	Yes	Yes
		ID.RA-P3: Potential problematic data actions and associated problems are identified.	Yes	Yes
		ID.RA-P4: Problematic data actions, likelihoods, and impacts are used to determine and prioritize risk.	Yes	Yes
		ID.RA-P5: Risk responses are identified, prioritized, and implemented.	Yes	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	ID.DE-P1: Data processing ecosystem risk management policies, processes, and procedures are identified, established, assessed, managed, and agreed to by organizational stakeholders.	Yes	Yes
		ID.DE-P2: Data processing ecosystem parties (e.g., service providers, customers, partners, product manufacturers, application developers) are identified,	Yes	Yes

Function	Category	Subcategory	Addressed in Denali's Privacy Policy	
			CY	PY
	within the data processing ecosystem.	prioritized, and assessed using a privacy risk assessment process.		
		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	Yes
		ID.DE-P4: Interoperability frameworks or similar multi-party approaches are used to manage data processing ecosystem privacy risks.	Yes	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	No
GOVERN-P (GV-P): Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's 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	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	Yes	Yes

Function	Category	Subcategory	Addressed in Denali's Privacy Policy	
			CY	PY
management priorities that are informed by privacy risk.	requirements are understood and inform the management of privacy risk.	processing) are established and communicated.		
		GV.PO-P2: Processes to instill organizational privacy values within system/product/service development and operations are established and in place.	Yes	Yes
		GV.PO-P3: Roles and responsibilities for the workforce are established with respect to privacy.	Yes	Yes
		GV.PO-P4: Privacy roles and responsibilities are coordinated and aligned with third-party stakeholders (e.g., service providers, customers, partners).	Yes	Yes
		GV.PO-P5: Legal, regulatory, and contractual requirements regarding privacy are understood and managed.	Yes	Yes
		GV.PO-P6: Governance and risk management policies, processes, and procedures address privacy risks.	Yes	Yes
	Risk Management Strategy (GV.RM-P): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to	GV.RM-P1: Risk management processes are established, managed, and agreed to by organizational stakeholders.	Yes	Yes

Function	Category	Subcategory	Addressed in Denali's Privacy Policy	
			CY	PY
	support operational risk decisions.	GV.RM-P2: Organizational risk tolerance is determined and clearly expressed.	Yes	Yes
		GV.RM-P3: The organization's determination of risk tolerance is informed by its role(s) in the data processing ecosystem.	Yes	Yes
	Awareness and Training (GV.AT-P): The organization's 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-P1: The workforce is informed and trained on its roles and responsibilities.	Yes	Yes
		GV.AT-P2: Senior executives understand their roles and responsibilities.	Yes	Yes
		GV.AT-P3: Privacy personnel understand their roles and responsibilities.	Yes	Yes
		GV.AT-P4: Third parties (e.g., service providers, customers, partners) understand their roles and responsibilities.	Yes	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	Yes	Yes

Function	Category	Subcategory	Addressed in Denali's Privacy Policy	
			CY	PY
		systems/products/services change.		
		GV.MT-P2: Privacy values, policies, and training are reviewed and any updates are communicated.	Yes	Yes
		GV.MT-P3: Policies, processes, and procedures for assessing compliance with legal requirements and privacy policies are established and in place.	Yes	Yes
		GV.MT-P4: Policies, processes, and procedures for communicating progress on managing privacy risks are established and in place.	Yes	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	No
		GV.MT-P6: Policies, processes, and procedures incorporate lessons learned from problematic data actions.	Yes	No

Function	Category	Subcategory	Addressed in Denali's Privacy Policy	
			CY	PY
		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	No
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	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	Yes
		CT.PO-P3: Policies, processes, and procedures for enabling individuals' data processing preferences and requests are established and in place.	Yes	Yes

Function	Category	Subcategory	Addressed in Denali's Privacy Policy	
			CY	PY
		CT.PO-P4: A data life cycle to manage data is aligned and implemented with the system development life cycle to manage systems.	Yes	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 implementation of privacy principles (e.g., individual participation, data quality, data minimization).	CT.DM-P1: Data elements can be accessed for review.	Yes	Yes
		CT.DM-P2: Data elements can be accessed for transmission or disclosure.	Yes	Yes
		CT.DM-P3: Data elements can be accessed for alteration.	Yes	Yes
		CT.DM-P4: Data elements can be accessed for deletion.	Yes	Yes
		CT.DM-P5: Data are destroyed according to policy.	Yes	Yes
		CT.DM-P6: Data are transmitted using standardized formats.	Yes	Yes
		CT.DM-P7: Mechanisms for transmitting processing permissions and related data values with data elements are established and in place.	Yes	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	Yes

Function	Category	Subcategory	Addressed in Denali's Privacy Policy	
			CY	PY
		CT.DM-P9: Technical measures implemented to manage data processing are tested and assessed.	Yes	No
		CT.DM-P10: Stakeholder privacy preferences are included in algorithmic design objectives and outputs are evaluated against these preferences.	Not Applicable to Denali Commission	Not Applicable to Denali Commission
	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	No
		CT.DP-P2: Data are processed to limit the identification of individuals (e.g., de-identification privacy techniques, tokenization).	Yes	Yes
		CT.DP-P3: Data are processed to limit the formulation of inferences about individuals' behaviors or activities (e.g., data processing is decentralized, distributed architectures).	Yes	Yes
		CT.DP-P4: System or device configurations permit selective collection or disclosure of data elements.	Yes	Yes

Function	Category	Subcategory	Addressed in Denali's Privacy Policy	
			CY	PY
		CT.DP-P5: Attribute references are substituted for attribute values.	Yes	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	Yes
		CM.PO-P2: Roles and responsibilities (e.g., public relations) for communicating data processing purposes, practices, and associated privacy risks are established.	Yes	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	Yes
		CM.AW-P2: Mechanisms for obtaining feedback from individuals (e.g., surveys or focus groups) about data processing and associated privacy risks	No	No

Function	Category	Subcategory	Addressed in Denali's Privacy Policy	
			CY	PY
		are established and in place.		
		CM.AW-P3: System/product/service design enables data processing visibility.	Yes	Yes
		CM.AW-P4: Records of data disclosures and sharing are maintained and can be accessed for review or transmission/disclosure.	Yes	No
		CM.AW-P5: Data corrections or deletions can be communicated to individuals or organizations (e.g., data sources) in the data processing ecosystem.	Yes	No
		CM.AW-P6: Data provenance and lineage are maintained and can be accessed for review or transmission/disclosure.	Yes	No
		CM.AW-P7: Impacted individuals and organizations are notified about a privacy breach or event.	Yes	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	No

Function	Category	Subcategory	Addressed in Denali's Privacy Policy	
			CY	PY
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	Yes
		PR.PO-P2: Configuration change control processes are established and in place.	Yes	Yes
		PR.PO-P3: Backups of information are conducted, maintained, and tested.	Yes	Yes
		PR.PO-P4: Policy and regulations regarding the physical operating environment for organizational assets are met.	Yes	Yes
		PR.PO-P5: Protection processes are improved.	Yes	Yes
		PR.PO-P6: Effectiveness of protection technologies is shared.	No	No
		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	No
		PR.PO-P8: Response and recovery plans are tested.	Yes	Yes

Function	Category	Subcategory	Addressed in Denali's Privacy Policy	
			CY	PY
		PR.PO-P9: Privacy procedures are included in human resources practices (e.g., deprovisioning, personnel screening).	Yes	Yes
		PR.PO-P10: A vulnerability management plan is developed and implemented.	Yes	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	Yes
		PR.AC-P2: Physical access to data and devices is managed.	Yes	No
		PR.AC-P3: Remote access is managed.	Yes	Yes
		PR.AC-P4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	Yes	Yes
		PR.AC-P5: Network integrity is protected (e.g., network segregation, network segmentation).	Yes	Yes
		PR.AC-P6: Individuals and devices are proofed and bounded to credentials and authenticated	Yes	Yes

Function	Category	Subcategory	Addressed in Denali's Privacy Policy	
			CY	PY
		commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).		
	Data Security (PR.DS-P): Data are managed consistent with the organization's risk strategy to protect individuals' privacy and maintain data confidentiality, integrity, and availability.	PR.DS-P1: Data-at-rest are protected.	Yes	Yes
		PR.DS-P2: Data-in-transit are protected.	Yes	Yes
		PR.DS-P3: Systems/products/services and associated data are formally managed throughout removal, transfers, and disposition.	Yes	Yes
		PR.DS-P4: Adequate capacity to ensure availability is maintained.	Yes	No
		PR.DS-P5: Protections against data leaks are implemented.	No	No
		PR.DS-P6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	Yes	Yes
		PR.DS-P7: The development and testing environment(s) are separate from the production environment.	Yes	No
		PR.DS-P8: Integrity checking mechanisms are used to verify hardware integrity.	Yes	No

Function	Category	Subcategory	Addressed in Denali's Privacy Policy	
			CY	PY
	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	No
		PR.MA-P2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	No	No
	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	No
		PR.PT-P2: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	Yes	No
		PR.PT-P3: Communications and control networks are protected.	Yes	Yes
		PR.PT-P4: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.	Yes	No