

Denali Commission OIG

Results of the Evaluation of the FY 2023 Denali Commission Federal
Information Security Modernization Act of 2014 (FISMA) Reporting
Metrics
OIG-ER-24-004



Denali Commission
Office of Inspector General



INSPECTOR GENERAL

MEMORANDUM

DATE: March 25, 2024

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

Micaela Fowler
State Co-Chair, Deputy Commissioner, Department of Commerce,
Community and Economic Development for the State of Alaska

Alicia Amberg
Executive Director, Associated General Contractors of Alaska

Julie E. Kitka
President, Alaska Federation of Natives

Nils Andreassen
Executive Director, Alaska Municipal League

Pat Pitney
Interim President, University of Alaska

Joelle Hall
Executive President, Alaska State AFL-CIO

FROM: Roderick H. Fillinger
Inspector General

SUBJECT: Results of the Evaluation of the FY 2023 Denali Commission Federal
Information Security Modernization Act of 2014 (FISMA) Reporting
Metrics (Report No. OIG-ER-24-004)

I am pleased to provide you with the attached evaluation report in which SB & Company, LLC (SBC), an independent public accounting firm, determined that Denali Commission's overall information security program was "Defined." This report summarizes the results of the fiscal year (FY 2023) Federal Information Security Modernization Act (FISMA) evaluation and assesses the

maturity of controls used to address risks in each of the nine information security areas, called domains. This review assessed the effectiveness of information security programs and practices, including the Commission's compliance with FISMA and related information security policies, procedures, standards and guidelines for the period October 1, 2022, to September 30, 2023. SBC rated the Denali Commission's overall program of information security as "effective," because a majority of the FY 2023 FISMA metrics were rated Defined (Level 2). The final recommendation for corrective action from the FY 2021 evaluation was implemented.

My office oversaw the evaluation performance, including the review of SBC's report and related documentation and inquiries of its representatives. This review was conducted in accordance with CIGIE Quality Standards for Inspection and Evaluation and applicable American Institute of Certified Public Accountants (AICPA) standards, applying the FY 2023-2024 FISMA Reporting Metrics criteria developed by the Department of Homeland Security in conjunction with the Office of Management and Budget and the Council of the Inspectors General on Integrity and Efficiency (CIGIE).

I 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: John Whittington
Judy Herrick

**FY 2023 Denali Commission
Federal Information Security Modernization
Act of 2014 (FISMA) Reporting Metrics**

Table of Contents

Independent Accountants' Report	3
Background	5
Scope and Methodology	6
Prior Audit	8
Results	9
Conclusion	10
Recommendations	10
Status of Recommendations and Potential Monetary Benefits	11

Appendices

A. OIG-Completed Department of Homeland Security CyberScope 2023 IG FISMA Metrics	12
B. Status of the Denali Commission Corrective Actions for FY 2022 FISMA Audit Recommendations	37



SB & COMPANY, LLC
KNOWLEDGE • QUALITY • CLIENT SERVICE

Report of Independent Public Accountants

To the Management of Denali Commission:

This report presents the results of our independent evaluation of the Denali Commission's information security program and practices. The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies, including Denali Commission, to have an annual independent evaluation performed of their information security program and practices and to report the results of the evaluations to the Office of Management and Budget (OMB). OMB has delegated its responsibility for the collection of annual FISMA responses to the Department of Homeland Security (DHS). DHS, in conjunction with OMB and the Council of the Inspectors General on Integrity and Efficiency (CIGIE), developed the Fiscal Year (FY) 2023 - 2024 FISMA Reporting Metrics to collect these responses. FISMA requires the agency Inspector General (IG) or an independent external auditor to perform the independent evaluation as determined by the IG. The Denali Commission Office of Inspector General (OIG) contracted SB & Company, LLC (SBC) to conduct this independent evaluation and monitored our work to ensure we met professional standards and contractual requirements.

We conducted our independent evaluation in accordance with CIGIE Quality Standards for Inspection and Evaluation and applicable American Institute of Certified Public Accountants (AICPA) standards.

The objective for this independent evaluation was to assess the effectiveness of Denali Commission's information security program and practices, including Denali Commission's compliance with FISMA and related information security policies, procedures, standards, and guidelines for the period October 1, 2022 to September 30, 2023. We based our work on a selection of Denali Commission-wide security controls and a selection of system specific security controls across Denali Commission information systems. Additional details regarding the scope of our independent evaluation are included in the report, Background, Scope, and Methodology. Appendix A contains the CyberScope 2023 IG FISMA Metrics.

Consistent with applicable FISMA requirements, OMB policy and guidance, and National Institute of Standards and Technology (NIST) standards and guidelines, Denali Commission established and maintained its information security program and practices for its information systems for the five cybersecurity functions and nine FISMA metric domains. Based on the results entered into CyberScope, we determined that Denali Commission's overall information security program was "Defined" because a majority of the FY 2023 FISMA metrics were rated Defined (Level 2).



S B & COMPANY, LLC
KNOWLEDGE • QUALITY • CLIENT SERVICE

This independent evaluation did not constitute an engagement in accordance with Generally Accepted Government Auditing Standards. SBC did not render an opinion on Denali Commission's internal controls over financial reporting or over financial management systems as part of this evaluation. We caution that projecting the results of our evaluation to future periods or other Denali Commission information systems not included in our selection is subject to the risk that controls may become inadequate because of changes in technology or because compliance with controls may deteriorate.

Washington, D.C.
December 12, 2023

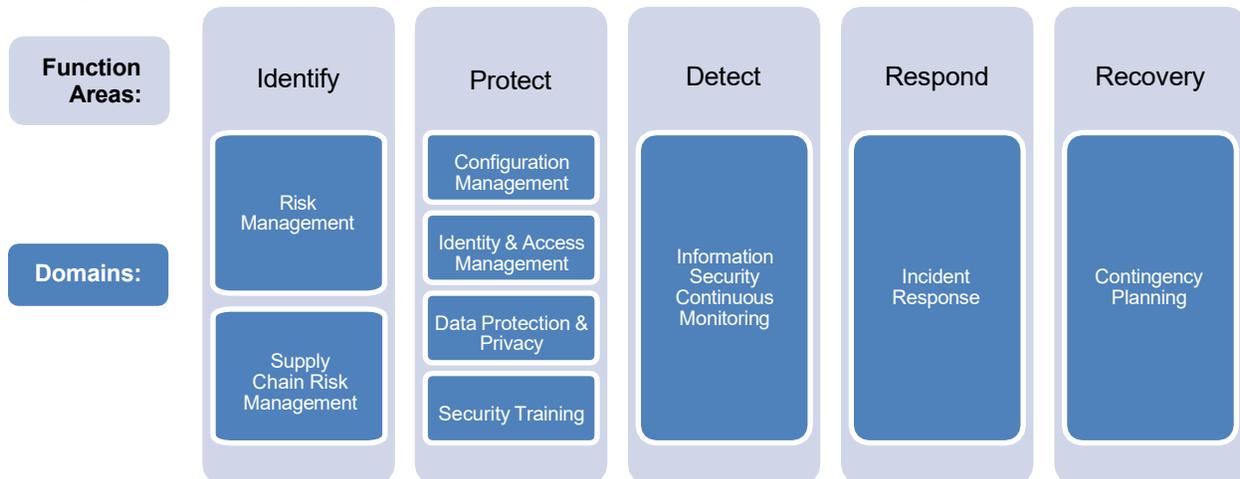
S B & Company, LLC

Background

Under the Federal Information Security Modernization Act of 2014 (FISMA), agency heads are responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification or destruction of information and information systems.

Each fiscal year, the U.S. Department of Homeland Security and the Office of Management and Budget issue an *IG FISMA Reporting Metrics* template for the IG of each federal agency to use to assess the agency’s information security program. The *FY 2023 – 2024 IG FISMA Reporting Metrics*¹, which can be found in Appendix A, identifies nine domains within the five security functions defined in the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (Figure 1)². This cybersecurity framework provides agencies with a common structure for identifying and managing cybersecurity risks to critical infrastructure across the enterprise.

Figure 1: FY 2023 cybersecurity framework security function areas and domains



Source: OIG-created graphic based on *FY 2023 IG FISMA Reporting Metrics* information.

The effectiveness of an agency’s information security program is based on a five-tiered maturity model spectrum (Table 1). An agency’s IG is responsible for annually assessing the agency’s rating along this spectrum by determining whether the agency possesses the required policies, procedures and strategies for each of the nine domains. The IG makes this determination by answering a series of questions about the domain-specific criteria that are presented in the annual *IG FISMA*

¹ *FY 2023 - 2024 IG FISMA Reporting Metrics*. These metrics were developed as a collaborative effort between the Office of and Budget, the Department of Homeland Security, and the Council of the Inspectors General on Integrity Management and Efficiency, in consultation with the Federal Chief Information Officer Council.

² Executive Order 13636, Improving Critical Infrastructure Cybersecurity, was issued February 19, 2013 and directed NIST to develop a voluntary framework based on existing standards, guidelines, and practices to reduce cyber risks to critical infrastructure.

Reporting Metrics template.

An agency must fully satisfy each maturity level before it can be evaluated at the next maturity level. This approach requires the agency to develop the necessary policies, procedures and strategies during the foundational levels (1 and 2). The advanced levels (3, 4 and 5) describe the extent to which the agencies have institutionalized those policies and procedures.

Table 1: Maturity model spectrum

Maturity level		Description
1	Ad Hoc	Policies, procedures and strategies are not formalized; activities are performed in an ad hoc, reactive manner.
2	Defined	Policies, procedures and strategies are formalized and documented but not consistently implemented.
3	Consistently Implemented	Policies, procedures and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
4	Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures and strategies are collected across the organization and used to assess them and make necessary changes.
5	Optimized	Policies, procedures and strategies are fully institutionalized, repeatable, self-generating, consistently implemented and regularly updated based on a changing threat and technology landscape and business/mission needs.

Source: *FY 2023 IG FISMA Reporting Metrics*.

Scope and Methodology

SB & Company, LLC (SBC or We) conducted this evaluation audit from May to July 2023 in accordance with CIGIE Quality Standards for Inspection and Evaluation and applicable American Institute of Certified Public Accountants (AICPA) standards.

During our evaluation, we assessed whether the Denali Commission exceeded Maturity Level 1, *Ad-Hoc*, for each of the 66 questions for the nine domains in the *FY 2023 - 2024 IG FISMA Reporting Metrics*. We conducted a risk assessment of the FY 2023 and Core IG FISMA metrics to determine whether changes made to the underlying criteria of the FISMA metric questions significantly changed since the FY 2022 evaluation.

We also evaluated the new FY 2023 and Core criteria to assess whether they significantly changed the Denali Commission’s responses to the overall metric questions since the FY 2020 audit. We assessed each new criterion as either:

- **High Risk**—The Office of Management and Budget introduced new reporting metrics, or the Denali Commission made significant changes to its information security program since the FY 2022 audit for the identified metric question.

- Low Risk—The Denali Commission made no significant changes to its information security program since the FY 2022 audit for the identified metric question.

We relied on the responses to the FY 2022 Denali Commission FISMA metric questions to answer the FY 2023 metric questions rated as *low risk*, and we conducted additional audit work to answer the questions rated as *high risk*.

We limited our assessment to determine whether the agency possessed the noted policies, procedures and strategies required for each metric under the function area. If the policies, procedures and strategies were formalized and documented, we rated the agency at Level 2, Defined. If not, we rated the agency at Level 1, *Ad Hoc*.

We worked closely with the Denali Commission and briefed the agency on the audit results for each function area of the *FY 2023 - 2024 IG FISMA Reporting Metrics*.

Appendix A provides the OIG response to each FISMA metric, as submitted to the Office of Management and Budget on July 31, 2023.

Prior Audit

During our testing of the Denali Commission’s FY 2023 FISMA compliance, SBC followed up on deficiencies identified in the FY 2022 FISMA evaluation. We reported that the Denali Commission lacked documented procedures and needed improvement in 1 domains: “Contingency Planning.” Specifically, SBC found that the Denali Commission did not:

1. Test the Contingency Plan annually to allow the Commission to effectively respond to incidents and disasters, and to identify any additional information that should be included in the plan to comply with NIST SP 800-34; NIST SP 800-53 REV. 4: CP-3 and CP-4; FY 2021 CIO FISMA Metrics, Section 5; CSF: ID.SC-5 and CSF: PR.IP-10.

The Denali Commission completed corrective actions for the recommendation listed above. See Appendix B for more details on the status of these corrective actions.

Results

The Denali Commission’s information security program is assessed overall at the Level 2, Defined, maturity level. Table 2 specifies the maturity level for each function area and the associated domains.

Table 2: Maturity level of reviewed Denali Commission function areas and domains

Function area	Domain	Overall OIG-assessed maturity level
Identify	Risk Management	Level 2, <i>Defined</i>
Identify	Supply Chain Risk Management	Level 2, <i>Defined</i>
Protect	Configuration Management	Level 2, <i>Defined</i>
Protect	Identity and Access Management	Level 2, <i>Defined</i>
Protect	Data Protection and Privacy	Level 2, <i>Defined</i>
Protect	Security Training	Level 2, <i>Defined</i>
Detect	Information Security Continuous Monitoring	Level 2, <i>Defined</i>
Respond	Incident Response	Level 2, <i>Defined</i>
Recover	Contingency Planning	Level 2, <i>Defined</i>

Source: FY 2023 IG FISMA Reporting Metrics.

In FY 2023, while there were no new recommendations for improvements, the Denali Commission is recommended to continue working on improving their maturity level in each of the five domains.

Conclusion

The Denali Commission would improve and strengthen its cybersecurity program by continuing to work on improving their maturity level in each of the five domains.

Status of Recommendations and Potential Monetary Benefits

RECOMMENDATIONS

Rec. No.	Page No.	Subject	Status¹	Action Official	Planned Completion Date	Potential Monetary Benefits (in \$000s)
		Not applicable				

¹ C = Corrective action completed.

R = Recommendation resolved with corrective action pending.

U = Recommendation unresolved with resolution efforts in progress.

Inspector General

Section Report

2023

Denali Commission

Function 0: Overall

- 0.1 Please provide an overall IG self-assessment rating (Effective/Not Effective)

Effective

- 0.2 Please provide an overall assessment of the agency's information security program. The narrative should include a description of the assessment scope, a summary on why the information security program was deemed effective/ineffective and any recommendations on next steps. Please note that OMB will include this information in the publicly available Annual FISMA Report to Congress to provide additional context for the Inspector General's effectiveness rating of the agency's information security program. OMB may modify the response to conform with the grammatical and narrative structure of the Annual Report.

Although the assessment of the metrics and the overall assessment is at the defined level, the controls are appropriate for an agency of the size of the Denali Commission. Two of the areas in which they are ad hoc are data exfiltration prevention and lack of a trusted internet connection, which is problematic for agencies the size of the Denali Commission in Alaska. There has been continued growth and maturity during FY2023. Denali has reduced the number of ad hoc ratings from 5 in FY2022 to 2 in FY2023 and continued to use the DHS CISA's Continuous Diagnostic and Mitigation (CDM) Program.

Function 1A: Identify - Risk Management

1. To what extent does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public facing websites, and third-party systems), and system interconnections?

Defined (Level 2)

Comments : The Denali Commission has processes and software in place for maintaining a comprehensive and accurate inventory of its inventory systems.

2. To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets (including GFE and Bring Your Own Device (BYOD) mobile devices) connected to the organization's network with the detailed information necessary for tracking and reporting?

Defined (Level 2)

Comments : The Denali Commission has defined a process for using standard data elements/taxonomy to develop and maintain an up-to-date Inventory. The hardware inventory is maintained and is current.

3. To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting?

Defined (Level 2)

Comments : The Denali Commission has defined a process for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of software assets and licenses utilized in the organization's environment with the detailed information necessary for tracking and reporting. The inventory is maintained and is current.

4. To what extent has the organization categorized and communicated the importance/priority of information systems in enabling its missions and business functions, including for high value assets?

Defined (Level 2)

Comments : The Denali Commission has categorized and communicated the importance and priority of its information systems in enabling its missions and business functions, including high value assets, through its Information Security Policy.

5. To what extent does the organization ensure that information system security risks are adequately managed at the organizational, mission/business process, and information system levels?

Defined (Level 2)

Comments : The Denali Commission has policies and procedures defining their risk management strategy and the requirements for performing a risk assessment across the organization, department, and information system levels in its Information Security Policy.

6. To what extent does the organization use an information security architecture to provide a disciplined and structured methodology for managing risk, including risk from the organization's supply chain?

Defined (Level 2)

Comments : The Denali Commission has defined and utilized their security processes, information security systems, personnel, and organizational divisions, showing their alignment with the Denali Commission’s mission and strategic plans for managing risks in its Information Security Policy.

7. To what extent have the roles and responsibilities of internal and external stakeholders involved in cybersecurity risk management processes been defined, communicated, implemented, and appropriately resourced across the organization?
Defined (Level 2)

The Denali Commission has defined the roles and responsibilities of internal and external stakeholders involved in cybersecurity risk management processes and communicated and implemented those roles and responsibilities across the organization through its Information Security Policy.

8. To what extent has the organization ensured that plans of action and milestones (POA&Ms) are used for effectively mitigating security weaknesses?
Defined (Level 2)

Comments : The Denali Commission has defined its use of plans of action and milestones to track the weaknesses to resolution in the areas of vulnerability management, and external audit reports..

9. To what extent does the organization ensure that information about cybersecurity risks is communicated in a timely and effective manner to appropriate internal and external stakeholders?
Defined (Level 2)

Comments : The Denali Commission meets several times a year to discuss cybersecurity threats and records the minutes of the meeting to follow up and make sure the vulnerabilities and risks are addressed. In addition, members of the Denali Commission senior management team receive directives on emergent cybersecurity threats from CISA, evaluates the risk impact on the Denali Commission, and develops appropriate action plans.

10. To what extent does the organization use technology/automation to provide a centralized, enterprise wide (portfolio) view of cybersecurity risk management activities across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards?
Defined (Level 2)

Comments : The Denali Commission has defined how cybersecurity risks are communicated in a timely and effective manner to appropriate internal and external stakeholders. In addition, the Denali Commission has implemented the Continuous Diagnostics and Mitigation (CDM) platform offered by CISA.

- 11.1 Please provide the assessed maturity level for the agency's Identify - Risk Management program.
Defined (Level 2)

Comments : Based on the maturity level of the individual areas within Risk Management, the domain is assessed as “Defined.”

- 11.2 Provide any additional information on the effectiveness (positive or negative) of the organizations risk management program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the risk management program effective?

Based on the maturity level of the individual areas within the Risk Management domain, the domain is assessed as “Defined.” We limited our testing to those questions that would materially change our FY 2022 response. For those metrics whose policies, procedures, and strategies were not documented, we rated the Denali Commission at Level 2, “Defined.” However, we did not test to determine what additional steps the Denali Commission needs to complete to achieve a higher maturity level.

Function 1B: Identify - Supply Chain Risk Management

12. To what extent does the organization use an organization wide SCRM strategy to manage the supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services?
Defined (Level 2)

Comments : The Denali Commission has procedures in place to manage the supply chain risks associated with the acquisition, maintenance, and disposal of systems, system components, and system services through the exclusive use of vendors approved by the GSA (General Services Administration) and BFS (Bureau of Fiscal Services) for hardware and software procurement. These higher-level agencies dictate what, where, and from whom the Commission can purchase assets.

13. To what extent does the organization use SCRM policies and procedures to manage SCRM activities at all organizational tiers?

Defined (Level 2)

Comments : The Denali Commission has procedures in place to manage the supply chain risks associated with the acquisition, maintenance, and disposal of systems, system components, and system services through the exclusive use of vendors approved by the GSA (General Services Administration) and BFS (Bureau of Fiscal Services) for hardware and software procurement. These higher-level agencies dictate what, where, and from whom the Commission can purchase assets.

14. To what extent does the organization ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain requirements?

Defined (Level 2)

Comments : The Denali Commission has tactical SCRM tools in place to monitor key issues that may arise from the Commission's relationship with these vendors and their products. Additionally, the Denali Commission routinely monitors media sources for notification of potential and realized threats within the supply chain.

15. To what extent does the organization ensure that counterfeit components are detected and prevented from entering the organization's systems?

Defined (Level 2)

Comments : The Denali Commission has tactical SCRM tools in place to monitor key issues that may arise from the Commission's relationship with these vendors and their products. Additionally, the Denali Commission routinely monitors media sources for notification of potential and realized threats within the supply chain.

- 16.1 Please provide the assessed maturity level for the agency's Identify - Supply Chain Risk Management program.

Defined (Level 2)

Comments : Based on the maturity level of the individual areas within the Supply Chain Risk Management program, the domain is assessed as "Defined."

- 16.2 Please provide the assessed maturity level for the agency's Identify Function.
Defined (Level 2)

Comments : Based on the maturity level of the individual areas within the Risk Management and Supply Chain Risk Management domains, the Identify function is assessed as “Defined.” We limited our testing to those questions that would materially change our FY 2022 response. Due to the “Defined” status for the Identify function, we did not test to determine what additional steps the Denali Commission needs to complete to achieve a higher maturity level.

- 16.3 Provide any additional information on the effectiveness (positive or negative) of the organizations supply chain risk management program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the risk management program effective?

The Denali Commission utilizes GSA and BFS for its SCRM strategy. Additionally, it has tactical SCRM tools in place to monitor key issues that may arise from the Commission’s relationship with vendors and their products. Furthermore, the Denali Commission routinely monitors media sources for notification of potential and realized threats within the supply chain. The risk management program is effective based upon the controls in place for an agency the size of the Denali Commission.

Function 2A: Protect - Configuration Management

17. To what extent have the roles and responsibilities of configuration management stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced?
Defined (Level 2)

Comments : The Denali Commission has defined the roles and responsibilities of configuration management stakeholders and communicated them across the agency in the Information Security Policy – Configuration Management Section.

18. To what extent does the organization use an enterprise wide configuration management plan that includes, at a minimum, the following components: roles and responsibilities, including establishment of a Change Control Board (CCB) or related body; configuration management processes, including processes for: identifying and managing configuration items during the appropriate

phase within an organization's SDLC; configuration monitoring; and applying configuration management requirements to contractor operated systems?

Defined (Level 2)

Comments : The Denali Commission has defined, in the Configuration Management Section of the Information Security Policy, an enterprise-wide configuration plan that contains the components as required by NIST, including roles and responsibilities; configuration management processes; configuration monitoring; and applying configuration management requirements to contractor operated systems.

19. To what extent does the organization use baseline configurations for its information systems and maintain inventories of related components at a level of granularity necessary for tracking and reporting?

Defined (Level 2)

Comments : The Denali Commission utilizes baseline configurations for its information systems and maintains inventories of related components for tracking and reporting.

20. To what extent does the organization use configuration settings/common secure configurations for its information systems?

Defined (Level 2)

Comments : The Denali Commission utilizes baseline configurations for its information systems.

21. To what extent does the organization use flaw remediation processes, including asset discovery, vulnerability scanning, analysis, and patch management, to manage software vulnerabilities on all network addressable IP- assets?

Defined (Level 2)

Comments: The Denali Commission has defined its flaw remediation processes, including patch management, to manage software vulnerabilities in the Configuration Management section of its Information Security Policy. Additionally, a POA&M is used to track vulnerabilities identified and a ticketing system is used to track changes.

22. To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network?

Ad Hoc (Level 1)

Comments: The Denali Commission has extended the RFP multiple times, seeking a contract with a vendor who could provide the necessary infrastructure required to meet this requirement. No bids have been received.

23. To what extent has the organization defined and implemented configuration change control activities including: determination of the types of changes that are configuration controlled; review and approval/disapproval of proposed changes with explicit consideration of security impacts and security classification of the system; documentation of configuration change decisions; implementation of approved configuration changes; retaining records of implemented changes; auditing and review of configuration changes; and coordination and oversight of changes by the CCB, as appropriate?

Defined (Level 2)

Comments: The Denali Commission has defined its configuration control activities including the types of changes to be controlled, the approval process, documentation of changes, and the implementation approval process. Additionally, a risk analysis and vulnerability scan is performed post-implementation.

24. To what extent does the organization use a vulnerability disclosure policy (VDP) as part of its vulnerability management program for internet- accessible federal systems?

Defined (Level 2)

Comments: The Denali Commission has developed and deployed a Vulnerability Disclosure Policy to their forward-facing websites.

- 25.1 Please provide the assessed maturity level for the agency's Protect - Configuration Management program.

Defined (Level 2)

Comments: Based on the maturity level of the individual areas within the Configuration Management program, the domain is assessed as "Defined."

- 25.2 Provide any additional information on the effectiveness (positive or negative) of the organizations configuration management program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the configuration management program effective?

Based on the maturity level of the individual areas within Configuration Management, the domain is assessed as "Defined." We limited our testing to those questions with criteria added to the metric that

would materially change our FY 2022 response. If the policies, procedures, and strategies were documented, we rated the Denali Commission at Level 2, "Defined." However, we did not test to determine what additional steps the Denali Commission needs to complete to achieve a higher maturity level.

Function 2B: Protect - Identity and Access Management

26. To what extent have the roles and responsibilities of identity, credential, and access management (ICAM) stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced?

Defined (Level 2)

Comments: The roles and responsibilities for Identity, Credential, And Access Management (ICAM) have been defined, communicated, and implemented across the Denali Commission as well as being appropriately resourced.

27. To what extent does the organization use a comprehensive ICAM policy, strategy, process, and technology solution roadmap to guide its ICAM processes and activities?

Defined (Level 2)

Comments: The Denali Commission utilizes a comprehensive ICAM policy, strategy, process, and technology solution roadmap to guide its ICAM processes and activities using positional risk assessment and screening, non-disclosure agreements for all employees and vendors who access the system, acceptable use policies, and multi-factor authentication.

28. To what extent has the organization developed and implemented processes for assigning position risk designations and performing appropriate personnel screening prior to granting access to its systems?

Defined (Level 2)

Comments: The Denali Commission has developed and implemented processes for assigning position risk designations and performing appropriate personnel screening prior to granting access to the systems. A positional risk posture assessment is performed annually by the CIO and each new employee must undergo and pass a comprehensive background check prior to being granted access to the system.

29. To what extent does the organization ensure that access agreements, including nondisclosure agreements, acceptable use agreements, and rules of behavior, as appropriate, for individuals (both privileged and non-privileged users) that access its systems are completed and maintained?

Defined (Level 2)

Comments: The Denali Commission has defined its processes for developing, documenting, and maintaining nondisclosure agreements for individuals that access its systems. Acceptable use banners are displayed each time a user logs on to the system.

30. To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (e.g., PIV, FIDO or web authentication) for non-privileged users to access the organization's facilities [organization-defined entry/exit points], networks, and systems, including for remote access?

Defined (Level 2)

Comments: The Denali Commission and its technology vendor use various technology solutions to connect to and perform privileged actions on their network.

31. To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (e.g., PIV, FIDO or web authentication) for privileged users to access the organization's facilities [organization-defined entry/exit points], networks, and systems, including for remote access?

Defined (Level 2)

Comments : The Denali Commission and its technology vendor use various technology solutions to connect to and perform privileged actions on their network.

32. To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed?

Defined (Level 2)

Comments: The Denali Commission has defined procedures for the provisioning and management of privileged accounts. All privileged accounts must be reviewed and approved by the Federal Co Chair. In addition, the Federal Co Chair is

responsible for periodically reviewing the access permissions for privileged accounts.

33. To what extent does the organization ensure that appropriate configuration/connection requirements are maintained for remote access connections? This includes the use of appropriate cryptographic modules, system time-outs, and the monitoring and control of remote access sessions?

Defined (Level 2)

Comments : All remote access to Denali Commission systems for staff is performed through a secured and encrypted gateway. This system is included in the recurring HTTPS scans to make sure it is not using weak ciphers or protocols.

- 34.1 Please provide the assessed maturity level for the agency's Protect - Identity and Access Management program.

Defined (Level 2)

Comments: Based on the maturity level of the individual areas within the Identity and Access Management program, the domain is assessed as "Defined."

- 34.2 Provide any additional information on the effectiveness (positive or negative) of the organizations identity and access management program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the identity and access management program effective?

Based on the maturity level of the individual areas within Identity and Access Management, the domain is assessed as "Defined." We limited our testing to those questions with criteria added to the metric that would materially change our FY 2022 response. For those metrics whose policies, procedures, and strategies were documented, we rated the Denali Commission at Level 2, "Defined." However, we did not test to determine what additional steps the Denali Commission needs to complete to achieve a higher maturity level.

Function 2C: Protect - Data Protection and Privacy

35. To what extent has the organization developed a privacy program for the protection of personally identifiable information (PII) that is collected, used, maintained, shared, and disposed of by information systems?

Defined (Level 2)

Comments: The Denali Commission has developed a privacy program that identifies personally identifiable information (PII), its retention, disposal, and disclosure.

36. To what extent has the organization implemented the following security controls to protect its PII and other agency sensitive data, as appropriate, throughout the data lifecycle?
- Encryption of data at rest
 - Encryption of data in transit
 - Limitation of transfer to removable media
 - Sanitization of digital media prior to disposal or reuse.

Defined (Level 2)

Comments: The Denali Commission has implemented encryption of data in transit and data at rest including laptops and workstations. The Denali Commission contracts with a technology vendor to perform the sanitization of digital media. However, the limitation of transfer to removable media has not been defined.

37. To what extent has the organization implemented security controls (e.g., EDR) to prevent data exfiltration and enhance network defenses?

Ad Hoc (Level 1)

Comments: The Denali Commission is researching potential solutions that enable data exfiltration controls. The Commission will evaluate the technology, the budget, and the potential to complete this in the future as resources are available.

38. To what extent has the organization developed and implemented a Data Breach Response Plan, as appropriate, to respond to privacy events?

Defined (Level 2)

Comments: The Denali Commission has defined and communicated its Data Breach Response Plan, including its processes and procedures for data breach notification. A breach response team has been established that includes the appropriate agency officials.

39. To what extent does the organization ensure that privacy awareness training is provided to all individuals, including role-based privacy training?(Note: Privacy awareness training topics should include, as appropriate: responsibilities under the

Privacy Act of and E- Government Act of 20 consequences for failing to carry out responsibilities, identifying privacy risks, mitigating privacy risks, and reporting privacy incidents, data collections and user requirements)

Defined (Level 2)

Comments: The Denali Commission requires all employees to take privacy awareness training as part of the required annual security awareness training. Employees completed the Cyber Awareness challenge in FY 2023 which includes training reinforcing best practices to protect classified, controlled unclassified information (CUI), and personally identifiable information (PII).

40.1 Please provide the assessed maturity level for the agency's Protect - Data Protection and Privacy program.

Defined (Level 2)

Comments: Based on the maturity level of the individual areas within the Data Protection and Privacy program, the domain is assessed as “Defined.”

40.2 Provide any additional information on the effectiveness (positive or negative) of the organizations data protection and privacy program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the data protection and privacy program effective?

Based on the maturity level of the individual areas within the Data Protection and Privacy the domain is assessed as “Defined.” We limited our testing to those questions with criteria added to the metric that would materially change our FY 2022 response. For those metrics whose policies, procedures, and strategies were documented, we rated the Denali Commission at Level 2, "Defined." However, we did not test to determine what additional steps the Denali Commission needs to complete to achieve a higher maturity level.

Function 2D: Protect - Security Training

41. To what extent have the roles and responsibilities of security awareness and training program stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced? Note: This includes the roles and responsibilities for the effective establishment and maintenance of an organization wide security awareness and training program as well as the awareness and training related roles and responsibilities of system users and those with significant security responsibilities.

Consistently Implemented (Level 3)

Comments: The Denali Commission has processes in place to provide security training to Commission personnel. Evidence of completion certificates for a selection of employees was provided.

42. To what extent does the organization use an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of: identify, protect, detect, respond, and recover?

Defined (Level 2)

Comments: The Denali Commission conducts an annual security assessment for all staff who have access to organizational information systems. This assessment provides objective measurements as to staff understanding of Commission policies, procedures, and plans related to everyone's role in the organization. The assessment will reflect current threats and appropriate staff responses.

43. To what extent does the organization use a security awareness and training strategy/plan that leverages its skills assessment and is adapted to its mission and risk environment? Note: The strategy/plan should include the following components:

 The structure of the awareness and training program

 Priorities

 Funding

 The goals of the program

 Target audiences

 Types of courses/ material for each audience

 Use of technologies (such as email advisories, intranet updates/wiki pages/social media, web- based training, phishing simulation tools)

 Frequency of training

 Deployment methods

Defined (Level 2)

Comments: The Denali Commission has defined its security awareness and training strategy/plan that is adapted to its mission and risk environment. The Denali Commission conducts an annual security assessment for all staff who have access to organizational information systems and assigns training to employees based on this assessment.

44. To what extent does the organization ensure that security awareness training is provided to all system users and is tailored based on its mission, risk environment, and types of information systems? (Note: awareness training topics should include, as appropriate: consideration of organizational policies, roles and responsibilities, secure e-mail, browsing, and remote access practices, mobile device security, secure use of social media, phishing, malware, physical security, and security incident reporting?)

Defined (Level 2)

Comments: The Denali Commission provides security awareness training to all system users. The training is tailored based on the Commission’s mission, risk environment, and types of information systems. Any employee not achieving satisfactory completion must be retrained and reassessed until that person satisfies requirements. Upon training completion staff permissions to the systems will be restored. Any employee who repeatedly violates security policies or procedures must be subject to retraining and/or disciplinary actions.

45. To what extent does the organization ensure that specialized security training is provided to individuals with significant security responsibilities (as defined in the organization’s security policies and procedures and in accordance with 5 Code of Federal Regulation 930.301)?

Defined (Level 2)

Comments: The Denali Commission evaluates the need for staff assigned to crucial information security roles to receive additional security training based upon their respective roles within the organization. This training may consist of conferences, webinars, vendor training, academic education, and other training opportunities.

- 46.1 Please provide the assessed maturity level for the agency's Protect - Security Training program.

Defined (Level 2)

Comments: Based on the maturity level of the individual areas within the Security Training program, the domain is assessed as “Defined.”

- 46.2 Please provide the assessed maturity level for the agency's Protect Function.

Defined (Level 2)

Comments: Based on the maturity level of the individual areas within the Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training domains , the Protect function is assessed as “Defined.”

- 46.3 Provide any additional information on the effectiveness (positive or negative) of the organizations security training program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the security training program effective?

Based on the maturity level of the individual areas within the Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training domains, the Protect function is

assessed as “Defined.” We limited our testing to those questions with criteria added to the metric that would materially change our FY 2022 response. For those metrics whose policies, procedures, and strategies were documented, we rated the Denali Commission at Level 2, “Defined.” However, we did not test to determine what additional steps the Denali Commission needs to complete to achieve a higher maturity level.

Function 3: Detect - ISCM

47. To what extent does the organization use information security continuous monitoring (ISCM) policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier?

Defined (Level 2)

Comments: The Denali Commission continues to use the Continuous Diagnostics and Mitigation Program (CDM) with the Cybersecurity and Infrastructure Security Agency (CISA). The program provides asset management, identity and access management, network security management, data protection management, and dashboards to monitor risk.

48. To what extent have ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies been defined, communicated, and implemented across the organization?

Defined (Level 2)

Comments: The Denali Commission has defined the ISCM stakeholders as well as their roles and responsibilities and communicated them across the organization in the Information Security and Continuous Monitoring section of the Information Security Policy.

49. How mature are the organization’s processes for performing ongoing information system assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring system security controls?

Defined (Level 2)

Comments: The Denali Commission has policies for performing on going assessments and granting system authorizations. In addition, the Denali Commission continues to use the Continuous Diagnostics and Mitigation Program (CDM) with the Cybersecurity and Infrastructure Security Agency (CISA).

50. How mature is the organization's process for collecting and analyzing ISCM performance measures and reporting findings?

Defined (Level 2)

Comments: The Denali Commission continues to use the Continuous Diagnostics and Mitigation Program (CDM) with the Cybersecurity and Infrastructure Security Agency (CISA). The program network security management and dashboards to monitor risk.

- 51.1 Please provide the assessed maturity level for the agency's Detect - ISCM function.

Defined (Level 2)

Comments: Based on the maturity level of the individual areas within the Detect – ISCM function, the domain/function is assessed as “Defined.”

- 51.2 Provide any additional information on the effectiveness (positive or negative) of the organizations ISCM program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the ISCM program effective?

Based on the maturity level of the individual areas within Detect - ISCM, the domain/function is assessed as “Defined.” We limited our testing to those questions with criteria added to the metric that would materially change our FY 2022 response. For those metrics whose policies, procedures, and strategies were documented, we rated the Denali Commission at Level 2, "Defined." However, we did not test to determine what additional steps the Denali Commission needs to complete to achieve a higher maturity level.

Function 4: Respond - Incident Response

52. To what extent does the organization use an incident response plan to provide a formal, focused, and coordinated approach to responding to incidents?

Defined (Level 2)

Comments: The Denali Commission's Incident Response Plan is formally documented and contains a focused and coordinated approach to responding to incidents.

53. To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined, communicated, and implemented across the organization?

Defined (Level 2)

Comments: The Denali Commission's Incident Response Plan contains a list of incident response team stakeholders and their roles and responsibilities, which have been shared across the organization.

54. How mature are the organization's processes for incident detection and analysis?

Defined (Level 2)

Comments: The Denali Commission has defined its processes for detecting and analyzing incidents, including the types of precursors and indicators and how they are generated and reviewed, as well as the prioritization of incidents. In addition, the Denali Commission has defined tabletop exercises to be performed to rehearse for potential incidents.

55. How mature are the organization's processes for incident handling?

Defined (Level 2)

Comments: The Denali Commission has defined its processes for incident handling to include containment strategies for various types of major incidents, eradication activities to eliminate components of an incident, mitigation of any vulnerabilities that were exploited, and recovery of systems.

56. To what extent does the organization ensure that incident response information is shared with individuals with significant security responsibilities and reported to external stakeholders in a timely manner?

Defined (Level 2)

Comments: The Denali Commission has defined its requirements for personnel to report suspected security incidents to the Commission's incident response team within organization defined timeframes. In addition, the Denali Commission has defined its processes for reporting security incident information to US-CERT, law enforcement, the Congress (for major incidents) and the Office of Inspector General, as appropriate.

57. To what extent does the organization collaborate with stakeholders to ensure on-site, technical assistance/surge capabilities can be leveraged for quickly responding to incidents, including through contracts/agreements, as appropriate, for incident response support?

Defined (Level 2)

Comments: If additional support is required during the incident response efforts, the Denali Commission has defined a list of authorities to contact for additional assistance, including DHS, the Federal Bureau of Investigation, and other parties, as appropriate, to provide on-site, technical assistance/surge resources/special capabilities for quickly responding to incidents. In addition to the specified authorities, the Denali Commission has also specified third party contacts that can be contacted for additional support, including their IT vendor, cybersecurity insurance provider, and others.

58. To what extent does the organization use the following technology to support its incident response program?

- Web application protections, such as web application firewalls
- Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools
- Aggregation and analysis, such as security information and event management (SIEM) products
- Malware detection, such as antivirus and antispam software technologies
- Information management, such as data loss prevention
- File integrity and endpoint and serversecurity tools

Defined (Level 2)

Comments: The Denali Commission has identified and fully defined its requirements for the incident response technologies it plans to utilize in the specified areas. The Denali Commission continues to use the Cybersecurity and Infrastructure Security Agency’s (CISA) Continuous Diagnostics and Mitigation Program (CDM) which will monitor events across the entire Denali Commission.

- 59.1 Please provide the assessed maturity level for the agency's Respond - Incident Response function.

Defined (Level 2)

Comments: Based on the maturity level of the individual areas within the Respond – Incident Response function , the domain/function is assessed as “Defined.”

- 59.2 Provide any additional information on the effectiveness (positive or negative) of the organizations incident response program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the incident response program effective?

Based on the maturity level of the individual areas within Respond – Incident Response, the domain function is assessed as “Defined.” We limited our testing to those questions with criteria added to the metric that would materially change our FY 2022 response. For those metrics whose policies, procedures, and strategies were documented, we rated the Denali Commission at Level 2, "Defined." However, we did not test to determine what additional steps the Denali Commission needs to complete to achieve a higher maturity level.

Function 5: Recover - Contingency Planning

60. To what extent have roles and responsibilities of stakeholders involved in information systems contingency planning been defined, communicated, and implemented across the organization, including appropriate delegations of authority?

Defined (Level 2)

Comments: The Denali Commission has defined and communicated across the organization the roles and responsibilities of stakeholders involved in information systems contingency planning.

61. To what extent does the organization ensure that the results of business impact analyses (BIA) are used to guide contingency planning efforts?

Defined (Level 2)

Comments: The Denali Commission incorporates the results of business impact analyses of business functions in the Business Continuity Plan and are used to guide contingency planning efforts.

62. To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans?

Defined (Level 2)

Comments: The Denali Commission has defined processes for the information system contingency plan development and

maintenance in the Information Security Policy. The contingency plan has been developed as part of the Information Security Policy and is used in conjunction with the Incident Response Plan to address disruption to operations. A separate Business Impact Analysis has been developed and policies and procedures require that it be reviewed and updated annually.

63. To what extent does the organization perform tests/exercises of its information system contingency planning processes?
Defined (Level 2)

Comments: The Contingency Plan specifies that the contingency plan be tested annually using tabletop exercises. A tabletop exercise was performed in May 2023 using the Contingency and Incident Response Plans as a roadmap. In addition, the exercise was conducted using one of several predefined scenarios.

64. To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate?
Defined (Level 2)

Comments: The Denali Commission has processes and procedures in place to perform backup and storage, including offsite storage for the Denali Commission's data.

65. To what level does the organization ensure that information on the planning and performance of recovery activities is communicated to internal stakeholders and executive management teams and used to make risk-based decisions?
Defined (Level 2)

Comments: The Denali Commission has defined how the planning and performance of recovery activities are communicated to internal stakeholders and executive management teams in the Incident Response Plan.

- 66.1 Please provide the assessed maturity level for the agency's Recover - Contingency Planning function.
Defined (Level 2)

Comments: Based on the maturity level of the individual areas within the Recover – Contingency Planning function, the domain/function is assessed as “Defined.”

- 66.2 Provide any additional information on the effectiveness (positive or negative) of the organizations contingency planning program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the contingency program effective? **Based on the maturity level of the individual areas within Recover – Contingency Planning, the domain function is assessed as “Defined.” We limited our testing to those questions with criteria added to the metric that would materially change our FY 2022 response. For those metrics whose policies, procedures, and strategies were documented, we rated the Denali Commission at Level 2, “Defined.” However, we did not test to determine what additional steps the Denali Commission needs to complete to achieve a higher maturity level.**

APPENDIX A: Maturity Model Scoring

A.1 Please provide the assessed maturity level for the agency's Overall status.

Function	Core	FY23 Supplemental	FY24 Supplemental	FY23 Assessed Maturity	FY23 Effectiveness	Explanation
Identify	2.00	2.00	2.00	Defined (Level 2)	Effective	
Protect	1.88	2.00	2.00	Defined (Level 2)	Effective	
Detect	2.00	2.00	2.00	Defined (Level 2)	Effective	
Respond	2.00	2.00	2.00	Defined (Level 2)	Effective	
Recover	2.00	2.00	2.00	Defined (Level 2)	Effective	
Overall Maturity	1.98	2.00	2.00	Defined (Level 2)	Effective	

Function 1A: Identify – Risk Management

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	5	3
Consistently Implemented (Level 3)	0	0
Managed and Measurable (Level 4)	0	0
Optimized (Level 5)	0	0
Calculated Rating:	2.00	2.00

Function 1B: Identify – Supply Chain Risk Management

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	1	2
Consistently Implemented (Level 3)	0	0
Managed and Measurable (Level 4)	0	0
Optimized (Level 5)	0	0
Calculated Rating:	2.00	2.00

Function 2A: Protect – Configuration Management

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	1
Defined (Level 2)	2	2
Consistently Implemented (Level 3)	0	0
Managed and Measurable (Level 4)	0	0
Optimized (Level 5)	0	0
Calculated Rating:	2.00	1.67

Function 2B: Protect – Identity and Access Management

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	3	4
Consistently Implemented (Level 3)	0	0
Managed and Measurable (Level 4)	0	0
Optimized (Level 5)	0	0
Calculated Rating:	2.00	2.00

Function 2C: Protect – Data Protection and Privacy

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	1	0
Defined (Level 2)	1	1
Consistently Implemented (Level 3)	0	0
Managed and Measurable (Level 4)	0	0
Optimized (Level 5)	0	0
Calculated Rating:	1.50	2.00

Function 2D: Protect – Security Training

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	1	1
Consistently Implemented (Level 3)	0	1
Managed and Measurable (Level 4)	0	0
Optimized (Level 5)	0	0
Calculated Rating:	2.00	2.50

Function 3: Detect – ISCM

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	2	1
Consistently Implemented (Level 3)	0	0
Managed and Measurable (Level 4)	0	0
Optimized (Level 5)	0	0
Calculated Rating:	2.00	2.00

Function 4: Respond – Incident Response

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	2	2
Consistently Implemented (Level 3)	0	0
Managed and Measurable (Level 4)	0	0
Optimized (Level 5)	0	0
Calculated Rating:	2.00	2.00

Function 5: Recover – Contingency Planning

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	2	2
Consistently Implemented (Level 3)	0	0
Managed and Measurable (Level 4)	0	0
Optimized (Level 5)	0	0
Calculated Rating:	2.00	2.00

Appendix B

Status of the Denali Commission Corrective Actions for FY 2021 FISMA Audit Recommendations

The below table details the OIG’s analysis of the corrective actions that the Denali Commission has implemented for the recommendations issued in the FY 2021 FISMA Report.

Recommendation		Corrective Action	OIG Analysis Of Corrective Action Status
1	Test the Contingency Plan annually to allow the Commission to effectively respond to incidents and disasters, and to identify any additional information that should be included in the plan to comply with NIST SP 800-34; NIST SP 800-53 REV. 4: CP-3 and CP-4; FY 2021 CIO FISMA Metrics, Section 5; CSF: ID.SC-5 and CSF: PR.IP-10.	Implemented The Contingency Plan specifies that the contingency plan be tested annually using tabletop exercises. A tabletop exercise was performed in May 2023 using the Contingency and Incident Response Plans as a roadmap. In addition, the exercise was conducted using one of several predefined scenarios.	Closed – Corrective action completed.