Denali Commission

Results of the Evaluation of the FY 2021 Denali Commission Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics

FINAL REPORT
December 22, 2021
Report No. 2021.12.22
Denali Commission
Office of Inspector General

FY 2021 Denali Commission
Federal Information Security Modernization
Act of 2014 (FISMA) Reporting Metrics

Table of Contents

Appendices

SB & COMPANY, LLC
KNOWLEDGE • QUALITY • CLIENT SERVICE

Independent Accountants' Report

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) 2021 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, 2020, to September 30, 2021. 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 2021 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 2021 FISMA metrics were rated Defined (Level 2).

SB & 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, DC
December 22, 2021

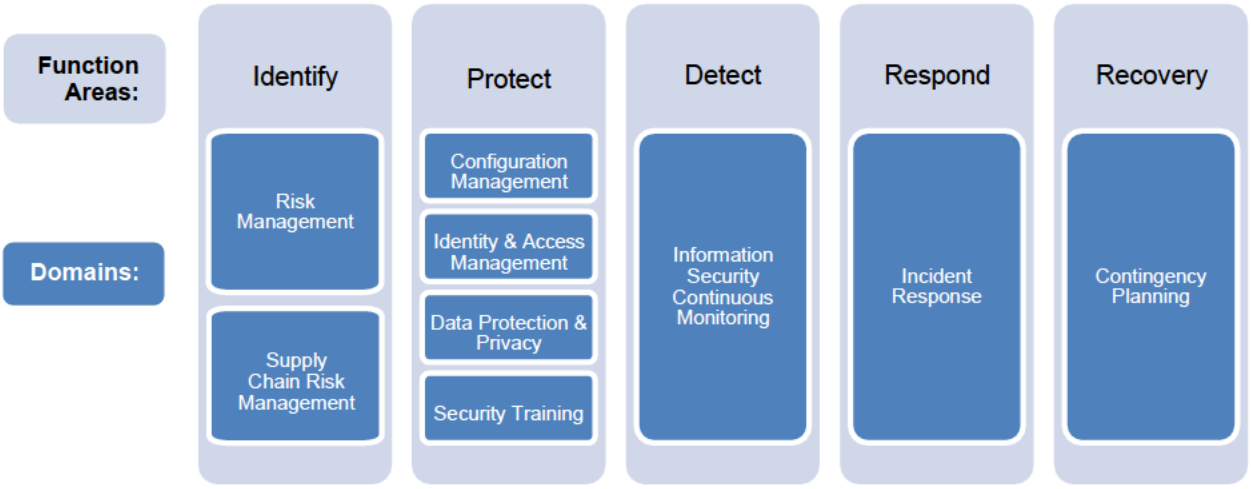
SB & Company, LLC

Background

Under 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 2021 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 2021 cybersecurity framework security function areas and domains



Source: OIG-created graphic based on *FY 2021 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 eight 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 Reporting Metrics* template.

[1] *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics,* Version 1.1, dated May 12, 2021. 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.

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 2021 IG FISMA Reporting Metrics*.

Scope and Methodology

We conducted this evaluation audit from June to October 2021 in accordance with 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 2021 IG FISMA Reporting Metrics*. We conducted a risk assessment of the FY 2021 IG FISMA metrics to determine whether changes made to the underlying criteria of the FISMA metric questions significantly changed since the FY 2020 evaluation.

We also evaluated the new FY 2021 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 2020 audit for the identified metric question.

- Low Risk—The Denali Commission made no significant changes to its information security program since the FY 2020 audit for the identified metric question.

We relied on the responses to the FY 2020 Denali Commission FISMA metric questions to answer the FY 2021 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 2021 IG FISMA Reporting Metrics*.

Appendix A provides the OIG response to each FISMA metric, as submitted to the Office of Management and Budget on October 25, 2021.

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, *Defined*
Identify	Supply Chain Risk Management	Level 1, *Ad-Hoc*
Protect	Configuration Management	Level 2, *Defined*
Protect	Identity and Access Management	Level 2, *Defined*
Protect	Data Protection and Privacy	Level 2, *Defined*
Protect	Security Training	Level 2, *Defined*
Detect	Information Security Continuous Monitoring	Level 2, *Defined*
Respond	Incident Response	Level 2, *Defined*
Recover	Contingency Planning	Level 2, *Defined*

Source: *FY 2021 IG FISMA Reporting Metrics.*

However, in FY 2021, the Denali Commission continued to need improvements for a specific question in the "Configuration Management," domain, as shown in Table 3.

Table 3: Denali Commission domains that require further improvement

Function area	Domain	FISMA questions that need improvement
Identify	Risk Management	The Denali Commission meets through the year to discuss cybersecurity risks and vulnerabilities and records the items to be followed up on, however they are not using plans of action and milestones (PO&AMs) to track the weaknesses to resolution *See Appendix A, FISMA Question 8.*
Protect	Identity and Access Management	The Denali Commission has not defined its processes for provisioning, managing, and reviewing privileged accounts. No defined processes cover approval and tracking, inventorying, and validating, and logging and reviewing privileged users' accounts. *See Appendix A, FISMA Question 32.*
Protect	Data Protection and Privacy	The Denali Commission has not provided support to show that Denali has defined and communicated its Data Breach Response Plan, including its processes and procedures for data breach notification. Further, a breach response team has not been established that includes the appropriate agency officials. *See Appendix A, FISMA Question 38.*

Function area	Domain	FISMA questions that need improvement
Recover	Contingency Planning	The Denali Commission's contingency plan specifies that the contingency plan be tested annually using tabletop exercises However, evidence that the exercises have been performed in the last twelve months has not been provided. *See Appendix A, FISMA Question 63.*

Source: SBC Recap

Conclusion

The Denali Commission would improve and strengthen its cybersecurity program through the utilization of Plans of Actions and Milestones (PO&AMs) to track and mitigate security weaknesses. Using PO&AMs will allow the Commission to effectively manage the mitigation of security weaknesses.

The Denali Commission would improve and strengthen its cybersecurity program through the development of procedures to appropriately provision and manage privileged user accounts. Appropriate provisioning procedures for privileged accounts will ensure that only authorized users have escalated permissions to access the organization's systems and aid in the prevention of theft of the agency's data or a disruption to its ongoing operations.

The Denali Commission would improve and strengthen its cybersecurity program through the development and deployment of a Data Breach Response Plan. A Data Breach Response Plan will allow the agency to respond effectively and efficiently in the event of a data breach.

The Denali Commission would improve and strengthen its cybersecurity program through the periodic testing of its contingency plan. Periodic testing of the contingency plan will allow the agency to effectively respond to incidents and disasters. Additionally, it will allow the agency to identify potential additions or revisions that should be included in the plan to increase its effectiveness.

Recommendations

We recommend that the Denali Commission:

1. Develop and deploy policies and procedures necessary to effectively use PO&AMs to track and mitigate security weaknesses to comply with NIST SP 800-53 Rev. 4: CA-5; NIST SP 800-37 (Rev. 2) Task A-6, R-3; OMB M-04-14, M-19-03, CSF v1.1, ID.RA-6.

2. Develop procedures to appropriately provision and manage privileged user accounts to comply with FY 2021 CIO FISMA Metrics: 2.3, 2.5, 2.6, and 2.7; OMB M-19-17, NIST SP 800-53 REV. 4: AC-1, AC-2, AC-5, AC-6, AC-17; AU-2, AU-3, AU-6, and IA-4; DHS ED 19-01; CSF: PR.AC-4.

3. Develop a Data Breach Response Plan to respond to potential data breaches more effectively and efficiently to comply with (NIST SP 800-122; NIST SP 800-53 REV. 4: Appendix J, SE-2; FY 2020 SAOP FISMA metrics, Section 12; OMB M-17-12; and OMB M-17-25.

4. 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.

Denali Commission Response and Procedures Performed

The Denali Commission concurs and accepts the recommendations. An update to the policy will address the use of PO&AMs to track and mitigate security weaknesses with an anticipated corrective action completion date of April 2022. This date is dependent upon timely contract modification establishing contractor's response and barring any unforeseen events.

The Denali Commission concurs and accepts the recommendations. A timeline to discuss and implement procedures to appropriately provision and manage privileged user accounts will be established, and progress monitored. Management anticipates a completion date of June 2022. This date is dependent upon timely contract modification establishing contractor's response and barring any unforeseen events.

The Denali Commission concurs and accepts the recommendations. A timeline to discuss and develop a Data Breach Response Plan will be established, and progress monitored. Management anticipates a completion date of June 2022. This date is dependent upon timely contract modification establishing contractor's response and barring any unforeseen events.

The Denali Commission concurs and accepts the recommendations. A timeline to discuss and implement contingency plan testing will be established, progress monitored, and testing scheduled. Management anticipates a completion date of June 2022. This date is dependent upon timely contract modification establishing contractor's response and barring any unforeseen events.

Status of Recommendations and Potential Monetary Benefits

RECOMMENDATIONS

Rec. No.	Page No.	Subject	Status[1]	Action Official	Planned Completion Date	Potential Monetary Benefits (in $000s)
1	10	Develop and deploy policies and procedures necessary to effectively use PO&AMs to track and mitigate security weaknesses to comply with NIST SP 800-53 Rev. 4: CA-5; NIST SP 800-37 (Rev. 2) Task A-6, R-3; OMB M-04-14, M-19-03, CSF v1.1, ID.RA-6.	U	Chairperson	April 2022	
2	10	Develop procedures to appropriately provision and manage privileged user accounts to comply with FY 2021 CIO FISMA Metrics: 2.3, 2.5, 2.6, and 2.7; OMB M-19-17, NIST SP 800-53 REV. 4: AC-1, AC-2, AC-5, AC-6, AC-17; AU-2, AU-3, AU-6, and IA-4; DHS ED 19-01; CSF: PR.AC-4.	U	Chairperson	June 2022	
3	10	Develop a Data Breach Response Plan to respond to potential data breaches more effectively and efficiently to comply with (NIST SP 800-122; NIST SP 800-53 REV. 4: Appendix J, SE-2; FY 2020 SAOP FISMA metrics, Section 12; OMB M-17-12; and OMB M-17-25.	U	Chairperson	June 2022	
4	10-11	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.	U	Chairperson	June 2022	

[1] C = Corrective action completed.
R = Recommendation resolved with corrective action pending.
U = Recommendation unresolved with resolution efforts in progress.

Inspector General

Section Report

2021

IG Annual

Denali Commission

Function 0: Overall

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

Not 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.
The reason it was assessed at this level is because this is a micro-agency not previously subject to all of the requirements of FISMA. It is not effective because the overall level is Defined. The agency has improved from ad hoc to defined in one fiscal year.

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 (NIST SP 800-53. Rev. 4: CA-3, PM-5, and CM-8; NIST Cybersecurity Framework (CSF): ID.AM-1 - 4; FY 2021 CIO FISMA Metrics: 1.1, 1.1.5 and 1.4, OMB A-130, NIST SP 800-37, Rev. 2: Task P-18).
Defined (Level 2)
Comments: The Denali Commission has processes and software in place for maintaining inventory systems, across software and hardware. From taxonomy perspective, all inventory reports include at minimum, computer ID, agent last contact date, agent name, agent type, agent status, agent serial number and agent asset tag. Additionally, the Commission retains an inventory of its public facing websites.

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 (NIST SP 800-53 Rev. 4: CA-7 and CM-8; NIST SP 800-137; NIST IR 8011; Federal Enterprise Architecture (FEA) Framework, v2; FY 2021 CIO FISMA Metrics: 1.2, 1.3, 2.2, 3.9, CSF: ID.AM-1; NIST SP 800-37, Rev. 2: Task P-10).
Defined (Level 2)
Comments: Based on the review of the reports for the Denali Commission's server and workstation inventory, the Commission

uses standard data elements/taxonomy to develop and maintain an inventory of hardware assets. All inventory reports include at minimum, computer ID, agent last contact date, agent name, agent type, agent status, agent serial number and agent asset tag.

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 (NIST SP 800-53 Rev. 4: CA-7, CM-8, and CM-10; NIST SP 800-137; NIST IR 8011; FEA Framework, v2; FY 2021 CIO FISMA Metrics: 1.2.5, 1.3.3, 1.3.9, 1.3.10, 3.10; CSF: ID.AM-2; NIST SP 800-37, Rev. 2: Task P-10)?
Defined (Level 2)
Comments: The Denali Commission uses

to track licenses.

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 (NIST SP 800-53 Rev. 4: RA-2, PM-7, and PM-11; NIST SP 800-60; NIST SP 800-37 (Rev. 2); CSF: ID.BE-3, ID.AM-5, and ID.SC-2; FIPS 199; FY 2021 CIO FISMA Metrics: 1.1; OMB M-19-03; NIST SP 800-37, Rev. 2: Task C-2, C-3, P-4, P-12, P-13, S-1 – S-3, NIST IR 8170)?
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 (NIST SP 800-39; NIST SP 800-53 Rev. 4: RA-3, PM-9; NIST IR 8286, CSF: ID RM-1 – ID.RM-3; OMB A-123; OMB M-16-17; OMB M-17-25; NIST SP 800-37 (Rev. 2): Tasks P-2, P-3, P-14, R-2, and R-3?
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 utilize an information security architecture to provide a disciplined and structured methodology for managing risk, including risk from the organization's supply chain (Federal Information Technology

Acquisition Reform Act (FITARA), NIST SP 800-39; NIST SP 800-160; NIST SP 800-37 (Rev. 2) Task P-16; OMB M-19-03; OMB M-15-14, FEA Framework; NIST SP 800-53 Rev. 4: PL-8, SA-3, SA-8, SA-9, SA-12, and PM-9; NIST SP 800-163, Rev. 1 CSF: ID.SC-1 and PR.IP-2; SECURE Technology Act: s. 1326)?

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 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, and implemented across the organization (NIST SP 800-39: Section 2.3.1, 2.3.2, and Appendix D; NIST SP 800-53 Rev. 4: RA-1; CSF: ID.AM-6, ID.RM-1, and ID.GV-2; NIST IR 8286, Section 3.1.1, OMB A-123; NIST SP 800-37 (Rev. 2) Section 2.8 and Task P-1; OMB M-19-03)?

Defined (Level 2)

Comments: 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 utilized for effectively mitigating security weaknesses (NIST SP 800-53 Rev. 4: CA-5; NIST SP 800-37 (Rev. 2) Task A-6, R-3; OMB M-04-14, M-19-03, CSF v1.1, ID.RA-6)?

Ad Hoc (Level 2)

Comments: The Denali Commission meets through the year to discuss cybersecurity risks and vulnerabilities and records the items to be followed up on, however they are not using plans of action and milestones to track the weaknesses to resolution.

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 (OMB A-123; OMB Circular A-11 and OMB M-19-03; CSF: Section 3.3; NIST SP 800-37 (Rev. 2) Task M-5; SECURE Technology Act: s. 1326, NIST IR 8170 and 8286)?

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, the Information Security Policy states that an Information Security Status Report will be produced annually. In addition, members of the Denali Commission senior management team receive directives on emergent cybersecurity threats from CISA, evaluates the risk impact on the Commission, and develops appropriate action plans. Email hits all at once.

10. To what extent does the organization utilize 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 (NIST SP 800-39; OMB A-123 and NIST IR 8286)?
Ad Hoc (Level 1)
Comments: The Denali Commission is in the process to license however this relationship has not been finalized.

11.1 Please provide the assessed maturity level for the agency's Identify – Risk Management program.
Defined (Level 1)

11.2 Provide any additional information on the effectiveness (positive or negative) of the organization's 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 and Supply Chain Risk Management domains, the overall maturity level of the Identify function is concluded as "Defined".

Function 1B: Identify – Supply Chain Risk Management

12. To what extent does the organization utilize 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? (The Federal Acquisition Supply Chain Security Act of 2018 (H.R. 7327, 41 USC Chap. 13 Sub chap. III and Chap. 47, P.L. 115-390) (Dec. 21, 2018), NIST SP 800-53, Rev. 5, PM-30, NIST IR 8276)?
Ad Hoc (Level 1)
Comments: The Denali Commission has not yet defined and implemented 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.

13. To what extent does the organization utilize SCRM policies and procedures to manage SCRM activities at all organizational tiers (The Federal Acquisition Supply Chain Security Act of 2018, NIST 800-53, Rev. 5, SR-1, NIST CSF v1.1, ID.SC-1 and ID.SC-5, NIST IR 8276)?

Ad Hoc (Level 1)
Comments: The Denali Commission has not yet defined and implemented 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.

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. (The Federal Acquisition Supply Chain Security Act of 2018, NIST SP 800-53 REV. 5: SA-4, SR-3, SR-5, SR-6 (as appropriate); NIST SP 800-152; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; OMB M-19-03; OMB A-130; CSF: ID.SC-2 through 4, NIST IR 8276).
Ad Hoc (Level 1)
Comments: The Denali Commission has not yet defined and implemented 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

15. To what extent does the organization maintain and monitor the provenance and logistical information of the systems and system components it acquires? (NIST SP 800-53 REV. 5: SR-4 and NIST SP 800-161, Provenance (PV) family)?
Ad Hoc (Level 1)
Comments: The Denali Commission has not yet defined and implemented 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.

16.1 Please provide the assessed maturity level for the agency's Identify – Supply Chain Risk Management program.
Ad Hoc (Level 1)
Comments: The Denali Commission has not yet defined and implemented an organization wide SCRM strategy to identify and manage the supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services.

16.2 Please provide the assessed maturity level for the agency's Identify Function.
Defined (Level 2)
Comments: The Denali Commission has not yet defined and implemented an organization wide SCRM strategy to identify and manage the supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services.

16.3 Provide any additional information on the effectiveness (positive or negative) of the organization's 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?

Based on the maturity level of the individual areas within the Risk Management and Supply Chain Risk Management domains, the overall maturity level of the identify

Function 2A: Protect – Configuration Management

17 To what degree have the roles and responsibilities of configuration management stakeholders been defined, communicated across the agency, and appropriately resourced (NIST SP 800-53 REV. 4: CM-1; NIST SP 800-128: Section 2.4)?

Defined (Level 2)

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

18 To what extent does the organization utilize 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 (NIST SP 800-128: Section 2.3.2; NIST SP 800-53 REV. 4: CM-9)?

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.

19 To what extent does the organization utilize baseline configurations for its information systems and maintain inventories of related components at a level of granularity necessary for tracking and reporting (NIST SP 800-53 REV. 4: CM-2 and CM-8; FY 2021 CIO FISMA Metrics: 2.2, 3.9.2, and 3.10.1; CSF: DE.CM-7 and PR.IP-1)?

Defined (Level 2)

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

20 To what extent does the organization utilize configuration settings/common secure configurations for its information systems? (NIST SP 800-53 REV. 4: CM-6, CM-7, RA-5, and SI-2; NIST SP 800-70, Rev. 4, FY 2021 CIO FISMA Metrics: 2.1, 2.2, 4.3; SANS/CIS Top 20 Security Controls 3.7; CSF: ID.RA-1 and DE.CM-8)?

Defined (Level 2)

Comments: The Denali Commission utilizes baseline configurations, through their technology vendor, for its information systems.

21 To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities (NIST SP 800-53 REV. 4: CM-3, RA-5, SI-2, and SI-3; NIST SP 800-40, Rev. 3; SANS/CIS Top 20, Control 4.5; FY 2021 CIO FISMA Metrics: 1.3.7, 1.3.8, 2.13, 2.14; CSF: ID.RA-1; DHS Binding Operational Directives (BOD) 18-02 and 19-02)?

Defined (Level 2)

The Denali Commission The Denali Commission has defined it flaw remediation processes, including patch management, to manage software vulnerabilities in the Configuration Management section of its Information Security Policy.

22 To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (OMB M-19-26)?

Ad Hoc (Level 1)

The Denali Commission has twice extended the RFP 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 (NIST SP 800-53 REV. 4: CM-2, CM-3 and CM-4; CSF: PR.IP-3).

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 will be performed post-implementation

24 To what degree does the organization utilize a vulnerability disclosure policy (VDP) as part of its vulnerability management program for internet-accessible federal systems (OMB M-20-32 and DHS BOD 20-01)?

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)

25.2 Provide any additional information on the effectiveness (positive or negative) of the organization's 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 the Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training domains, the overall maturity level of the Protect function is concluded as "Defined".

Function 2B: Protect - Identity and Access Management

26. To what degree have the roles and responsibilities of identity, credential, and access management (ICAM) stakeholders been defined, communicated across the agency, and appropriately resourced (NIST SP 800-53 REV. 4: AC-1, IA-1, and PS-1; NIST SP 800-63-3 and 800-63A, B, and C; Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM), OMB M-19-17)?
Defined (Level 2)
Comments: The roles and responsibilities have been defined, communicated, and implemented across the agency as well as being appropriately resourced.

27. To what degree does the organization utilize a comprehensive ICAM policy, strategy, process, and technology solution roadmap to guide its ICAM processes and activities (FICAM, OMB M-19-17; NIST SP 800-53 REV. 4: AC-1 and IA-1; OMB M-19-17; Cybersecurity Strategy and Implementation Plan (CSIP); SANS/CIS Top 20: 14.1; DHS ED 19-01; CSF: PR.AC-4 and 5)?
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 (NIST SP 800-53 REV. 4: PS-2 and PS-3; National Insider Threat Policy; CSF: PR.IP-11, OMB M-19-17)?
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 (NIST SP 800-53 REV. 4: AC-8, PL-4, and PS-6)?
Defined (Level 2)
Comments: The Denali Commission has defined its processes for developing, documenting, and maintaining access nondisclosure agreements for individuals that access its systems.

30. To what extent has the organization implemented strong authentication mechanisms (PIV or an Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3 credential) for non-privileged users to access the organization's facilities [organization-defined entry/exit points], networks, and systems, including for remote access (HSPD-12; NIST SP 800-53 REV. 4: AC-17, IA-2, IA-5, IA-8, and PE-3; NIST SP 800-128; FIPS 201-2; NIST SP 800-63, 800-157; FY 2021 CIO FISMA Metrics: 2.4, 2.7, CSF: PR.AC-1 and 6; OMB M-19-17, and NIST SP 800-157)?
Defined (Level 2)
Comments: Based on the review of the Denali Commissions access management, the technology vendor, AlasConnect, uses two systems to connect to and perform privileged actions on Denali Commission systems. The first,
The second,
which is hosted by . Remote Desktop manager requires a unique username and password, as well as two factor authentication through .

31. To what extent has the organization implemented strong authentication mechanisms (PIV or an Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3 credential) for privileged users to access the organization's facilities [organization-defined entry/exit points], networks, and systems, including for remote access (HSPD-12; NIST SP 800-53 REV.

4: AC-17, PE-3; NIST SP 800-128; FIPS 201-2; NIST SP 800-63 and 800-157; OMB M-19-17, FY 2021 CIO FISMA Metrics: 2.3, 2.5, and 2.7; CSF: PR.AC-1 and 6; and DHS ED 19-01)?

Defined (Level 2)

Comments: Based on the review of the Denali Commissions access management, the technology vendor, AlasConnect, uses two systems to connect to and perform privileged actions on Denali Commission systems. The first,

The second,

which is hosted by . Remote Desktop manager requires a unique username and password, as well as two factor authentication through .

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 (FY 2021 CIO FISMA Metrics: 2.3, 2.5, 2.6, and 2.7; OMB M-19-17, NIST SP 800-53 REV. 4: AC-1, AC-2, AC-5, AC-6, AC-17; AU-2, AU-3, AU-6, and IA-4; DHS ED 19-01; CSF: PR.AC-4).

Ad Hoc (Level 1)

Comments: The Denali Commission has not defined its processes for provisioning, managing, and reviewing privileged accounts. No defined processes cover approval and tracking, inventorying, and validating, and logging and reviewing privileged users' 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 (NIST SP 800-53 REV. 4: AC-11, AC-12, AC-17, AC-19, AU-2, IA-7, SC-10, SC-13, and SI-4; CSF: PR.AC-3; and FY 2021 CIO FISMA Metrics: 2.10 and 2.11).

Defined (Level 2)

Comments: Based on discussion with Denali Commission, all remote access to Denali Commission systems for Denali Commission staff is performed through Denali Commissions Remote Desktop Gateway system . This system is included in the recurring HTTPS scans to make sure it is not using weak ciphers or protocols. Based on the review of cyber hygiene report, the remote access gateway is scanned for vulnerability risk exposures.

34.1 Please provide the assessed maturity level for the agency's Protect – Identity and Access Management program.
Defined (Level 2)

34.2 Provide any additional information on the effectiveness (positive or negative) of the organization's 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 the Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training domains, the overall maturity level of the Protect function is concluded as "Defined".

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 (NIST SP 800-122; NIST SP 800-37 (Rev. 2) Section 2.3, Task P-1 ; OMB M-20-04; OMB M-19-03; OMB A-130, Appendix I; CSF: ID.GV-3; NIST SP 800-53 REV. 4: AR-4 and Appendix J, FY 2020 SAOP FISMA metrics, Sections 1 through 4, 5(b), NIST Privacy Framework)?
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. (NIST SP 800-53 REV. 4; Appendix J, SC-8, SC-28, MP-3, and MP-6; NIST SP 800-37 (Rev. 2); FY 2021 CIO FISMA Metrics: 2.8, 2.12; DHS BOD 18-02; CSF: PR.DS-1, PR.DS-2, PR.PT-2, and PR.IP-6)?
- 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 AlasConnect to perform the sanitization of digital media. However, limitation of transfer to removable media has not been defined.

37. To what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses? (NIST SP 800-53 REV. 4: SI-3, SI-7(8), SI-4(4) and (18), SC-7(10), and SC-18; FY 2021 CIO FISMA Metrics: 3.8; DHS BOD 18-01; DHS ED 19-01; CSF: PR.DS-5)?
Ad Hoc (Level 1)
Comments: The Denali Commission continues to work on policies and procedures for data exfiltration, enhanced network defenses, email authentication processes, and mitigation against DNS infrastructure tampering.

38. To what extent has the organization developed and implemented a Data Breach Response Plan, as appropriate, to respond to privacy events? (NIST SP 800-122; NIST SP 800-53 REV. 4: Appendix J, SE-2; FY 2020 SAOP FISMA metrics, Section 12; OMB M-17-12; and OMB M-17-25)?
Ad Hoc (Level 1)
Comments: The Denali Commission has not provided support to show that Denali has defined and communicated its Data Breach Response Plan, including its processes and procedures for data breach notification. Further, a breach response team has not 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 (NIST SP 800-53 REV. 4: AR-5, FY 2020 SAOP FISMA Metrics, Sections 9 10, and 11)?
Defined (Level 2)
Comments: The Denali Commission provides, to all employees, privacy awareness training as part of the required annual security awareness training.

40.1 Please provide the assessed maturity level for the agency's Protect – Data Protection and Privacy program.
Defined (Level 2)

40.2 Provide any additional information on the effectiveness (positive or negative) of the organization's 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 Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training domains, the overall maturity level of the Protect function is concluded as "Defined".

Function 2D: Protect – Security Training

41. To what degree have the roles and responsibilities of security awareness and training program stakeholders been defined, communicated 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 (NIST SP 800-53 REV. 4: AT-1; and NIST SP 800-50).
Defined (Level 2)
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 utilize 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 (NIST SP 800-53 REV. 4: AT-2 and AT-3; NIST SP 800-50: Section 3.2; Federal Cybersecurity Workforce Assessment Act of 2015; National Cybersecurity Workforce Framework v1.0; NIST SP 800-181; and CIS/SANS Top 20: 17.1)?
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 each individual's role in the organization.

43. To what extent does the organization utilize a security awareness and training strategy/plan that leverages its organizational skills assessment and is adapted to its culture? (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, and deployment methods (NIST SP 800-53 REV. 4: AT-1; NIST SP 800-50: Section 3; CSF: PR.AT-1).
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. This is supported by the list of personnel and courses provided.

44. To what degree does the organization ensure that security awareness training is provided to all system users and is tailored based on its organization requirements, culture, 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 (NIST SP 800-53 REV. 4: AT-2; FY 2021 CIO FISMA Metrics: 2.15; NIST SP 800-50: 6.2; CSF: PR.AT-2; SANS Top 20: 17.4).

Defined (Level 2)

Comments: The Denali Commission has provided security awareness training to all system users. The training is tailored based on the Commission's mission, risk environment, and types of information systems.

45. To what degree 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) (NIST SP 800-53 REV. 4: AT-3 and AT-4; FY 2021 CIO FISMA Metrics: 2.15)?

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 for the agency's Protect – Security Training program.

Defined (Level 2)

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

Defined (Level 2)

46.3 Provide any additional information on the effectiveness (positive or negative) of the organization's 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 overall maturity level of the Protect function is concluded as "Defined".

Function 3: Detect - ISCM

47. To what extent does the organization utilize information security continuous monitoring (ISCM) policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier (NIST SP 800-37 (Rev. 2) Task P-7; NIST SP 800-137: Sections 3.1 and 3.6)?
Defined (Level 2)
Comments: The Denali Commission has signed an memorandum of agreement (MOA) with the Cybersecurity and Infrastructure Security Agency (CISA) for the Continuous Diagnostics and Mitigation Program (CDM) which will provide the following tools: • Asset Management • Identity and Access Management • Network Security Management • Data Protection Management • Dashboards.

48. To what extent have ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies been defined, communicated across the organization (NIST SP 800-53 REV. 4: CA-1; NIST SP 800-137; CSF: DE.DP-1; NIST 800-37, Rev. 2 Task P-7 and S-5)
Defined (Level 2)
Comments: The Denali Commission has defined the ISCM stakeholders as well as their roles and responsibilities communicated to them across the organization in the ISPC-008 Information Security and Continuous Monitoring Policy which is part 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 (OMB A-130, NIST SP 800-137: Section 2.2; NIST SP 800-53 REV. 4: CA-2, CA-6, and CA-7; NIST Supplemental Guidance on Ongoing Authorization; NIST SP 800-37 (Rev. 2) Task S-5; NIST SP 800-18, Rev. 1, NIST IR 8011; OMB M-14-03; OMB M-19-03).
Ad Hoc (Level 1)
Comments: While the Denali Commission has signed an memorandum of agreement (MOA) with the Cybersecurity and Infrastructure Security Agency (CISA) for the Continuous Diagnostics and Mitigation Program (CDM), the program has not yet been implemented.

50. How mature is the organization's process for collecting and analyzing ISCM performance measures and reporting findings (NIST SP 800-137)?

Ad Hoc (Level 1)
Comments: While the Denali Commission has signed an memorandum of agreement (MOA) with the Cybersecurity and Infrastructure Security Agency (CISA) for the Continuous Diagnostics and Mitigation Program (CDM), the program has not yet been implemented.

51.1 Please provide the assessed maturity level for the agency's Detect - ISCM domain/function.
Defined (Level 2)

51.2 Provide any additional information on the effectiveness (positive or negative) of the organization's 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 overall maturity level of the domain/function is concluded as "Defined".

Function 4: Respond - Incident Response

52. To what extent does the organization utilize an incident response plan to provide a formal, focused, and coordinated approach to responding to incidents (NIST SP 800-53 REV. 4: IR-8; NIST SP 800-61 Rev. 2, section 2.3.2; CSF, RS.RP-1, Presidential Policy Directive (PPD) 8 - National Preparedness)?
Defined (Level 2)
Comments: Reviewed the Denali Commission's Incident Response Plan and verified that the plan contains a list of incident response team stakeholders and their roles and responsibilities, which have been shared across the organization.

53. To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined, communicated across the organization (NIST SP 800-53 REV. 4: IR-7; NIST SP 800-83; NIST SP 800-61 Rev. 2; CSF, RS.CO-1, OMB M-20-04; FY 2021 CIO FISMA Metrics: Section 4; CSF: RS.CO-1; and US-CERT Federal Incident Notification Guidelines)?
Defined (Level 2)
Comments: Reviewed the Denali Commission's Incident Response Plan and verified that the 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? (NIST 800-53: IR-4 and IR-6; NIST SP 800-61 Rev. 2; OMB M-20-04; CSF: DE.AE-1, DE.AE-2 -5, PR.DS-6, RS.AN-1 and 4, and PR.DS-8; and US-CERT Incident Response Guidelines)

Defined (Level 2)

Comments: The Denali Commission has defined a common threat vector taxonomy and developed handling procedures for specific types of incidents, as appropriate. In addition, the Commission has defined its processes for detecting and analyzing incidents, including the types of precursors and indicators and how they are generated and reviewed, and for prioritizing incidents. In addition, the Denali Commission has defined tabletop exercises to be performed in order to rehearse for potential incidents.

55. How mature are the organization's processes for incident handling (NIST 800-53: IR-4; NIST SP 800-61, Rev. 2; CSF: RS.MI-1 and 2)

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 and 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 (FISMA; OMB M-20-04; NIST SP 800-53 REV. 4: IR-6; US-CERT Incident Notification Guidelines; PPD-41; CSF: RS.CO-2 through 5; DHS Cyber Incident Reporting Unified Message)

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 (NIST SP 800-86; NIST SP 800-53 REV. 4: IR-4; OMB M-20-04; PPD-41).

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 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 degree does the organization utilize 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 server security tools (NIST SP 800-137; NIST SP 800-61, Rev. 2; NIST SP 800-44)

Defined (Level 2)

Comments: Defined The Denali Commission has identified and fully defined its requirements for the incident response technologies it plans to utilize in the specified areas. While tools are implemented to support some incident response activities, the tools are not interoperable to the extent practicable, do not cover all components of the organization's network, and/or have not been configured to collect and retain relevant and meaningful data consistent with the organization's incident response policy, plans, and procedures. However, the Denali Commission has signed an MOA with the Cybersecurity and Infrastructure Security Agency to license their Continuous Diagnostics and Mitigation Program which will monitor events across the entire Denali network. Some of the tools currently use, .

59.1 Please provide the assessed maturity level for the agency's Respond – Incident Response domain/function.
Defined (Level 2)

59.2 Provide any additional information on the effectiveness (positive or negative) of the organization's 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 overall maturity level of the domain/function is concluded as "Defined".

Function 5: Recovery - Contingency Planning

60. To what extent have roles and responsibilities of stakeholders involved in information systems contingency planning been defined and communicated across the organization, including appropriate delegations of authority (NIST SP 800-53 REV. 4: CP-1, CP-2, and CP-3; NIST SP 800-34; NIST SP 800-84; FCD-1: Annex B)?
Defined (Level 2)
Comments: The Denali Commission has defined the roles and responsibilities of stakeholders involved in information systems contingency planning have been defined and communicated and implemented those roles and responsibilities across the organization through its Information Security Policy.

61. To what degree does the organization ensure that the results of business impact analyses (BIA) are used to guide contingency planning efforts (NIST SP 800-53 REV. 4: CP-2; NIST SP 800-34, Rev. 1, 3.2; NIST IR 8286; FIPS 199; FCD-1; OMB M-19-03; FY 2021 CIO FISMA Metrics, Section 5; CSF:ID.RA-4)?
Defined (Level 2)
Comments: The results of business impact analyses of business functions have been incorporated 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 (NIST SP 800-53 REV. 4: CP-2; NIST SP 800-34; FY 2021 CIO FISMA Metrics: 5.1; OMB M-19-03; CSF: PR.IP-9)?
Defined (Level 2)
Comments: Processes for information system contingency plan development and maintenance have been defined 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 (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)?

Ad Hoc (Level 1)

Comments: The contingency plan in the Information Security Policy specifies that the contingency plan be tested annually using tabletop exercises However, evidence that the exercises have been performed in the last twelve months has not been provided. In addition, the contingency plan testing does not include, as applicable, notification procedures, system recovery on an alternate platform from backup media, internal and external connectivity, system performance using alternate equipment, restoration of normal procedures, and coordination with other business areas/continuity plans, and tabletop and functional exercises.

64. To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate (NIST SP 800-53 REV. 4: CP-6, CP-7, CP-8, and CP-9; NIST SP 800-34: 3.4.1, 3.4.2, 3.4.3; FCD-1; NIST CSF: PR.IP-4; FY 2021 CIO FISMA Metrics, Section 5; and NARA guidance on information systems security records)?

Defined (Level 2)

Comments: Processes and procedures are in place to perform backup and 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 (CSF: RC.CO-3; NIST SP 800-53 REV. 4: CP-2 and IR-4)?

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 contingency planning section of the Information Security Policy.

66.1 Please provide assessed maturity level for the agency's Recover – Contingency Planning domain/function.

Defined (Level 2)

66.2 Provide any additional information on the effectiveness (positive or negative) of the organization's 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 overall maturity level of the domain/function is concluded as “Defined”.

APPENDIX A: Maturity Model Scoring

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

Function 1A: Identify - Risk Management

Function	Count
Ad-Hoc	2
Defined	8
Consistently Implemented	0
Managed and Measurable	0
Optimized	0

Calculated Rating: Defined (Level 2)

Assessed Rating: Defined (Level 2)

Function 1B: Identify - Supply Chain Risk Management

Function	Count
Ad-Hoc	4
Defined	0
Consistently Implemented	0
Managed and Measurable	0
Optimized	0

Calculated Rating: Ad Hoc (Level 1)

Assessed Rating: Ad Hoc (Level 1)

APPENDIX A: Maturity Model Scoring

Function 2A: Protect - Configuration Management

Function	Count
Ad-Hoc	1
Defined	7
Consistently Implemented	0
Managed and Measurable	0
Optimized	0

Calculated Rating: Defined (Level 2)

Assessed Rating: Defined (Level 2)

Function 2B: Protect - Identity and Access Management

Function	Count
Ad-Hoc	1
Defined	7
Consistently Implemented	0
Managed and Measurable	0
Optimized	0

Calculated Rating: Defined (Level 2)

Assessed Rating: Defined (Level 2)

APPENDIX A: Maturity Model Scoring

Function 2C: Protect - Data Protection and Privacy

Function	Count
Ad-Hoc	2
Defined	3
Consistently Implemented	0
Managed and Measurable	0
Optimized	0

Calculated Rating: Defined (Level 2)

Assessed Rating: Defined (Level 2)

Function 2D: Protect - Security Training

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	0
Managed and Measurable	0
Optimized	0

Calculated Rating: Defined (Level 2)

Assessed Rating: Defined (Level 2)

Function 3: Detect - ISCM

Function	Count
Ad-Hoc	2
Defined	2
Consistently Implemented	0
Managed and Measurable	0
Optimized	0

Calculated Rating: Defined (Level 2)

Assessed Rating: Defined (Level 2)

Function 4: Respond - Incident Response

Function	Count
Ad-Hoc	0
Defined	7
Consistently Implemented	0
Managed and Measurable	0
Optimized	0

Calculated Rating: Defined (Level 2)

Assessed Rating: Defined (Level 2)

APPENDIX A: Maturity Model Scoring

Function 5: Recover - Contingency Planning

Function	Count
Ad-Hoc	1
Defined	5
Consistently Implemented	0
Managed and Measurable	0
Optimized	0

Calculated Rating: Defined (Level 2)

Assessed Rating: Defined (Level 2)

APPENDIX A: Maturity Model Scoring

Overall

Function	Calculated Maturity Level	Accessed Maturity Level	Explanation
Function 1: Identify - Risk Management / Supply Chain RiskManagement	Defined (Level 2)	Defined (Level 2)	The Denali Commission has not yet defined and implemented an organization wide SCRM strategy to identify and manage the supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services.
Function 2: Protect - Configuration Management / Identity & Access Management / Data Protection & Privacy / Security Training	Defined (Level 2)	Defined (Level 2)	
Function 3: Detect - ISCM	Defined (Level 2)	Defined (Level 2)	
Function 4: Respond - IncidentResponse	Defined (Level 2)	Defined (Level 2)	
Function 5: Recover - Contingency Planning	Defined (Level 2)	Defined (Level 2)	
Overall	**Not Effective**	**Not Effective**	