



**STATE OF ALASKA**  
**STATEWIDE**  
**CYBERSECURITY STRATEGIC**  
**PLAN (SCSP)**

*THIS PAGE INTENTIONALLY LEFT BLANK*

---

## TABLE OF CONTENTS

LETTER FROM CYBERSECURITY PLANNING COMMITTEE .....	2
CYBERSECURITY PLAN ELEMENTS .....	6
ENHANCE PREPAREDNESS .....	9
FUNDING & SERVICES .....	16
ASSESS CAPABILITIES .....	16
IMPLEMENTATION PLAN .....	17
APPENDIX A: SAMPLE CYBERSECURITY PLAN CAPABILITIES ASSESSMENT .....	19
APPENDIX B: PROJECT SUMMARY WORKSHEET .....	23
APPENDIX C: ENTITY METRICS .....	24
APPENDIX D: ACRONYMS .....	26
APPENDIX E: REQUIRED, ENCOURAGED, AND OPTIONAL SERVICES, MEMBERSHIPS, AND RESOURCES .....	27
APPENDIX F: KEY TERMS AND DEFINITIONS.....	29

---

# LETTER FROM CYBERSECURITY PLANNING COMMITTEE

Dear Cybersecurity Practitioners,

On behalf of the Alaska State and Local Cybersecurity Grant Program (SLCGP) Planning Committee I am pleased to introduce the 2023 Statewide Alaska Cybersecurity Strategic Plan. This plan reflects the State's continued dedication to enhancing cybersecurity and supporting the public entities within Alaska, as well as collaborating with our local partners.

The Cybersecurity Plan was developed through a collaborative effort of the State of Alaska (SOA) boroughs, cities, tribes, public education, and health institutions throughout the state. It incorporates best practices for managing cybersecurity risks and includes actionable and measurable goals and objectives focusing on the following priorities:

1. Enhance Cybersecurity Resilience and Interoperability
2. Foster a Cybersecurity Culture
3. Strengthen Cybersecurity Collaboration and Partnerships
4. Improve Cyber Incident Management and Response Capabilities

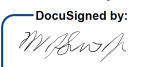
These goals and objectives are designed to help us navigate the ever-changing cybersecurity landscape and plan for new technologies. The Cybersecurity Plan aligns with the requirements of the U.S. Department of Homeland Security for the State and Local Cybersecurity Grant Program (SLCGP) and will serve as a reference point to help evaluate grants requested under that program. In addition, it is a powerful resource to provide practical guidance, coordination, and common understanding throughout the public sector in Alaska.

We recognize the importance of collaboration across disciplines and jurisdictions. Our plan emphasizes the need for partnership and information sharing with local governments, tribes, federal agencies, private sector, academic institutions, and non-profit organizations.


We are committed to achieving the goals outlined in the Cybersecurity Plan and to increase Alaska's cyber resilience. With the help of cybersecurity practitioners and engaged leaders, we can continue to improve our resilience and ensure the safety and security of our state's critical systems and information.

Thank you for your efforts to improve cybersecurity performance throughout the state. We look forward to continuing to work with you to achieve our cybersecurity objectives.

Sincerely,

DocuSigned by:  
  
F32700319D0047B

**Bill Smith**  
Chief Information Officer  
State of Alaska | Department of Administration  
Planning Committee Co-Chair

DocuSigned by:  
  
F32700319D0047B

**Bryan J Fisher**  
State Authorized Agent  
Planning Committee Co-Chair

---

## INTRODUCTION

The State of Alaska Statewide Cybersecurity Strategic Plan (SCSP) is a key component to helping Alaska increase its cyber resilience. Representatives from across the spectrum of Alaska public sector agencies used existing plans, structures, and other relevant efforts to develop this comprehensive cybersecurity plan. Building upon existing structures and capabilities allows Alaska to provide governance and a framework to meet Alaska's critical cybersecurity needs while making the best use of available resources. Members of the planning committee consulted with local governments and associations of local governments and incorporated their feedback into this cybersecurity plan through a collaborative approach. The Department of Military and Veteran Affairs and the Office of the CIO in the Department of Administration partnered to form a Statewide Alaska Cybersecurity Strategic Plan Support Team. The support team established regular communication channels with local governments to gather feedback and input on the cybersecurity plan. This involved holding regular meetings to discuss cybersecurity challenges, share best practices, and gather feedback. This plan represents a baseline that will continue to improve and evolve over time, incorporating continuous input and responding to the ever-changing threat landscape. It is designed to focus on common principles that will help build a strong foundation across all levels of public agencies.

The SCSP support team recognizes the importance of involving these stakeholders in the cybersecurity planning process and ensured that their perspectives and insights were incorporated into the plan. By incorporating feedback from local jurisdictions, the State of Alaska meets requirements **SLCGP: e.2.A.ii**.

The Cybersecurity Plan is a two-year strategic planning document that contains the following components:

- **Vision and Mission:** The vision of the plan is to enhance Alaska's cybersecurity posture and resilience to mitigate cyber threats and vulnerabilities. The mission is to develop and implement a comprehensive cybersecurity strategy that involves all stakeholders and ensures the safety and security of Alaska's critical infrastructure and systems.
- **Organization, and Roles and Responsibilities:** This section describes the current roles and responsibilities for cybersecurity within the state, including any governance mechanisms in place. It also identifies the successes, challenges, and priorities for improvement. The plan outlines a strategy for the cybersecurity program and the organization structure that supports it. Additionally, the governance framework outlines authorities and requirements for the cybersecurity program. The Cybersecurity Plan is a guiding document and does not create any authority or direction over any state or local systems or agencies.
- **How feedback and input from local governments and associations was incorporated.** The plan describes how feedback and input from local governments and associations were incorporated to reduce overall cybersecurity risk across Alaska. This was achieved through stakeholder engagement, meetings, and workshops, to ensure a holistic approach to developing the cybersecurity plan.
- **Cybersecurity Plan Elements:** This section outlines the technology and operations needed to maintain and enhance resilience across the cybersecurity landscape. The plan includes the 16 required elements outlined in the State and Local Cybersecurity

---

Improvement Act, including managing, monitoring, and tracking information systems, enhancing preparation and response to incidents, implementing continuous cybersecurity risk management practices, adopting best practices and methodologies, promoting the delivery of safe and trustworthy online services, ensuring continuity of operations, enhancing the cybersecurity workforce, and mitigating risks to critical infrastructure and key resources.

- **Funding:** The plan describes funding sources and allocations to build cybersecurity capabilities within the state, along with methods and strategies for funding sustainment and enhancement to meet long-term goals. This includes using cybersecurity grant funding to provide cost-effective and scalable cybersecurity services to local governments, including rural communities.
- **Implementation Plan:** The plan describes the state's approach to implementing, maintaining, and updating the Cybersecurity Plan to enable continued evolution and progress toward the identified goals. It includes a timeline for implementation and identifies the necessary resources needed to achieve the plan's objectives.
- **Metrics:** The plan describes how the state will measure the outputs and outcomes of the program across the state, including the use of key performance indicators (KPIs) to measure progress against the identified goals. This includes tracking the number of assessments, audits, exercises, and training sessions conducted, as well as the number of entities completing each component of the curriculum.

## Vision and Mission

Alaska's vision and mission for improving cybersecurity practices statewide:

### **Vision:**

Create a secure and resilient cybersecurity environment for the State of Alaska, where all state, local, and tribal governments work together seamlessly to protect against cybersecurity risks and threats to information systems owned or operated by, or on behalf of, our public sector agencies, and in the public interest.

### **Mission:**

Develop and implement a comprehensive cybersecurity plan for the State of Alaska that incorporates existing plans and feedback from local governments, promotes the adoption of best practices and methodologies, and ensures the continuity of operations in the event of a cybersecurity incident. The outcomes from this planning effort and implementation will include: assessment of the capabilities of the eligible entity relating to the actions described in the plan and identify and mitigate any gaps in the cybersecurity workforce, enhancement of the delivery of safe and trustworthy online services and work to establish strong partnerships to improve information sharing and collaboration. , and collaboratively striving to achieve measurable progress towards reducing cybersecurity risks and identifying, responding to, and recovering from

cybersecurity threats to information systems owned or operated by, or on behalf of, our public sector agencies, and in the public interest.

## Cybersecurity Program Goals and Objectives

State of Alaska Cybersecurity goals and objectives include the following:

Cybersecurity Program	
Program Goal	Program Objectives
<p><b>1. Enhance Cybersecurity Resilience and Interoperability.</b> Encourage and support cybersecurity resilience by promoting the adoption of risk management programs that incorporate best practices and methodologies. Encourage alignment of information and operational technology cybersecurity objectives, and advocate for the establishment of an information and operational technology modernization cybersecurity review process.</p>	<p>1.1 Support and encourage a cybersecurity risk assessment of state and local government information systems to identify vulnerabilities and develop a risk management plan. Support the establishment of risk assessment protocols and provide guidance and resources to aid in the identification of potential cybersecurity risks and vulnerabilities.</p> <p>1.2 Support and encourage the implementation of a continuous monitoring program to identify and mitigate cybersecurity risks and threats to information systems owned or operated by the state or local governments within Alaska. Promote the adoption of continuous monitoring practices and provide support to organizations and agencies in their efforts to identify and mitigate potential cybersecurity risks and threats.</p>
<p><b>2. Foster a Cybersecurity Culture.</b> Encourage and support the fostering of a cybersecurity culture by promoting awareness and training programs for state employees, contractors, and local government personnel. Encourage the adoption of such programs and support the efforts of organizations and agencies in providing cybersecurity education and training to their employees and stakeholders.</p>	<p>2.1 Support and encourage the development and delivery of cybersecurity awareness and training programs to state employees, contractors, and local government personnel. Promote the adoption of such programs and provide resources and guidance to aid in the development and delivery of effective cybersecurity education and training.</p> <p>2.2 Support and encourage the establishment of a cybersecurity awareness program to educate citizens on best practices and cybersecurity risks. Advocate for the adoption of awareness programs and provide resources and guidance to organizations and agencies in their efforts to educate citizens on cybersecurity risks and promote best practices.</p>

Program Goal	Program Objectives
<p><b>3. Enhance Cybersecurity Collaboration and Partnerships.</b> Support and encourage the enhancement of Cybersecurity Collaboration and Partnerships by promoting the development of a cybersecurity information sharing program with local governments, neighboring states, and federal agencies, and fostering cybersecurity partnerships and collaborations with the private sector, academic institutions, and non-profit organizations. Advocate for the establishment of information sharing protocols and encourage organizations and agencies to form partnerships and collaborations that promote effective cybersecurity practices and information sharing.</p>	<p>3.1 Support and encourage the development and implementation of a cybersecurity information sharing program with local governments, neighboring states, and federal agencies. Advocate for the establishment of information sharing protocols and provide resources and guidance to organizations and agencies in their efforts to develop and implement effective information sharing programs.</p> <p>3.2 Foster cybersecurity partnerships and collaborations with the private sector, academic institutions, and non-profit organizations to develop and implement best practices.</p>
<p><b>4. Improve Cybersecurity Incident Management and Response Capabilities.</b> Support and encourage the development and implementation of a cybersecurity incident response plan that outlines the roles, responsibilities, and procedures for responding to and recovering from cybersecurity incidents. Provide guidance and resources to aid in the establishment of incident response protocols and support organizations and agencies in their efforts to effectively respond to cybersecurity incidents.</p>	<p>3.3 Support and encourage the establishment of a cybersecurity incident response team with appropriate roles and responsibilities and promote the training and equipping of the team to respond to cybersecurity incidents. Provide resources and guidance to organizations and agencies in their efforts to establish incident response teams and ensure their readiness to respond to cybersecurity incidents.</p> <p>3.4 Support and encourage the development and implementation of a cybersecurity incident management plan that outlines the procedures for responding to cybersecurity incidents and the roles and responsibilities of all stakeholders involved. Advocate for the adoption of incident management plans and provide support to organizations and agencies in their efforts to effectively respond to cybersecurity incidents.</p>

## CYBERSECURITY PLAN ELEMENTS

This plan incorporates the following plans:

- State of Alaska Emergency Operations Plan (EOP) available at <https://ready.alaska.gov/plans/>
- State of Alaska 2023 -2025 Integrated Preparedness Plan (IPPW) available at <https://ready.alaska.gov/Documents/Preparedness/Exercise/IPP%20SFY2023-2025.pdf>
- Small Community Emergency Response Plan (SCERP), plan can be accessed by contacting the Alaska Division of Homeland Security and Emergency Management at [mvaplanning@alaska.gov](mailto:mvaplanning@alaska.gov)
- State of Alaska Hazard Mitigation Plan, available at <https://ready.alaska.gov/Mitigation/SHMP>

## MANAGE, MONITOR, AND TRACK



---

---

The State of Alaska recognizes the critical importance of managing, monitoring, and tracking information systems, applications, and user accounts to effectively protect against cybersecurity risks and threats. To achieve this goal, the State will take – and encourage local governments to take – a comprehensive, integrated, and risk-based approach that incorporates the best practices and methodologies outlined in the Cybersecurity plan. Our strategic approach will focus on the following key areas.

### **Inventory Management**

The State of Alaska encourages and supports the development of an inventory management program that includes all hardware and software used by the State, to include local government entities as feasible and decided locally. The inventory management program should incorporate prioritized risk to each item and should be reviewed and updated at least annually. This program will ensure that we have an accurate and up-to-date inventory of all information systems, applications, and user accounts, as well as any legacy systems that are no longer supported by the manufacturer. We encourage and support the development of policies and procedures for managing, monitoring, and tracking these systems to ensure that they are effectively protected against cybersecurity risks and threats.

### **Continuous Monitoring**

The State of Alaska encourages and supports a continuous monitoring program that includes monitoring of activity, and behavior across all information systems, applications, and user accounts owned or operated by the State and encouraged for all local governments to implement and share. The program should leverage advanced technologies and tools to identify and mitigate cybersecurity risks and threats, including those that may target legacy systems. We also encourage and support the establishment of processes for responding to any alerts or incidents identified through the continuous monitoring program. The monitoring program should include identification of privileged accounts, key data and where it is stored and ensure it confidentiality, integrity, and availability.

### **Risk-Based Vulnerability Management**

We encourage a risk-based vulnerability management program that includes regular vulnerability assessments and threat mitigation practices prioritized by the degree of risk to address cybersecurity risks and threats on all information systems, applications, and user accounts owned or operated by the state or local governments. This program should incorporate best practices and methodologies, to ensure that we are effectively managing, monitoring, and tracking vulnerabilities and threats.

### **Legacy System Management**

We recognize that legacy systems that are no longer supported by the manufacturer are particularly vulnerable to cybersecurity threats. To address this vulnerability, we will encourage and support the implementation of a comprehensive legacy system management program that includes special focus on managing, monitoring, and tracking these systems to effectively protect, detect, respond to, and recover from cybersecurity incidents. This program should also include strategies for modernizing or replacing legacy systems where necessary.

While we understand that some eligible grant recipients may face constraints preventing them from replacing their legacy systems, we strongly encourage them to prioritize the implementation of compensating controls. Compensating controls serve as alternative measures to achieve cybersecurity objectives when traditional controls are not feasible or practical. By implementing these controls, entities

---

---

can mitigate the risks associated with legacy systems and reduce the likelihood and impact of cybersecurity incidents. We are committed to collaborating with such entities, assisting them in identifying and implementing compensating controls that are suitable for their specific needs and circumstances.

By adopting a comprehensive, integrated, and risk-based approach to managing, monitoring, and tracking information systems, applications, and user accounts, the State of Alaska will improve its cybersecurity resilience and interoperability over the next two years, and beyond. This approach will ensure that we are effectively protecting against cybersecurity risks and threats, including those that target legacy systems, and that we are able to detect, respond to, and recover from incidents in a timely and effective manner meet the requirement SLCGP: e.2.B.iv.

## MONITOR, AUDIT, AND TRACK

The State of Alaska recognizes the importance of monitoring, auditing, and tracking network traffic and activity to enhance cybersecurity resilience across state and local government entities. While Alaska does not have a centralized security / information technology operation center (SOC / ITOC) to monitor, audit, and track network traffic and activity across all SLTTs currently, the state does support and encourage the following to monitor, audit, and track network traffic and activity:

- **Decentralized Monitoring:** SLTTs can be responsible for monitoring, auditing, and tracking their own network traffic and activity. This can be done using a combination of commercial and open-source tools and can be supplemented by training and information sharing initiatives to ensure that entities have the knowledge and skills necessary to monitor their networks effectively.
- **Partnerships with Managed Security Service Providers (MSSPs):** SLTTs can establish partnerships with MSSPs to monitor, audit, and track network traffic and activity on behalf of entities within their jurisdiction. This can be done through contracts with the MSSPs, who can provide centralized monitoring and reporting capabilities.
- **Cloud-based Security Services:** SLTTs can leverage cloud-based security services to monitor, audit, and track network traffic and activity. This can be done through contracts with cloud service providers, who can provide centralized monitoring and reporting capabilities.
- **Collaborative Monitoring:** SLTTs can establish a collaborative monitoring program that brings together entities within their jurisdiction to share monitoring data and collaborate on threat identification and response. This can be done using a shared platform that enables entities to share data and collaborate on threat identification and response.

SLTTs are encouraged to leverage established partnerships with agencies such as CISA, MS-ISAC, and/or vendor network monitoring, auditing, and tracking services to enhance their capabilities for monitoring, auditing, and tracking network traffic and activity. By doing so, state and local government can leverage best practices and expertise across the cybersecurity community to enhance Alaska's overall cybersecurity posture. The State of Alaska has partnered with a variety of organizations to bolster its cybersecurity measures. One such partnership is with the Alaska Federation of Natives, which launched the Alaska Native Cybersecurity Enhancement Project to train Alaska Natives in cybersecurity skills. The state has also partnered with Arctic Slope Regional Corporation and the University of Alaska to establish the Alaska Cybersecurity Center, which offers

---

training and research opportunities to students and professionals. Additionally, the state has worked with the Department of Homeland Security to conduct cybersecurity risk assessments and develop response plans.

These partnerships demonstrate the State of Alaska's commitment to staying ahead of cyber threats and ensuring that its citizens, businesses, and infrastructure are protected. By collaborating with various organizations, the state can leverage their expertise and resources to create a more secure cyber landscape.

- **Network Security:** SLTTs can establish a comprehensive network security program that includes all information systems, applications, and user accounts owned or operated by the state or local government entities within the jurisdiction of the state. This program should incorporate best practices and methodologies to ensure that the SLTTs are effectively monitoring, auditing, and tracking vulnerabilities and threats. By doing so, the SLTTs will enhance their cybersecurity resilience and interoperability by ensuring that we are effectively securing our network infrastructure.

The State of Alaska and the SLCGP planning committee will identify and assist with coordinating activities between local government entities and federal partners to enhance network monitoring, auditing, and tracking of network traffic and activity. By leveraging partnerships, cloud-based services, collaborative monitoring programs, and cybersecurity services, the state aims to ensure effective cybersecurity resilience, information sharing, and interoperability across all levels of government. This commitment aligns with our goal to stay ahead of cyber threats and protect the state's citizens, businesses, and infrastructure, and enhance their overall cybersecurity resilience meeting the requirement of SLCGP: e.2.B.iv.

## ENHANCE PREPAREDNESS

The State of Alaska will collaborate with relevant agencies and stakeholders to develop and implement a comprehensive cybersecurity preparedness plan that includes all levels of government within the state. The plan will be based on Risk Management Best Practices and Frameworks and will identify and prioritize key resources that are vital to the state's economy, public health, and safety.

We will work with relevant state, local and federal agencies to provide training and exercise support to SLTT organizations to enhance their cybersecurity preparedness. The State of Alaska recommends these activities include tabletop exercises, functional exercises, and full-scale exercises to test and evaluate the state's cybersecurity response capabilities.

Additionally, we will expand ongoing training programs to enhance the knowledge and skills of personnel within the community to address cybersecurity risks and threats. The recommended topics include cybersecurity hygiene training, awareness campaigns, and training on the latest cybersecurity technologies and best practices.

To enhance our response capabilities, we will develop and implement incident response plans and procedures to address cybersecurity incidents promptly and effectively. We will also ensure that our response plans align with the National Incident Management System (NIMS) and the National Response Framework (NRF).

---

---

Through these efforts, the State of Alaska will enhance its preparation, response, and resiliency against cybersecurity risks and threats, and promote and support that for SLTTs. As we achieve our program objectives, we will report our progress and outcomes to relevant stakeholders and adjust our strategies as necessary.

### *Assessment and Mitigation*

The State of Alaska's strategic approach to implementing a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk will focus on improving the state's ability to identify and mitigate cybersecurity threats and vulnerabilities on information systems, applications, and user accounts across state and local governments.

To achieve this, the state will encourage, support, and collaborate with local entities to develop comprehensive cybersecurity risk assessments to be performed annually, including identifying potential vulnerabilities and prioritizing mitigation efforts based on the level of risk. The State will also encourage and support the development and implementation of policies and procedures for vulnerability management, including timely application of security patches and updates, regular vulnerability scans, and penetration testing.

The State of Alaska acknowledges the significance of identifying and mitigating cybersecurity threats and vulnerabilities to uphold the ongoing protection of critical information systems, applications, and user accounts. As part of its commitment, the State of Alaska will require, through the grant process, grantees conduct a self-assessment and engage in ongoing follow-ups. This collaborative effort between state and local government entities will establish a continuous process of cybersecurity vulnerability assessments and threat mitigation practices, prioritized based on the degree of risk.

To ensure that local entities have access to the necessary tools and resources, the State will expand ongoing training, cyber incident exercise, and cybersecurity information sharing. By regularly assessing and mitigating cybersecurity threats and vulnerabilities, the State of Alaska will improve the overall cybersecurity posture of state and local government entities and meet the requirement SLCGP: e.2.B.iv.

### *Best Practices and Methodologies*

The State of Alaska recognizes the importance of adopting and using best practices and methodologies to enhance cybersecurity. To improve the overall security posture of SLTT organizations, the following cybersecurity best practices will be encouraged, and eligible for available grant funding, to be implemented within a reasonable timeline according to the prioritization that emerges from the self-assessment:

- Implement multi-factor authentication.
- Implement enhanced logging.
- Data encryption for data at rest and in transit
- End use of unsupported/end of life software and hardware that are accessible from the Internet.
- Identify and implement compensating controls to mitigate threats to unsupported software and hardware
- Prohibit use of known/fixed/default passwords and credentials
- Ensure the ability to reconstitute systems (backups)
- Migrate to the .gov internet domain
- Implement network boundary filtering capabilities where practicable (e.g., DNS, URL, Email)
- Implement [cyber]security awareness training program.

- 
- Implement authentication and privileged account access in alignment with best practices and standards on an annual basis.
  - Implement a Patch Management Solution

These best practices will be incorporated statewide and individual projects that assist SLTT entities adopting these best practices will be prioritized.

### *NIST Principles*

In addition to the above best practices, the State of Alaska will adopt recognized frameworks such as NIST Cybersecurity Framework (CSF) or equivalent frameworks to significantly improve its ability to meet cybersecurity requirements. The State of Alaska will work to implement NIST CSF or an equivalent framework as the foundation for its Cybersecurity Program and work towards its widespread adoption among state and local entities.

### *Supply Chain Risk Management*

Supply Chain Risk Management is a critical aspect of cybersecurity, and the State of Alaska will adopt cyber supply chain risk management (C-SCRM) best practices identified by NIST. The state will identify, prioritize, and assess information technology suppliers, vendors, and service providers – including to work with and through local partners - to understand the related and/or cascading risks to the state and local supply chain.

### *Tools and Tactics*

To continuously improve cybersecurity best practices, the State of Alaska will engage with MS-ISAC, CISA, and other partners and systems to gain access to knowledge bases of adversary tools and tactics. The State encourages SLTTs to participate in government and cybersecurity conferences and liaise with cybersecurity professionals from federal, state, and private entities to share indicators of compromise, best practices, and threat intelligence. Partnerships with affiliated organizations will enhance the State's ability to share opportunities and information.

## **Safe Online Services**

The State of Alaska is committed to promoting the delivery of safe, recognizable, and trustworthy online services. As part of this effort, the state is encouraging the use of the .gov internet domain for all state agencies and local entities that are eligible for the domain.

To support the adoption of the .gov domain, the state is providing technical assistance and resources to eligible entities. This includes guidance on how to obtain a .gov domain, as well as assistance with domain registration and implementation. Additionally, the state is promoting the use of cybersecurity tools, such as external vulnerability scanning, automated vulnerability monitoring, scanning, and reporting to ensure that online services are safe and secure.

The state is also committed to ongoing education and awareness efforts to promote safe online practices among employees and the public. This includes regular cybersecurity training and awareness campaigns, as well as public outreach initiatives to raise awareness about online risks and best practices for staying safe online.

---

---

By promoting the use of the .gov domain and providing resources and support for safe online services, the State of Alaska is demonstrating its commitment to enhancing cybersecurity and ensuring the delivery of safe and trustworthy online services.

## **Continuity of Operations**

Continuity of Operations (COOP) planning is essential to ensure the delivery of critical services and operations in the event of a cyber incident. The State of Alaska will establish a comprehensive COOP program to ensure the continuity of critical services and operations during and after a cyber incident. This program will be developed in coordination with the Alaska Division of Homeland Security and Emergency Management and will include partnerships with local and tribal governments.

The State of Alaska will provide resources to support COOP planning and emergency response efforts. The State will also promote ongoing training and exercises to enhance COOP preparedness and response capabilities.

For this two-year Plan, the State of Alaska will prioritize the development of viable, comprehensive COOP plans and business continuity programs for state agencies, local governments, and tribal entities. The State will collaborate with partners to expand ongoing training, cyber incident exercise, and cybersecurity information sharing, which will support local entities' COOP planning efforts.

The State will also establish performance measures to track the maturity of COOP planning efforts and incident response preparedness. The State of Alaska is committed to ensuring continuity of operations in the face of cyber incidents and demonstrates that the plan meets requirement SLCGP: e.2.B.vii.

## **Workforce**

The State of Alaska is committed to using the National Initiative for Cybersecurity Education (NICE) Workforce Framework to identify and mitigate any gaps in the cybersecurity workforce. This includes enhancing recruitment and retention efforts, as well as improving personnel's knowledge, skills, and abilities to address cybersecurity risks and threats.

To support this initiative, the State of Alaska will work to build alliances with employers, educational institutions, and public and private partners to develop training and educational pathways to provide the needed skilled workers in the cybersecurity field.

Initiatives will focus on developing internships and apprenticeships, promoting cybersecurity education in K-12 and higher education, and utilizing state-supported internship programs.

The State of Alaska will also provide ongoing training to personnel at all levels in good cyber hygiene and best cybersecurity practices. This will include promoting the adoption of the NICE Framework in state and local hiring practices and encouraging interested individuals to further develop their cybersecurity skills through internships and educational opportunities.

The State will continue to monitor the its cybersecurity workforce and promote the adoption of best practices and the NICE Framework to ensure the State of Alaska has a skilled and effective cybersecurity workforce, meeting requirement SLCGP: e.2.B.viii.

## **Continuity of Communications and Data Networks**

The State of Alaska recognizes the critical need for cross-jurisdictional continuity of communications and data networks in the event of an incident involving those communications or data networks. To address this need, the State of Alaska will ensure that all entities have access to a comprehensive and regularly

---

---

updated Incident Response Plan that provides instructions for communication during an incident and how to handle situations where the secure and preferred communication method is unavailable.

The State of Alaska will ensure that all entities are trained in the use of these communication and data network systems and will conduct regular exercises to test their effectiveness in maintaining continuity of operations. The State of Alaska will also establish procedures for the use of Traffic Light Protocol (TLP) when sharing incident information to ensure that sensitive information is only shared with appropriate audiences.

Through these efforts, the State of Alaska will ensure cross-jurisdictional continuity of communications and data networks in the event of an incident involving those communications or data networks, meeting requirement SLCGP: e.2.B.ix.

## **Assess and Mitigate Cybersecurity Risks and Threats to Critical Infrastructure and Key Resources**

The State of Alaska Division of Homeland Security and Emergency Management (DHSEM) conducts a federally required Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) every three years. The State recognizes the importance of assessing and mitigating cybersecurity risks and threats to critical infrastructure and key resources, such as power and telecommunications, that may impact the performance of information systems within its purview. To accomplish this goal, the state will conduct regular assessments of its capabilities across relevant mission areas, including Prevention, Protection, Mitigation, Response, and Recovery.

Alaska will encourage and support the use of established frameworks, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework or equivalent, to guide its assessment and mitigation efforts. These assessments target federal and state funding to mitigate cybersecurity risks and threats to critical infrastructure and key resources.

The state will work closely with its partners, including local jurisdictions and private sector organizations, to identify and prioritize critical infrastructure and key resources and develop strategies to enhance their cybersecurity posture. The state will share and promote the adoption of best practices and cybersecurity frameworks, such as the NIST Cybersecurity Framework, to ensure that critical infrastructure and key resources are protected to the greatest degree possible.

Alaska recognizes that assessing and mitigating cybersecurity risks and threats to critical infrastructure and key resources is an ongoing process that requires continuous monitoring and improvement. The state will regularly review and update its strategies and plans to ensure that they remain effective and responsive to the evolving threat landscape. These efforts demonstrate that the state is committed to meeting requirement SLCGP: e.2.B.x.

## **Cyber Threat Indicator Information Sharing**

The State of Alaska is committed to enhancing its capacity and capabilities to share cyber threat indicators and related information with relevant stakeholders. To achieve this goal, we will leverage CISA's Cyber Information Sharing and Collaboration Program (CISCP), CISA's Automated Indicator Sharing capability and systems, and other applicable systems and processes.

Additionally, we will encourage all entities to subscribe to and participate in the MS-ISAC Real-Time Indicator Feeds to stay up to date on emerging threats and vulnerabilities. We will also promote the adoption of CISA's free cybersecurity services to local entities through outreach efforts and state and federal partnerships.

---

---

As part of our commitment to information-sharing, we will maintain active collaborations with our federal, state, local, tribal (SLTT) partners, as well as organizations like the Alaska Municipal League (AML), to collectively identify and address cybersecurity threats and vulnerabilities. By leveraging these partnerships, we aim to enhance our ability to identify and mitigate potential risks to our critical infrastructure and key resources, thereby ensuring the uninterrupted continuity of our operations even in the face of a cyber incident. This comprehensive plan aligns with and fulfills the requirement SLCGP: e.2.B.xii.

#### *Department Agreements*

The State of Alaska is committed to sharing cyber threat indicators and related information with all SLTTs, including expanding information sharing agreements with CISA. Alaska will expand information sharing by working with partners by developing options for centralizing communication and information sharing to share cyber threat information products with federal, and SLTT partners. The SLCGP committee will continue to work towards expanding and evolving the sharing of cyber threat indicators, incidents after action reports, and other related information with CISA and MS-ISAC. As part of Alaska's cybersecurity plan, we will focus on improving and enhancing cybersecurity intelligence and information sharing across all levels of government, including local, regional, state, and federal organizations. Through this plan, we will initiate projects to achieve this goal and expand our capability to share cyber threat indicator information with DHS, meeting requirement SLCGP: e.2.B.xi.I-II.

### **Leverage CISA Services**

The State of Alaska recognizes the importance of leveraging the cybersecurity services offered by CISA to enhance our cybersecurity posture. Alaska currently participates in several CISA programs, including the Automated Indicator Sharing (AIS) and the Cyber Hygiene program.

The Alaska Division of Homeland Security and Emergency Management (DHSEM) will continue to collaborate with CISA to identify opportunities to expand our participation in these programs and explore additional cybersecurity services offered by CISA that could benefit our state.

DHSEM will also work to increase awareness of the benefits of these services among state and local entities and promote adoption of CISA's cybersecurity best practices and guidelines. The State encourages CISA to ensure adequate timeliness and responsiveness to needs especially of SLTTs, including to provide technical assistance as they implement local planning efforts.

Through these efforts, Alaska aims to strengthen our cybersecurity capabilities and meet the requirements of SLCGP: e.2.B.xii.

#### Information Technology and Operational Technology Modernization Review

The State of Alaska is committed to ensuring alignment between information technology (IT) and operational technology (OT) cybersecurity objectives. As part of this Statewide Alaska Cybersecurity Strategic Plan, we will encourage and support a modernization review process to identify and mitigate cybersecurity risks and threats to IT and OT systems.

The State encourages and supports regular assessments of IT and OT systems to ensure they are properly secured and updated. We will prioritize the implementation of security controls and risk management strategies to address any vulnerabilities identified during these assessments.

To ensure effective alignment between IT and OT cybersecurity objectives, we will encourage and support the creation of a cross-functional team comprising IT and OT professionals from SLTTs who will work collaboratively to identify and mitigate cybersecurity risks and threats. This team will be responsible for



---

---

evaluating new technologies and solutions to ensure they are secure and compatible with both IT and OT systems.

We will continue to establish partnerships with industry experts and vendors who specialize in OT cybersecurity to gain valuable insights and expertise in securing critical infrastructure and key resources. These partnerships will help us identify emerging threats and vulnerabilities, as well as best practices for securing IT and OT systems.

Through these efforts, we will ensure that our IT and OT systems are secure and resilient, and that we can effectively respond to and mitigate cybersecurity risks and threats to our critical infrastructure and key resources.

## **Cybersecurity Risk and Threat Strategies**

The SLCGP Committee of the State of Alaska will develop and coordinate strategies to address cybersecurity risks and threats in collaboration with other organizations. This will include consulting with local governments and associations of local governments, neighboring entities, and Tribal governments, or members of an ISAC; and other states. We will establish a process to ensure effective communication and collaboration with relevant entities and organizations. We will participate in the activities of organizations such as the Multi-State Information Sharing and Analysis Center (MS-ISAC) to enhance information sharing and collaboration with other states.

Our approach will involve regular coordination and information sharing with neighboring entities, , and Tribal governments to ensure that we have a comprehensive understanding of cybersecurity risks and threats in our region. We will work with these entities to develop coordinated response plans and strategies to address cybersecurity incidents that affect our jurisdictions.

In addition, we will collaborate with federal agencies such as the Department of Homeland Security and the Federal Bureau of Investigation to enhance our cybersecurity capabilities and ensure effective incident response. The State of Alaska is committed to a proactive and collaborative approach to cybersecurity risk and threat strategies, meeting requirement SLCGP: e.2.B.xiv.

## **Rural Communities**

The State of Alaska recognizes the importance of ensuring that rural communities have adequate access to and can participate in cybersecurity services and activities. As a geographically expansive state, with many rural and remote communities, the state government is committed to providing cybersecurity services and resources to all Alaska public and local entities, regardless of their location or socioeconomic status.

To achieve this goal, the state government will work closely with local governments, associations of local governments, and tribal governments to identify and address any barriers to access that may exist in rural communities. This will involve consultation with these communities to understand their unique needs and challenges related to cybersecurity.

The state government will also help public sector entities explore the use of technology to provide cybersecurity services and resources to rural communities. This may include the use of virtual training and educational materials, as well as remote access to cybersecurity experts and support services.

In addition, the state government will promote public-private partnerships that can help to address the cybersecurity needs of rural communities. This may involve working with local businesses, non-profits, and other organizations to provide cybersecurity training and support to individuals and organizations in rural areas.

---

Overall, the State of Alaska is committed to ensuring that all Alaska entities, regardless of their location or background, have access to the cybersecurity services and resources they need to protect themselves and their communities from cyber threats.

## **FUNDING & SERVICES**

The State of Alaska plans to utilize grant funding to support its comprehensive cybersecurity plan, including initiatives to improve the cybersecurity practices of state agencies and local entities. The state will distribute funds, items, services, capabilities, or activities to local governments, including plans to distribute at least 25% of cybersecurity grant funding received to rural areas.

In the first year of the program, the State of Alaska will focus on providing cost-effective and scalable cybersecurity services to local governments, including rural communities. These services will include assessments, audits, continuity planning, response planning, exercises, and skill enhancement for local entities. The state will work directly and collaborate with relevant agencies and partners to ensure a comprehensive and multi-faceted approach.

The State of Alaska will also work to expand and evolve cybersecurity practices across state agencies through improving vulnerability management and penetration testing and creating metrics and reports to prioritize remediation action. The state will use NIST 800-53 as a framework for implementing these initiatives.

### **Distribution to Local Governments**

The State of Alaska aims to support local governments through implementing its comprehensive cybersecurity plan and by providing resources that enable delivery of the plan's objectives. These details will be listed in a table found in Appendix B: Project Summary Worksheet. To ensure the successful implementation of the cybersecurity plan, the state will distribute funds, items, services, capabilities, or activities to local governments. Additionally, the state plans to allocate at least 25% of the cybersecurity grant funding received specifically to rural areas.

## **ASSESS CAPABILITIES**

The State of Alaska will adopt a strategic approach to assess the capabilities of entities applying for funding through the grant program for the various cybersecurity plan elements. This approach aims to comprehensively evaluate the cybersecurity capabilities of each entity, specifically addressing the requirements outlined in Appendix A: Cybersecurity Plan Capabilities Assessment. The assessment of Alaska's cybersecurity capabilities will be conducted at different levels, namely Foundational, Fundamental, Intermediate, and Advanced.

To assess these capabilities, the State of Alaska will leverage the NIST Cybersecurity Framework and the NICE Workforce Framework for Cybersecurity. Furthermore, a gap analysis will be conducted to identify areas that require improvement and enhancement in terms of cybersecurity capabilities. The State will support and encourage SLTTs to perform their own gap analysis that can be funded through the grant program.

Based on the assessment outcomes, Alaska will identify areas that necessitate increased capabilities and will develop action plans to address those gaps. Clear assignment of responsibilities to relevant parties and target completion dates will be established for each action plan.

---

---

In addition, periodic assessments will be conducted to ensure the continuous effectiveness of Alaska's cybersecurity capabilities in addressing emerging cyber threats and risks. These assessments will follow a regular schedule and involve all relevant stakeholders.

Overall, Alaska remains dedicated to the ongoing enhancement of its cybersecurity capabilities, ensuring effective protection of information systems and critical infrastructure against cyber threats and risks.

## IMPLEMENTATION PLAN

### Organization, Roles and Responsibilities

The Department of Administration, under the State of Alaska, takes the lead in managing the executive branch cybersecurity program. Specifically, it oversees the Office of Information Technology (OIT), which is responsible for safeguarding and managing the IT infrastructure of the state's executive branch. The OIT ensures the implementation of cybersecurity policies and standards, and its primary focus is on securing the executive branch's IT systems and infrastructure. The SLCGP Committee, consisting of representatives from various state agencies and levels of government, is responsible for developing and implementing the Statewide Alaska Cybersecurity Strategic Plan. The Committee will coordinate with local governments and associations, neighboring entities, Tribal governments, and ISACs to ensure effective implementation of the Plan.

The following roles and responsibilities have been defined for the implementation of the Statewide Alaska Cybersecurity Strategic Plan:

- The Department of Administration will serve as the lead agency for the cybersecurity program and oversee the implementation of the Plan.
- The OIT will manage and secure the state's IT infrastructure, oversee compliance with cybersecurity policies and standards, and ensure the implementation of the Plan.

The State of Alaska, through its Emergency Management and grant administration, will play a vital role in the development, implementation, and coordination of the comprehensive cybersecurity plan. The SLCGP (State and Local Cyber Grant Program) Committee will take the lead in developing and implementing the plan, ensuring effective coordination with other organizations involved in cybersecurity efforts.

Furthermore, the committee will oversee the overall implementation of the plan, working closely with the State of Alaska Emergency Management and grant administration to ensure its successful execution. Each goal and objective in the Plan has a timeline with a target completion date and one or more owners responsible for overseeing and coordinating its completion. Accomplishing the goals and objectives will require support and cooperation from various individuals, groups, or agencies. Regular governance body meetings will include formal agenda items for reviewing the progress of the Plan's implementation.

**Appendix B: Project Summary Worksheet** provides a list of cybersecurity projects to complete that tie to each goal and objective of the Cybersecurity Plan.

### Resource Overview and Timeline Summary

The implementation of this comprehensive cybersecurity plan will require collaboration, resources, and investments across the State of Alaska. The resources needed to execute this plan include funding, personnel, and technology.

Funding will be needed to support the implementation of cybersecurity tools and technologies, as well as to develop and execute training and awareness programs. Personnel will be required to support the implementation of the cybersecurity plan, including cybersecurity professionals to conduct risk

---

---

assessments, manage cybersecurity tools, and provide training to personnel. Technology investments will be necessary to enhance the security posture of the state's information systems and networks.

The timeline for implementing the cybersecurity plan is as follows, for the State, with corresponding support for local governments and Tribes to align their efforts to this schedule:

- Year 1: Conduct a comprehensive risk assessment of the state's information systems and networks, identify critical infrastructure, and key resources, and develop a cybersecurity training and awareness program for state personnel.
- Year 2: Implement additional cybersecurity tools and technologies, including endpoint protections, data loss prevention, and multifactor authentication. Continue to expand the use of the .gov domain and cybersecurity tools to boroughs and cities. Grantees can apply for funding to implement these tools.
- Year 3: Develop and implement a continuity of operations plan for cybersecurity incidents and conduct regular exercises to test the plan. Expand ongoing training, cyber incident exercises, and cybersecurity information sharing to support local entities.
- Year 4: Focus on workforce development, using the National Initiative for Cybersecurity Education (NICE) Workforce Framework to identify and mitigate any gaps in the state's cybersecurity workforce. Continue to leverage CISA services and expand information sharing agreements with local governments. Conduct a review of information technology and operational technology modernization to ensure alignment between cybersecurity objectives.
- Year 5: Develop and coordinate strategies to address cybersecurity risks and threats with other organizations, including consultation with local governments, neighboring entities, territories, and tribal governments. Ensure rural communities have adequate access to and can participate in cybersecurity services and activities.

These timelines are subject to change based on the availability of resources and other factors that may impact the state's ability to implement this comprehensive cybersecurity plan. The State of Alaska will regularly review and update this plan to ensure its effectiveness and relevance to the current cybersecurity landscape.

## APPENDIX A: SAMPLE CYBERSECURITY PLAN CAPABILITIES ASSESSMENT

COMPLETED BY PLANNING COMMITTEE				FOR ASSESSOR
Cybersecurity Plan Required Elements	Brief Description of Current Capabilities of SLTT within the Eligible Entity	Select capability level from: Foundational Fundamental Intermediary Advanced	Project # (s) <i>(If applicable – as provided in Appendix B)</i>	Met
1. Manage, monitor, and track information systems, applications, and user accounts	State agencies and some local jurisdictions currently manage, monitor, and track varying levels of information systems, applications, and user accounts	Foundational		
2. Monitor, audit, and track network traffic and activity	State agencies and some local jurisdictions currently monitor, audit, and track network traffic and activity	Foundational		
3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts	State agencies and some local jurisdictions engage in practices to enhance preparation, response, and resiliency	Foundational	1	
4. Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk	State agencies and some local jurisdictions engage in regular cybersecurity assessments and risk	Foundational	2	

	management activities			
5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST)	State agencies and some local jurisdictions implement the best practices listed in Plan Element 5	Foundational		
a. Implement multi-factor authentication	State agencies and some local jurisdictions implement MFA	Foundational		
b. Implement enhanced logging	State agencies and some local jurisdictions implement enhanced logging	Foundational		
c. Data encryption for data at rest and in transit	State agencies and some local jurisdictions utilize encryption for data at rest and in transit	Foundational		
d. End use of unsupported/end of life software and hardware that are accessible from the Internet	State agencies and some local jurisdictions exercise life cycle management practices to end use of unsupported/end of life software and hardware	Foundational		
e. Prohibit use of known/fixed/default passwords and credentials	State agencies and some local jurisdictions prohibit use of known/fixed/default password and credentials	Foundational		

f. Ensure the ability to reconstitute systems (backups)	State agencies and some local jurisdictions ensure the ability to reconstitute critical systems	Foundational		
g. Migration to the .gov internet domain	State agencies and some local jurisdictions have or plan to migrate to .gov	Foundational		
6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain	State agencies and some local jurisdictions promote the delivery of safe, recognizable and trustworthy online services	Foundational		
7. Ensure continuity of operations including by conducting exercises	State agencies and some local jurisdictions conduct exercises	Foundational		
8. Identify and mitigate any gaps in the cybersecurity workforces, enhance recruitment and retention efforts, and bolster the knowledge, skills, and abilities of personnel (reference to NICE Workforce Framework for Cybersecurity)	State agencies and some local jurisdictions identify and mitigate any gaps in the cybersecurity workforces	Foundational		
9. Ensure continuity of communications and data networks in the event of an incident involving communications or data networks	State agencies and some local jurisdictions ensure continuity of communications and data networks	Foundational		
10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the	State agencies and some local jurisdictions assess and mitigate cybersecurity risks	Foundational	2	

performance of information systems within the jurisdiction of the eligible entity	and threats to critical infrastructure			
11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department	State agencies and some local jurisdictions enhance capabilities to share cyber threat indicators and information	Foundational		
12. Leverage cybersecurity services offered by the Department	State agencies and some local jurisdictions leverage cybersecurity services offered by the Department	Foundational		
13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives	State agencies and some local jurisdictions implement modernization cybersecurity review process	Foundational		
14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats	State agencies and some local jurisdictions develop and coordinate strategies to address cybersecurity strategies and risks	Foundational		
15. Ensure rural communities have adequate access to, and participation in plan activities	State agencies and some local rural jurisdictions have adequate access to and participation in plan activities	Foundational		
16. Distribute funds, items, services, capabilities, or activities to local governments	State agencies are prepared to distribute grant funds and some services appropriately	Foundational	1	



## APPENDIX B: PROJECT SUMMARY WORKSHEET

**Purpose:** The **Project Summary Worksheet** is a list of cybersecurity projects that the entity plans to complete to develop or improve any needed cybersecurity capabilities identified in **Appendix A: Sample Cybersecurity Plan Capabilities Assessment**.

1. Rank	2. Project Name	3. Project Description	4. Related Required Element #	5. Cost	6. Status	7. Priority	8. Project Type
1	Statewide Cybersecurity Plan Refinement	Additional planning by Cybersecurity Planning Committee to refine the cybersecurity plan submission for FY2023	1, 2, 3, 4, 5, 6, 10, 12, 13, 14, 15, 16	\$20K (TBD)	Ongoing	High	Plan
2	Direct pass-through funds to eligible local government entities based on strength of application, demonstrated need, rural designation, and evidence of ability to sustain investment	Applications will be prioritized based on following identified cybersecurity components: <ul style="list-style-type: none"> <li>- Conduct vulnerability assessments</li> <li>- Implement multi-factor authentication</li> <li>- Implement enhanced logging</li> <li>- Data encryption for data at rest and in transit</li> <li>- End use of unsupported / end of life software and hardware that are accessible from the internet</li> <li>- Prohibit use of known/fixed/default passwords and credentials</li> <li>-Ensure ability to reconstitute systems (backups)</li> </ul>	1, 2, 3, 4, 5, 6, 8, 10, 12, 13, 14, 15, 16	\$XXM (TBD)	Future	High	Equip

## APPENDIX C: ENTITY METRICS

The below table should reflect the goals and objectives the Cybersecurity Planning Committee establishes.

Cybersecurity Plan Metrics		
Cybersecurity Plan Metrics		
Goal	Step	Key Performance Indicator
1. Enhance Cybersecurity Resilience and Interoperability by developing and implementing a comprehensive cybersecurity risk management program that incorporates the latest cybersecurity best practices and methodologies.	<ul style="list-style-type: none"> <li>Develop a comprehensive cybersecurity risk management program that incorporates the latest cybersecurity best practices and methodologies.</li> <li>Develop and implement a security awareness training program</li> </ul>	<ul style="list-style-type: none"> <li>Number of cybersecurity risk assessments conducted annually.</li> <li>Percentage of vulnerabilities remediated within a defined timeframe.</li> <li>Compliance with relevant cybersecurity regulations and standards</li> </ul>
2. Foster a Cybersecurity Culture by developing and delivering cybersecurity awareness and training programs to state employees, contractors, and local government personnel.	<ul style="list-style-type: none"> <li>Develop and deliver cybersecurity awareness and training programs to state employees, contractors, and local government personnel.</li> <li>Develop and implement a security awareness campaign to increase awareness and promote best practices</li> </ul>	<ul style="list-style-type: none"> <li>Number of training sessions conducted.</li> <li>Percentage of employees completing the training</li> <li>Number of reported security incidents related to employee behavior</li> </ul>

<b>Cybersecurity Plan Metrics</b>		
<b>Goal</b>	<b>Step</b>	<b>Key Performance Indicator</b>
<p>3. Enhance Cybersecurity Collaboration and Partnerships by developing and implementing a cybersecurity information sharing program with local governments, neighboring states, and federal agencies, and foster cybersecurity partnerships and collaborations with the private sector, academic institutions, and non-profit organizations.</p>	<ul style="list-style-type: none"> <li>• Develop and implement a cybersecurity information sharing program with local governments, neighboring states, and federal agencies.</li> <li>• Foster cybersecurity partnerships and collaborations with the private sector, academic institutions, and non-profit organizations</li> </ul>	<ul style="list-style-type: none"> <li>• Number of cybersecurity risk assessments conducted annually.</li> <li>• Percentage of vulnerabilities remediated within a defined timeframe.</li> <li>• Compliance with relevant cybersecurity regulations and standards</li> </ul>
<p>4. Improve Cyber Incident Management and Response Capabilities by developing and implementing a cybersecurity incident management plan that is tested and updated on a regular basis and establish a cybersecurity incident response team with appropriate roles and responsibilities and ensure that the team is trained and equipped to respond to cybersecurity incidents.</p>	<ul style="list-style-type: none"> <li>• Develop and implement a cybersecurity incident management plan that is tested and updated on a regular basis.</li> <li>• Establish a cybersecurity incident response team with appropriate roles and responsibilities and ensure that the team is trained and equipped to respond to cybersecurity incidents.</li> <li>• Conduct regular cybersecurity incident response exercises and drills</li> </ul>	<ul style="list-style-type: none"> <li>• Number of cybersecurity incident response exercises conducted annually.</li> <li>• Percentage of incidents handled within defined timeframes.</li> <li>• Effectiveness of incident response team in mitigating the impact of cybersecurity incidents.</li> </ul>

## APPENDIX D: ACRONYMS

Acronym	Definition
ISAC	Information Sharing and Analysis Center
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CSO	Chief Security Officer
SLCGP	State and Local Cybersecurity Grant Program
IT	Information Technology
SOC	Security Operations Center
ITOC	Information Technology Operations Center
MSSP	Managed Security Service Provider
CISA	Cybersecurity and Infrastructure Security Agency
MS-ISAC	Multi-State Information Sharing and Analysis Center
NIST	National Institute of Standards and Technology
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework
C-SCRM	Cyber Supply Chain Risk Management
COOP	Continuity of Operations
DHSEM	Division of Homeland Security and Emergency Management
THIRA	Threat and Hazard Identification and Risk Assessment
SPR	Security and Privacy Requirements
CIMS	Cyber Incident Management System
TLP	Traffic Light Protocol
CISCP	Certified Information Systems Cybersecurity Professional
AIS	Automated Information System
SLTT	State, Local, Tribal, and Territorial

## APPENDIX E: REQUIRED, ENCOURAGED, AND OPTIONAL SERVICES, MEMBERSHIPS, AND RESOURCES

All recipients and subrecipients of the Statewide Alaska Cybersecurity Grant Program (SLCGP) are required to participate in the following free services provided by the Cybersecurity and Infrastructure Security Agency (CISA). Please note that participation in these services is not mandatory for grant submission and approval but is a post-award requirement.

### REQUIRED SERVICES AND MEMBERSHIPS

#### Cyber Hygiene Services:

- **Web Application Scanning:** A service that assesses the health of publicly accessible web applications, identifies vulnerabilities, and recommends security enhancements.
- **Vulnerability Scanning:** Continuous scanning of public, static IPs for accessible services and vulnerabilities, providing weekly vulnerability reports and ad-hoc alerts.

To register for these services, email [vulnerability\\_info@cisa.dhs.gov](mailto:vulnerability_info@cisa.dhs.gov) with the subject line "Requesting Cyber Hygiene Services – SLCGP." In the body of your email, mention that you are requesting these services as part of the SLCGP. For more information, visit [CISA's Cyber Hygiene Information Page](#).

#### Nationwide Cybersecurity Review (NCSR):

The NCSR is an annual self-assessment that measures the cybersecurity programs' gaps and capabilities of state, local, and tribal (SLT) entities. It is based on the National Institute of Standards and Technology Cybersecurity Framework and sponsored by the Department of Homeland Security (DHS) and the Multi-State Information Sharing and Analysis Center (MS-ISAC). Entities and subrecipients should complete the NCSR annually.

For more information, visit the [Nationwide Cybersecurity Review \(NCSR\) website \(cisecurity.org\)](#).

### ENCOURAGED SERVICES, MEMBERSHIPS, AND RESOURCES

#### Membership in the Multi-State Information Sharing and Analysis Center (MS-ISAC) and/or Election Infrastructure Information Sharing and Analysis Center (EI-ISAC):

Recipients and subrecipients are strongly encouraged to become members of the MS-ISAC and/or EI-ISAC, as applicable. Membership is free.

The MS-ISAC: DHS-designated cybersecurity ISAC for SLT governments, providing services and information sharing to enhance their cybersecurity capabilities.

The EI-ISAC: Focuses on election infrastructure cybersecurity, offering cyber defense tools, threat intelligence products, incident response and forensics, cybersecurity awareness, and training.

To register, please visit the MS-ISAC registration page or the EI-ISAC registration page. For more information, visit [MS-ISAC \(cisecurity.org\)](#) and [Election Infrastructure Security \(cisa.gov\)](#).

## CISA Recommended Resources, Assessments, and Memberships (not mandatory):

The following resources, assessments, and memberships are recommended by CISA:

- [Cyber Resource Hub](#)
- [Ransomware Guide \(Sept. 2020\)](#)
- [Ransomware Readiness Assessment \(RRA\)](#)
- [Cyber Security Evaluation Tool \(CSET\)](#)
- [Malicious Domain Blocking and Reporting](#)
- [Cyber Resilience Review](#)
- [External Dependencies Management Assessment](#)
- [EDM Downloadable Resources](#)
- [Cyber Infrastructure Survey](#)
- [Validated Architecture Design Review](#)
- [CISA Services Catalog](#)
- [Free Public and Private Sector Cybersecurity Tools and Services](#)

For reporting a cybersecurity incident, visit CISA Central at [us-cert.gov/report](https://us-cert.gov/report). For additional CISA services, refer to the [CISA Services Catalog](#). Information on memberships can be found at the [Information Sharing and Analysis Organization Standards Organization](#).

Note: The inclusion of optional resources and memberships in this appendix does not imply mandatory participation but is provided for informational purposes and to support the enhancement of cybersecurity capabilities.

## APPENDIX F: KEY TERMS AND DEFINITIONS

**Alaska Cybersecurity Center:** An organization established in partnership with the Alaska Federation of Natives and the University of Alaska to provide training and research opportunities in cybersecurity.

**Alaska Federation of Natives:** A partner organization that launched the Alaska Native Cybersecurity Enhancement Project to train Alaska Natives in cybersecurity skills.

**Alaska Native Cybersecurity Enhancement Project:** A collaborative initiative aimed at providing cybersecurity training to Alaska Natives.

**Automated Indicator Sharing (AIS):** A capability provided by the Cybersecurity and Infrastructure Security Agency (CISA) that allows for the automated exchange of cyber threat indicators.

**Cloud-based Security Services:** Security services and tools offered by cloud service providers (CSPs) to protect and monitor network infrastructure and data stored in cloud environments.

**Collaborative Monitoring:** A cooperative approach where multiple entities within a jurisdiction share resources, data, and expertise to collectively monitor and respond to cybersecurity threats.

**Continuity of Operations (COOP) Planning:** Efforts to ensure the continuity of critical services and operations in the event of a cybersecurity incident.

**Continuity of Operations Plan (COOP):** A plan outlining actions and procedures to be taken during and after a cybersecurity incident to ensure the continuity of critical operations.

**Cross-Functional Team:** A team comprising professionals from different disciplines or areas of expertise working together to achieve a common cybersecurity goal.

**Cyber Incident Exercise:** Simulated exercises designed to test the response and resilience of entities in handling cybersecurity incidents.

**Cyber Information Sharing and Collaboration Program (CISCP):** A program operated by the Cybersecurity and Infrastructure Security Agency (CISA) that facilitates information sharing and collaboration among cybersecurity stakeholders.

**Cybersecurity Services:** Services provided by specialized organizations or agencies to support the prevention, detection, response, and recovery from cybersecurity incidents.

**Data Encryption:** The process of converting data into a coded form to prevent unauthorized access, ensuring its confidentiality and integrity.

**Data Loss Prevention (DLP):** Measures and technologies implemented to prevent the unauthorized disclosure or loss of sensitive data.

**Endpoint Protections:** Security measures and tools implemented on endpoints (e.g., computers, laptops, mobile devices) to protect against cyber threats.

**Funding Prioritization:** The allocation of resources and funding based on prioritized cybersecurity risks and threats.

**Gap Analysis:** The process of identifying gaps or deficiencies in cybersecurity capabilities and developing plans to address them.

**Governance Body:** A formal body responsible for overseeing the implementation and progress of the cybersecurity plan.

**Information Sharing:** The process of exchanging relevant and actionable information between organizations or entities to enhance situational awareness, threat detection, and incident response capabilities.

**Information Sharing Agreements:** Formal agreements established to facilitate the sharing of cyber threat indicators and related information with local governments and other stakeholders.

**Local Government:** The governing body responsible for the administration and governance of specific local jurisdictions within a state, such as counties, cities, towns, or municipalities.

**Managed Security Service Providers (MSSPs):** Companies or organizations that offer outsourced cybersecurity services to assist in monitoring, managing, and enhancing an organization's security posture.

**Mitigation:** Actions taken to reduce the impact of cybersecurity incidents and vulnerabilities.

**Modernization Review Process:** A systematic assessment of IT and OT systems to identify and mitigate cybersecurity risks and threats.

**Monitoring:** The process of observing and collecting data or information to track the performance, behavior, or status of a system, network, or activity.

**Multi-State Information Sharing and Analysis Center (MS-ISAC):** An organization that facilitates the sharing of cyber threat information and collaboration among states.

**Multifactor Authentication:** A security mechanism that requires the use of multiple factors (e.g., password, biometric, token) for user authentication.

**National Initiative for Cybersecurity Education (NICE) Workforce Framework:** A framework used to categorize and describe cybersecurity work roles and required competencies.

**Network Activity:** Actions and interactions occurring within a computer network.

**Network Traffic:** The flow of data packets transmitted over a computer network.

**NIST 800-53:** A set of security and privacy controls published by the National Institute of Standards and Technology (NIST) for federal information systems and organizations.



**Prevention:** Activities and measures aimed at preventing cybersecurity incidents and mitigating potential risks.

**Protection:** Measures implemented to safeguard critical infrastructure and key resources from cybersecurity threats.

**Public-Private Partnerships:** Collaborative efforts between public and private sector organizations to address cybersecurity challenges and share resources.

**Real-Time Indicator Feeds:** Timely and up-to-date information feeds containing indicators of emerging cyber threats and vulnerabilities.

**Recovery:** Activities undertaken to restore and recover systems and operations following a cybersecurity incident.

**Response:** Coordinated efforts to address and mitigate the effects of cybersecurity incidents when they occur.

**Risk Assessment:** The process of identifying, analyzing, and evaluating potential risks and vulnerabilities to determine their potential impact and likelihood.

**Security Patches and Updates:** Software updates or fixes released by vendors to address identified vulnerabilities and enhance system security.

**Self-Assessment:** An evaluation conducted by grantees themselves to assess their own cybersecurity preparedness and identify areas for improvement.

**SLTTs (State, Local, Tribal, and Territorial):** Refers to the collective entities comprising state governments, local governments, tribal governments, and territorial governments.

**Stakeholder Preparedness Review (SPR):** A federally required review conducted every three years to assess the preparedness of stakeholders in addressing threats and hazards.

**Territorial Government:** The governing body responsible for the administration and governance of a specific territory or territorial possessions under the jurisdiction of a country.

**Threat and Hazard Identification and Risk Assessment (THIRA):** A federally required assessment conducted every three years to identify and evaluate threats, hazards, and risks.

**Threat Mitigation Practices:** Measures and actions taken to reduce or eliminate cybersecurity risks and threats.

**Traffic Light Protocol (TLP):** A framework used to classify and control the dissemination of sensitive incident-related information.

**Tracking:** The process of tracing and recording the movement or progress of something.

**Tribal Government:** The governing body responsible for the administration and governance of Native American tribes or indigenous communities within a country.

**Vulnerability Management:** The process of identifying, assessing, and addressing vulnerabilities in information systems, applications, and user accounts.

**Certificate Of Completion**

Envelope Id: E85C5188711042D281F52623E8DDFF10	Status: Completed
Subject: Complete with DocuSign: SoA SLCGP Cybersecurity Plan (Final Draft).docx	
Source Envelope:	
Document Pages: 34	Signatures: 2
Certificate Pages: 4	Initials: 0
AutoNav: Enabled	Envelope Originator:
Envelope Stamping: Disabled	Bill Smith
Time Zone: (UTC-09:00) Alaska	PO Box 110206
	Juneau, AK 99811
	bill.smith@alaska.gov
	IP Address: 158.145.14.25


**Record Tracking**

Status: Original	Holder: Bill Smith	Location: DocuSign
8/10/2023 2:48:48 PM	bill.smith@alaska.gov	
Security Appliance Status: Connected	Pool: StateLocal	
Storage Appliance Status: Connected	Pool: State of Alaska	Location: DocuSign

**Signer Events**

Bill Smith  
 bill.smith@alaska.gov  
 CIO  
 State of Alaska Office of Information Technology  
 Security Level: Email, Account Authentication (None)

**Signature**

DocuSigned by:  
  
 DFC79A53C0734CD...  
 Signature Adoption: Uploaded Signature Image  
 Using IP Address: 10.2.15.7

**Timestamp**

Sent: 8/10/2023 2:50:34 PM  
 Viewed: 8/10/2023 2:50:44 PM  
 Signed: 8/10/2023 2:50:55 PM

**Electronic Record and Signature Disclosure:**

Accepted: 3/9/2022 11:45:27 AM  
 ID: bc6ab434-c70f-461d-9daf-26bbb2fbe1a5  
 Company Name: State of Alaska

Bryan J Fisher  
 b.fisher@alaska.gov  
 Security Level: Email, Account Authentication (None)

DocuSigned by:  
  
 F327D0318DCB47B...  
 Signature Adoption: Uploaded Signature Image  
 Using IP Address: 158.145.14.24

Sent: 8/10/2023 2:50:56 PM  
 Viewed: 8/10/2023 3:19:23 PM  
 Signed: 8/10/2023 3:19:53 PM

**Electronic Record and Signature Disclosure:**

Accepted: 8/10/2023 3:19:23 PM  
 ID: 1a8da33d-2794-4ad4-bac5-a356a3c0f9f6  
 Company Name: State of Alaska

**In Person Signer Events      Signature      Timestamp**

**Editor Delivery Events      Status      Timestamp**

**Agent Delivery Events      Status      Timestamp**

**Intermediary Delivery Events      Status      Timestamp**

**Certified Delivery Events      Status      Timestamp**

**Carbon Copy Events      Status      Timestamp**

Bill Dennis  
 bill.dennis@alaska.gov  
 Administrative Operations Manager  
 Security Level: Email, Account Authentication (None)

**COPIED**

Sent: 8/10/2023 3:19:55 PM

<b>Carbon Copy Events</b>	<b>Status</b>	<b>Timestamp</b>
---------------------------	---------------	------------------

**Electronic Record and Signature Disclosure:**  
Accepted: 5/24/2021 7:33:16 AM  
ID: 41c94d05-9122-462a-bc2a-1005b430e143  
Company Name: State of Alaska

<b>Witness Events</b>	<b>Signature</b>	<b>Timestamp</b>
-----------------------	------------------	------------------

<b>Notary Events</b>	<b>Signature</b>	<b>Timestamp</b>
----------------------	------------------	------------------

<b>Envelope Summary Events</b>	<b>Status</b>	<b>Timestamps</b>
--------------------------------	---------------	-------------------

Envelope Sent	Hashed/Encrypted	8/10/2023 2:50:34 PM
Certified Delivered	Security Checked	8/10/2023 3:19:23 PM
Signing Complete	Security Checked	8/10/2023 3:19:53 PM
Completed	Security Checked	8/10/2023 3:19:55 PM

<b>Payment Events</b>	<b>Status</b>	<b>Timestamps</b>
-----------------------	---------------	-------------------

<b>Electronic Record and Signature Disclosure</b>
---

## **ELECTRONIC RECORD AND SIGNATURE DISCLOSURE**

Please read this Electronic Records and Signature Disclosure (ERSD). It concerns your rights regarding electronically undertaking, and the conditions under which you and the State of Alaska agree to electronically undertake, the transaction to which it relates (the "TRANSACTION").

### **Consent to Electronically Undertake the TRANSACTION**

You can electronically undertake the TRANSACTION only if you confirm that you meet the following requirements by selecting the box next to "I agree to use electronic records and signature" (the "AGREE BOX"):

1. you can fully access and have read this ERSD;
2. you can fully access all of the information in the other TRANSACTION records;
3. you can retain all of the TRANSACTION records in a form that you will be able to fully access for later reference;
4. you consent to undertake the TRANSACTION electronically; and
5. you are authorized to undertake the TRANSACTION. (Please note that falsely undertaking the TRANSACTION may subject you to civil liabilities and penalties and/or to criminal penalties.)

If you cannot or are not willing to confirm each of these five things, do not select the AGREE BOX.

### **Withdrawing Consent**

If you select the AGREE BOX, you can withdraw your consent to electronically undertake the TRANSACTION at any time before you complete the TRANSACTION: simply do not finalize it. The only consequence of withdrawing your consent is that you will not finalize the TRANSACTION.

If you select the AGREE BOX, your consent will apply only to this TRANSACTION. You must separately consent to electronically undertake any other transaction with the State of Alaska.

### **Paper Option for Undertaking the TRANSACTION**

You may undertake the TRANSACTION with the State of Alaska using paper records. (State of Alaska employees who want to undertake the TRANSACTION in paper should contact the agency responsible for the TRANSACTION.) Print the paper records on the website of the State of Alaska agency responsible for the TRANSACTION, or request them from the agency. The State of Alaska homepage is at <http://alaska.gov/>.

### **Copies of TRANSACTION Records**

After completing the TRANSACTION but before closing your web browser, you should download the TRANSACTION records. Or you can download the records within 30 days after

completing the TRANSACTION using the link in the DocuSign email sent to the email address you used to complete the TRANSACTION. The State of Alaska will not provide a paper copy of the TRANSACTION records as part of the TRANSACTION. Under the Alaska Public Records Act (APRA), AS 40.25.100–.295, you can request a copy from the agency responsible for the TRANSACTION, but if too much time has passed, the agency may no longer have the records when you make your request. If required under the APRA, the agency will charge a fee.

### **Required Hardware and Software**

For the minimum system requirements to electronically undertake the TRANSACTION, including accessing and thereby retaining the TRANSACTION records, visit <https://support.docusign.com/guides/signer-guide-signing-system-requirements>. These requirements may change. In addition, you need access to an email account.

### **How to Contact the State of Alaska**

To ask a question on this ERSD or the DocuSign document generated after you complete the TRANSACTION or on using DocuSign to electronically undertake the TRANSACTION, contact the Alaska Department of Administration at either of the following addresses:

State of Alaska  
Department of Administration  
550 West 7th Avenue  
Suite 1970  
Anchorage, AK 99501  
Reference: DocuSign

doa.commissioner@alaska.gov  
Subject: DocuSign

To ask any other question on the TRANSACTION records or to update the information for contacting you electronically, contact the State of Alaska agency responsible for the TRANSACTION using the contact information in the TRANSACTION records or, if those records contain no contact information, using the contact information on the agency's website. Again, the State of Alaska homepage is at <http://alaska.gov/>.