STATE OF MAINE CYBERSECURITY PLAN

Developed in fulfillment of the State and Local Cybersecurity Grant Program

September 2023

Created in consultation with Tidal Basin Government Consulting

TABLE OF CONTENTS

LETTER FROM THE PLANNING COMMITTEE

Greetings,

The State and Local Cybersecurity Grant Program (SLCGP) Planning Committee is pleased to present the Fiscal Year 2022 - 2023 State of Maine Cybersecurity Plan (Plan). The Plan represents Maine's continued commitment to strengthening cybersecurity and meets the requirements of the SLCGP outlined by the U.S. Department of Homeland Security (DHS).

Supported by the Maine Office of Information Technology (MaineIT) and the Maine Emergency Management Agency (MEMA), the SLCGP Planning Committee developed this Plan with goals and objectives that focus on fostering partnerships, cybersecurity training and awareness initiatives, essential shared services, and executing requirements of the SLCGP to enable future funding allocations.

Organizations across Maine are currently facing a daunting and complex cyber threat landscape and lack the resources to tackle this challenge independently. This Plan provides a strategic roadmap to increase Maine's defensive posture through a whole-of-state approach, seeking to provide a common direction for the many cybersecurity initiatives underway at the organizational, regional, and statewide levels. This Plan does not mandate requirements upon organizations in Maine, nor does it supersede any organization's existing plans.

The success of this effort is critical to all who call Maine "home" and will require federal, state, and local organizations to partner to strengthen the State's information systems, networks, and critical infrastructure. We look forward to working with you as we move this Plan forward to improve cyber resilience statewide.

Sincerely,

(Original document is signed)

Nicholas Marquis – Co-Chair
Acting State Chief Information Officer
Maine Office of Information Technology
State of Maine

Nathan Willigar – Co-Chair
State Chief Information Security Officer
Maine Office of Information Technology
State of Maine

Peter Rogers
Director
Maine Emergency Management Agency

INTRODUCTION

Executive Summary

This Plan represents Maine's continued commitment to strengthening cybersecurity. This Plan fulfills Maine's requirements under the State and Local Cybersecurity Grant Program (SLCGP), enabling Maine's participation in this first-of-its-kind national program. The SLCGP is a federal grant program administered by the United States Department of Homeland Security (DHS) and funded by the Infrastructure Investment and Jobs Act (IIJA). This Plan describes the State of Maine's approach to provide local governments the opportunity to participate in shared cybersecurity services and resources. The priorities and objectives contained in this Plan focus on improving the cybersecurity posture of state, local, and territorial (SLT) government organizations by providing assistance for managing and reducing systemic cyber risk. The Maine Emergency Management Agency (MEMA) and Maine Office of Information Technology (MaineIT), supported by the SLCGP Planning Committee, participated in an iterative planning process from February – September of 2023 to develop this Plan. The SLCGP Planning Committee serves as a representative voice for local input, and includes representation from state, county, and local government, public education, public health, public safety, emergency communications, election infrastructure, the judicial system, public critical infrastructure, and the Maine National Guard (full list of members is available in Appendix C). To collect local government input and inform Maine's SLCGP approach and programmatic offerings, a survey was distributed to municipalities, counties, and school districts. The survey approach is described further in the Assess Capabilities section of this Plan. This Plan is a living document that will be reevaluated regularly based on changes to the cybersecurity landscape, stakeholder input, and SLCGP guidance and requirements. The vision for the plan is, "A cyber-resilient Maine that realizes the opportunities afforded by technological innovation and balances the cybersecurity protections necessary to safeguard its data and critical infrastructure."

Planning Assumptions

- Maine is considered a strong "home rule" state, and the state constitution delegates broad home rule ordinance powers to municipal governments. Like the rest of New England but in contrast to the rest of the country, Maine has strong municipal governments. Elections for example are administered at the municipal level.
- Local governments[1] referenced throughout this Plan are defined as:
  - A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments, regional or interstate government entity, or agency or instrumentality of a local government.
  - An Indian tribe or authorized tribal organization.[2]
  - A rural community, unincorporated town or village, or other public entity.
- Individual organizations vary in cybersecurity capabilities, but a common theme across the State is a lack of dedicated staff and the fiscal resources necessary to meet increasing cybersecurity requirements and sustainably implement best practices.
- The State of Maine maintains information systems, assets, and networks that are accessed by certain organizations and may be accessed by the public when external facing. Local governments maintain information systems, assets, and networks. Nothing in this Cybersecurity Plan mandates technical-level cybersecurity requirements for information systems, assets, and networks owned by these entities. The State's role in the SLCGP is that of a leader and convener; individual organizations are not mandated to participate in State-led SLCGP initiatives.
- While this Plan incorporates the role of the State as a service provider to achieve economies of scale that effectively build cyber resilience statewide, this approach also recognizes the important authorities, roles, and responsibilities of individual local governments in Maine. The counties and Maine Municipal Association will be critical partners in efforts to ensure services meet the needs of local government. Every effort will be made to ensure that the shared services model incorporates a risk-based approach that reaches their foundational needs and strengthens the cyber

[1] 6 U.S.C. § 101(13)
[2] Federal guidance indicates a Tribal Cybersecurity Grant Program funding stream and Notice of Funding Opportunity will be announced. Anticipating this announcement, Maine's initial SLCGP assessment did not include tribes.

resilience of our State's rural communities. The Plan is intended to augment their capabilities to reduce cyber risk, strengthen their security postures, and enhance their defenses against emerging cyber threats. The Committee will continue to explore, based on annual cyber needs assessments and ongoing work with state and local partners, whether the Plan requires any modification to the shared services model approach including but not limited to possible individual grant opportunities for local government partners and/or direct investment in local cybersecurity infrastructure in the future to best reflect the needs of the State as a whole.

- The solutions identified in this Cybersecurity Plan include short-term, long-term, and enduring initiatives to address key known and emerging vulnerabilities and align with the SLCGP Notice of Funding Opportunity (NOFO) criteria.
- **The cessation of the SLCGP funding would eliminate cybersecurity initiatives outlined in this plan without viable alternate funding sources. Therefore, it is assumed**:
  - The State will continue to provide matching funds for the SLCGP, ensuring future federal funding allocations.
  - The federal government will continue to provide SLCGP funding as well as programmatic guidance and support beyond the first four fiscal years of the program.
- MEMA will maintain the capacity to act as the State Administrative Agency (SAA), performing essential SLCGP grant management activities. MaineIT will coordinate the Planning Committee and serve as the technical lead for cybersecurity initiatives to implement the SLCGP. The Department of the Secretary of State (SoS) will coordinate with MEMA, MaineIT and the Planning Committee on cybersecurity initiatives unique to elections critical infrastructure.
- Nothing in this plan restricts, supersedes, or otherwise replaces the legal authorities or regulatory responsibilities of any government agency or organization. All information will be handled, transmitted, distributed, released, and/or stored in accordance with applicable laws and policies.

Introduction

The Cybersecurity Plan is a strategic planning document that contains the following components:[3]

- **Vision and Mission** articulate the Planning Committee's vision for improving statewide cybersecurity and their mission to coordinate its implementation.
- **Goals and Objectives** outlines the strategic goals and tactical objectives that will guide SLCGP implementation.
- **Cybersecurity Plan Elements** outlines the desired future state of cybersecurity across each of the 16 required elements of the SLCGP, as detailed in the NOFO.
- **Funding and Services** details the SLCGP funding source and the State's allocation. This section also describes the State's strategy and methods for distributing SLCGP funds to eligible stakeholders.
- **Assess Capabilities** provides a high-level overview of the methodology used to obtain feedback and input from local governments through a statewide cybersecurity survey.
- **Implementation Plan** describes the current roles and responsibilities of key organizations that are relevant to implementation of this Plan.
- **Appendix A: Project Summary Worksheet** provides a high-level overview of SLCGP projects.
- **Appendix B: Metrics** describes how the State will measure progress and success of the projects.
- **Additional Appendices include:** Planning Committee Members/Core Team and Staff Members, Organization Roles and Responsibilities, Acronyms, Glossary, and References, Plan Signatures and a Record of Changes

The Cybersecurity Plan has also been informed by and is in alignment with the following:

- **Maine Economic Development Strategy** (2020-2029) outlines seven strategies to help Maine achieve its vision of "a diverse and sustainable economy for all." Economic development strategies to grow local talent and attract new talent align with cybersecurity workforce development efforts under the SLCGP. Economic development strategies to expand or modernize services in Maine through online platforms require secure State infrastructure.
- **State of Maine Information Security Strategic Plan** (2021-2026) outlines the vision, mission and goals of the MaineIT Information Security Office and the initiatives to implement them.

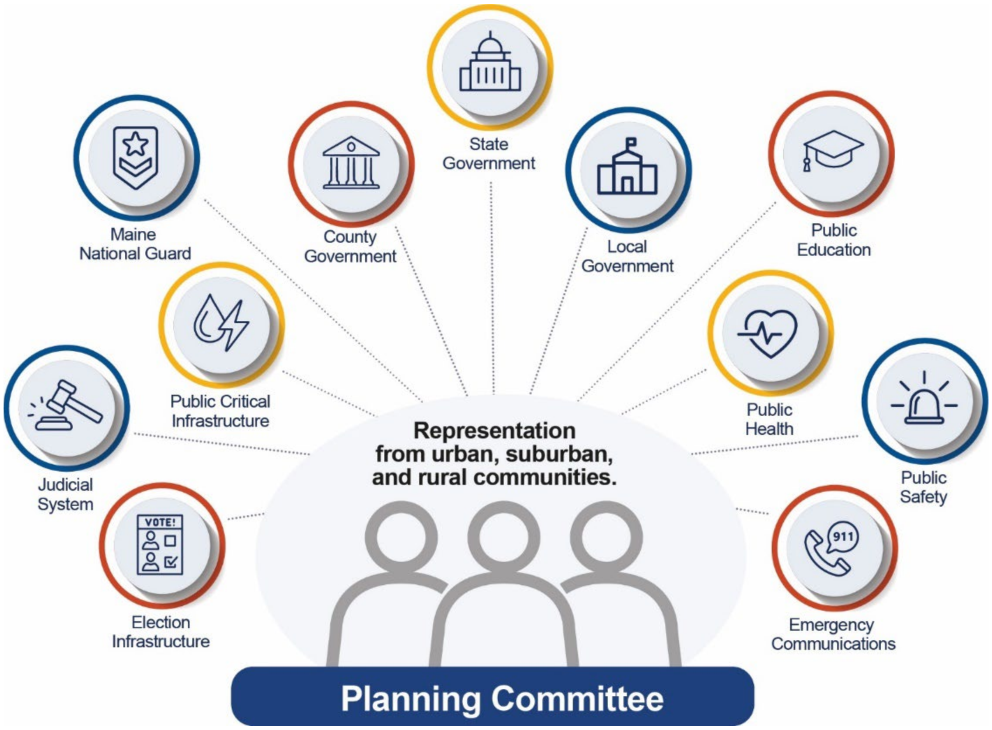
[3] CISA SLCGP Cybersecurity Plan Template

- **State of Maine Homeland Security Strategy** (2023-2025) identifies a statewide strategic direction to prevent and reduce the vulnerability of Maine from acts of terrorism. Cybersecurity is identified as a State Priority, with the goal of "enhancing cybersecurity awareness and practices across the whole community." The initiatives (objectives) to implement this goal are coordinated by the Cybersecurity State Priority Area Working Group.
- **State of Maine Communication Interoperability Plan**[4] (March 2023) outlines Maine's vision, mission, goals, and objectives for improving emergency communications interoperability and supporting public safety practitioners. It also includes Maine's self-assessment of interoperability maturity. The initiatives to implement its goals are coordinated by the Maine Interoperable Communications Committee (MICC).
- **Best practices** gleaned from analysis from other states' SLCGP Cybersecurity Plans and adapted for Maine.

Organization Roles and Responsibilities

Appendix D lists the organizations that are integral to SLCGP implementation in Maine and their roles and responsibilities, including individual organizations (i.e.: local governments), State Agencies, and Advisory Groups. State Agencies listed include those with key roles and responsibilities in cybersecurity, including MaineIT, MEMA, the SoS, the Maine Intelligence and Analysis Center (MIAC), the Maine National Guard (MENG), and the Maine Department of Education. In addition, the roles of the Cybersecurity Advisory Council, SLCGP Planning Committee and Homeland Security Advisory Council are defined.

Composition of Maine's SLCGP Planning Committee



[4] State of Maine Communication Interoperability Plan

Vision and Mission

This section describes the State's vision and mission for improving resiliency and maintaining cybersecurity.

Vision

A cyber-resilient Maine that realizes the opportunities afforded by technological innovation and balances the cybersecurity protections necessary to safeguard its data and critical infrastructure.

This vision is guided by the following principles:

- **Build and leverage partnerships**. Focus on building relationships with partners across Maine and maintaining open lines of communication with critical infrastructure sector leads to ensure a coordinated approach to implementing SLCGP initiatives.
- **Reduce barriers**. Strive to understand what barriers organizations face in implementing cybersecurity best practices and identify collective approaches to overcome them.
- **Increase resiliency**. Build capability and capacity at the organizational level to ensure the impact of these cybersecurity initiatives is enduring and sustainable.

Mission

The State of Maine will lead and coordinate initiatives to reduce cybersecurity risks against State and local government-owned or operated information systems, mitigating the impacts on Maine's essential services and community members.[5]

Cybersecurity Program Goals and Objectives

The State of Maine's cybersecurity goals and objectives include the following:

Cybersecurity Program	
Goals	**Objectives**
1. Identify, develop, and maintain partnerships.	1.1. Produce a comprehensive set of contacts inclusive of State and local government partners to facilitate future outreach, training, and resource offerings.
2. Enable cybersecurity training and awareness activities.	2.1. Provide centrally managed security awareness training for end users in qualifying entities. 2.2. Increase practitioners' awareness and implementation of federally offered free and fee-based cybersecurity resources.
3. Empower local governments to leverage essential shared services.	3.1. Provide multifactor authentication (MFA) services to qualifying entities to implement on their networks. 3.2. Provide a comprehensive service to qualifying entities to evaluate the capability of a .gov domain structure and support turnkey migration. 3.3. Provide an Endpoint Detection and Response (EDR) service to qualifying entities to monitor threat activity across Maine.
4. Execute requirements of the State and Local Cybersecurity Grant Program.	4.1. Maintain and refine the SLCGP Cybersecurity Plan. 4.2. Develop and document roles and responsibilities for State and local governments during cybersecurity incident response.

[5] *Cybersecurity Risk - An effect of uncertainty on or within information and technology. Cybersecurity risks relate to the loss of confidentiality, integrity, or availability of information, data, or information (or control) systems and reflect the potential adverse impacts to organizational operations (i.e., mission, functions, image, or reputation) and assets, individuals, other organizations, and the Nation. (Definition based on ISO Guide 73 [6] and NIST SP 800-60 Vol. 1 Rev. 1 [7])*

CYBERSECURITY PLAN ELEMENTS

The cybersecurity program goals and objectives aim to improve strategic capabilities in these Cybersecurity Plan elements. These plan elements represent tenets of a reasonable cybersecurity readiness. Within each element described, objectives are identified to address improvement. Improvements in some elements may be directly funded and some elements may be improved indirectly through objectives such as education and outreach. Appendix A displays a project summary by objective with the elements that are included.

Manage, Monitor, and Track

Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.

Entities should establish procedures and processes to manage, monitor, and track their assets (e.g., hardware, cloud services, information systems, applications, user accounts, etc.). By identifying all cybersecurity-related assets, entities can be better prepared to detect and respond to vulnerabilities.[6]

Recognizing the many barriers to implementing these procedures and processes, entities are encouraged to leverage low and no-cost resources that can improve continuous monitoring capabilities immediately, such as the Center for Internet Security (CIS) Hardware and Software Asset Tracker (no-cost federal resource) or other open-source tools. As outlined in Objective 2.2, education and outreach activities will be coordinated to increase the awareness and implementation of these resources. Additionally, the long-term goal of implementing Endpoint Detection and Response (Objective 3.3) will provide a resource to entities that may lack independent capacity.

Monitor, Audit, and Track

Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.

Entities should leverage services and solutions to monitor, audit, and track network activity. By maintaining situational awareness of their networks, entities are better positioned to efficiently and effectively respond to cyberattacks and maintain continuity of services.

Entities are encouraged to leverage no-cost federal offerings to improve continuous monitoring capabilities, such as the Cybersecurity and Infrastructure Security Agency (CISA)-provided vulnerability scanning, Malicious Domain Blocking and Reporting, and threat notification services offered by Multi-State Information Sharing and Analysis Center (MS-ISAC) and Elections Infrastructure Information Sharing and

[6] CISA Cross-Sector Cybersecurity Performance Goals

Analysis Center (EI-ISAC). As outlined in Objective 2.2, education and outreach activities will be coordinated to increase the awareness and implementation of these offerings. Additionally, the long-term goal of implementing Endpoint Detection and Response (Objective 3.3) will provide a resource to entities that may lack independent capacity.

Enhance Preparedness

Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.

Comprehensive preparedness requires a coordinated effort to plan, organize, equip, train, and exercise to foster a culture of security and cyber awareness beyond incident response.

Entities are encouraged to leverage no-cost federal offerings to enhance organizational resiliency, such as CISA's Cyber Resiliency Review, CISA & MS-ISAC's Ransomware Guide, ISAC incident response and policy templates, and CIS Secure Suite. As outlined in Objective 2.2, education and outreach activities will be coordinated to increase the awareness and implementation of these offerings.

MEMA, SoS and MaineIT will lead and coordinate efforts through the Planning Committee to encourage public-sector training providers, such as the Maine Municipal Association, the Maine School Safety Center, County Emergency Management Agencies, etc., to incorporate federal offerings into their training and awareness programs. These federal offerings include accredited training, exercise planning, and exercise conduct support services offered by the National Domestic Preparedness Consortium (NDPC), which includes FEMA, CISA, and other emergency management partners.

Assessment and Mitigation

Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.

Entities are encouraged to establish risk management practices to identify, assess, and address threats to their information systems, applications, and user accounts. Through risk management, entities can prioritize threats and allocate resources accordingly. This may be achieved through continuous monitoring and regular assessments to ensure adequate controls and practices are in place.

Education and outreach activities will be coordinated to provide entities with information about the free federal offerings that can be leveraged beyond the resources of the SLCGP (Objective 2.2). Examples of these offerings include the Ransomware Readiness Assessment by CISA, the MS-ISAC and EI-ISAC, and the CIS Controls Self-Assessment Tool (CSAT) Ransomware Business Impact Analysis tool.

Prior to receiving any resources through the SLCGP, Maine's subrecipients will be required to participate in CISA's Cyber Hygiene Vulnerability Scanning program, which provides a report of identified vulnerabilities. This requirement is put forth by CISA.

Best Practices and Methodologies

Ensure that the state or local governments within the state adopt and use best practices and methodologies to enhance cybersecurity.

The following cybersecurity best practices will be prioritized in SLCGP-funded projects:

- Implementation of multifactor authentication (Objective 3.1). MFA is an authentication system that requires more than one distinct factor for successful authentication. This can be performed using a multifactor authenticator or by a combination of authenticators that provide different factors (something you know, something you have, and something you are). Overall, the implementation of MFA is crucial for enhancing security, protecting against various attack vectors, and ensuring the integrity of digital systems and sensitive information. It is a proactive measure that significantly reduces the risk of unauthorized access.
- Migration to the .gov internet domain (Objective 3.2). The State's efforts to migrate to the .gov internet domain is detailed in the Safe Online Services section of this Plan.

The following cybersecurity best practices are currently beyond the initial resources of the SLCGP for direct implementation. However, education and awareness activities (Objective 2.2) will incorporate content on the following best practices:

- Implementing enhanced system and security logging and retention
- Encryption of data at rest and in transit
- Ending use of unsupported / end-of-life software and hardware that are accessible from the internet
- Prohibiting use of known/fixed/default passwords and credentials[7]
- Ensuring the ability to reconstitute systems through backups
- Adopton of the National Institute of Standards and Technology (NIST) cybersecurity framework
- Implementing cyber supply chain risk management practices to identify, prioritize, and assess IT suppliers, vendors, and service providers in order to understand cascading risks to the entity's supply chain
- Identification of the existing knowledge bases of adversary tools and tactics available through MS-ISAC, EI-ISAC, CISA, and other partners

Safe Online Services

Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.

[7] In ongoing initiatives coordinated by the SoS, Maine's municipalities will be required to use NIST-compliant passwords and multifactor authentication to access election infrastructure. Through this effort, municipal passwords and credentials will be strengthened.

Publicly-owned and operated online services, such as State and local government websites and email systems, are common targets for cyber attacks. The use of the .gov top-level domain fosters public trust in the authenticity of government communications and enhances cybersecurity. Maine's community members who navigate to .gov websites, or contact State or local government employees with .gov email addresses can maintain confidence that they are engaging with legitimate government organizations. SoS and MEMA will incorporate education about .gov websites and best practices for safe online web browsing into existing public outreach initiatives.

Entities who have not migrated to the .gov domain will be encouraged to participate in a managed service to assist with this migration (Objective 3.2). This migration will result in secondary security benefits, such as continuous monitoring of those websites by CISA for cybersecurity issues. Entities who are not eligible for or interested in migration to the .gov domain are encouraged to use Hypertext Transfer Protocol Secure (HTTPS) encryption on their websites to ensure authenticity.

Continuity of Operations

Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.

Maine residents expect that critical government services will continue to function with minimal disruption in the event of an emergency or major disaster.[8] To this end, MaineIT coordinates the State's strategy for Business Continuity / Disaster Recovery to ensure that State government can be restored to normal or near-normal operations as quickly as possible.

Entities are encouraged to leverage no-cost federal offerings to enhance continuity planning and organizational capability in the event of a cyber incident. These offerings include the CISA Exercise Teams and toolkits for conducting continuity exercises and the capabilities of the MS-ISAC and CIS Cyber Incident Response Team in the event of a cyber incident. Externally, MEMA provides continuity planning guidance and training to interested entities to build statewide capacity. Education and outreach activities will be coordinated by MEMA, MaineIT and other public and private partners to increase the awareness and implementation of these offerings (Objective 2.2).

Workforce

Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.

[8] MaineIT Business Continuity and Disaster Recovery Policy

Maine faces workforce recruitment and retention challenges across many industries. Complementary efforts are underway through Maine's Economic Development Strategy and the Maine Jobs and Recovery Plan, which includes statewide workforce investments to support recovery from the COVID-19 pandemic. Independent of the SLCGP, the University of Maine System (UMS) and its member institutions of higher education have established the Maine Cybersecurity Center (MCC) to provide the State with a trained cybersecurity workforce, aligned with the NICE Cybersecurity Workforce Framework.[9] Additionally, the UMS hosts the Maine Cyber Range to support cyber education and workforce development.[10] Institutions of higher education are closing the workforce gap through efforts such as Project Sentinel.[11] The Planning Committee will serve in a coordinating capacity for these types of independent workforce development efforts as appropriate, amplifying communications about existing efforts to their respective constituencies.

In any organization, end users remain the weakest link in cybersecurity, even with advanced security technologies and governance measures in place. Many cyber incidents occur due to accidental or negligent human error, such as falling victim to phishing scams, using weak passwords, or clicking on malicious links. Security awareness training educates end users about potential risks, best practices, and the importance of maintaining security protocols. The Planning Committee will enable cybersecurity awareness through centrally managed security awareness training (Objective 2.1) and outreach to practitioners regarding the myriad of free and fee-based cybersecurity resources (Objective 2.2).

Continuity of Communication and Data Networks

Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.

The State Interoperable Communications Plan (SCIP) outlines the strategic approach to improving emergency and public safety communications interoperability. Several of the goals identified in the SCIP may increase resiliency of communications and data networks:

- Goal #1, to reinvigorate the Maine Interoperable Communications Committee (MICC), includes the sub-objective to establish a funding working group to support broader outreach and inform stakeholders of funding opportunities which support long-term goals.
- Goal #4, to provide outreach on interoperability topics and establish appropriate notification methods for the emergency communications community, includes the sub-objective to establish a cybersecurity working group. This working group will provide information on cybersecurity best practices and current threats.
- Goal #5, to provide interoperable communications trainings, includes a sub-objective to develop a progressive cybersecurity training and exercise plan. Coordination of this effort may include training academies/authorities, MEMA, County Emergency Management Agencies, and the cybersecurity working group.

Ensuring the continuity of *all* data networks and communications across Maine is beyond the scope of the SLCGP and presents a significant risk to the state. Continuous refinement of this vulnerability will be

[9] Maine Cybersecurity Center, University of Maine System
[10] Maine Cyber Range, University of Maine at Augusta
[11] "Thomas College Receives Federal Grant for Growth of Cybersecurity Programs." May 24, 2023.

accomplished by leveraging the aggregated information provided by participants of the Nationwide Cybersecurity Review (NCSR).

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

Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to Maine's critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state

MEMA manages the Critical Infrastructure Protection Program in Maine, serving as a resource coordinator between the 16 sectors of critical infrastructure, local governments, and key state and federal agencies. MEMA's Critical Infrastructure Protection Officer works closely with state and federal agencies, including CISA and the MIAC, to liaise with public and private sector critical infrastructure partners during emergencies as well as day-to-day operations to enhance preparedness and protection.

The vast majority of critical infrastructure is owned and operated by the private sector. Assessing and mitigating cybersecurity risks and threats to all critical infrastructure and key resources is beyond the scope of the SLCGP, has limited federal resource offerings, and is beyond the capacity of the State to currently implement with existing resources. Election infrastructure however is wholly public infrastructure. The SoS, MaineIT and MEMA will partner to assess risks and coordinate mitigation through the SoS. The State of Maine will monitor the growth and evolution of threats to critical infrastructure through assessment data provided by the NCSR, and high-level assessments such as the Stakeholder Preparedness Review (SPR) and Threat and Hazard Identification and Risk Assessment (THIRA) coordinated by MEMA. The SPR and THIRA assess the State government's capabilities across 32 core capabilities, including cybersecurity. Understanding the risks and vulnerabilities to critical infrastructure will better position the State to align federal and State funding to mitigate threats and gaps in the future.

Cyber Threat Indicator Information Sharing

Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.

The MIAC serves as the State's fusion center to share intelligence between the federal government and the State and disseminate analytical products to statewide partners. The MIAC does not maintain the current capability to share cyber threat indicators with partners on a 24/7 basis. While the State currently does not have a 24/7 centralized security operations center that supports the whole of State vision, efforts are underway to build those supports in the future. In the short term, entities are encouraged to join information-sharing networks such as MS-ISAC and EI-ISAC and to leverage federal resource offerings such as the CISA Threat Intelligence Platform (coordinated through Objective 2.2).

Department Agreements

Cyber threat information will be shared through the MIAC as appropriate.

Leverage CISA Services

Leverage cybersecurity services offered by the Department.

The State of Maine is committed to increasing awareness of CISA's services and free tools (such as the Cyber Resource Hub), coupled with those available through MS-ISAC, EI-ISAC, CIS, and other federal providers. Maine's outreach initiative (Objective 2.2) may include several components including but not limited to:

- Targeted email communications to advise local governments about the available services and tools to enhance cybersecurity in their organization
- Organizing state-led webinars which feature partner organizations (such as MS-ISAC, EI-ISAC, CIS, and CISA) to provide local governments with education about the available services and tools
- Coordinating with state and federal agencies to align outreach and engagement initiatives

The State will monitor growth in awareness and implementation of these services and membership in organizations such as MS-ISAC and EI-ISAC, as outlined in Appendix B: Metrics.

Information Technology and Operational Technology Modernization Review

Implement a modernization review process that ensures alignment between information technology and operational technology cybersecurity objectives.

The State of Maine will increase awareness of CISA's Cyber Security Evaluation Tool (CSET) and other federal offerings that provide organizations with a repeatable assessment process to modernize their information technology and operational technology assets. The State will monitor growth in awareness and implementation of these offerings (Objective 2.2). Additionally, the State will encourage State and local entities to replace end of life hardware and software and share project funding opportunities as they become available. In some areas of critical infrastructure, like elections, the State will continue to identify opportunities for state procurement of systems and software for use by local entities.

Cybersecurity Risk and Threat Strategies

Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.

The Planning Committee will operate under its approved charter to support the strategy and implementation of the SLCGP. The Planning Committee contains representation from local governments, state partners, and other organizations which will be continuously engaged throughout the duration of this grant. The SLCGP has provided an opportunity to continue to build relationships between statewide partners that face similar challenges and resource constraints. A full list of Planning Committee members is provided in Appendix C.

Maine is also a member of the International Emergency Management Group (IEMG) which provides for the possibility of mutual assistance in managing an emergency or disaster among participating jurisdictions. Through a Memorandum of Understanding (The Compact), and in support of Resolution 23-5 of Conference of New England Governors and Eastern Canadian Premiers, the IEMG supports the process of planning, mutual cooperation, and emergency-related exercises, testing and other training activities. Maine is represented on the Executive Committees of the MS-ISAC and the EI-ISAC as well as multiple Government Coordinating Councils.

Rural Communities

Ensure adequate access to, and participation in, the services and programs described in this subparagraph by rural communities within the state.

Maine is the most rural state in the nation. With the exception of the City of Portland, all local governments meet the SLCGP definition of a "rural area," with a population of 50,000 or less.[12]

The Planning Committee serves as a voice for local input, and includes representation from state, county, and local government, public education, public health, public safety, emergency communications, election infrastructure, the judicial system, public critical infrastructure, and the Maine National Guard (full list of members is available in Appendix C. The Planning Committee has expert knowledge of Maine's urban, suburban, and rural areas, particularly the cyber unserved and the cyber underserved to ensure adequate representation in the State's cybersecurity strategic planning efforts. The State of Maine's whole-of-state approach to SLCGP implementation benefits rural communities in particular, which may lack the necessary financial and human capital resources necessary to implement cybersecurity programs, and as a result advances equity in this critical area.

[12] SLCGP Fiscal Year 2022 Notice of Funding Opportunity

Distribution to Local Governments

Funding Allocation

The following table details the State of Maine's anticipated SLCGP funding allocations by fiscal year, accompanied by the required amount of matching funds. The State intends to request these matching funds from the Legislature on behalf of the eligible subrecipients, removing the requirement for local entities to provide these matching funds.

Financial Resource Overview				
Federal Grant Fiscal Year	**Funding Allocation**	**Match Requirement**	**Amount of Match**	**Total Amount**
Fiscal Year 2022	$2,666,577.00	10%	$266,693.20	$2,933,625.20
Fiscal Year 2023	$5,439,273.00	20%	$1,087,854.60	$6,527,127.60

Distribution of Funds

Following a third-party assessment (methodology described in Assess Capabilities, the Planning Committee has determined the initial priorities presented in this Plan, which are outlined in Appendix A: Project Summary Worksheet.

The State of Maine intends to provide SLCGP-funded shared services to local governments. This approach leverages State purchasing power to realize cost-savings for cybersecurity technologies, standardization of products in use, and thorough vetting of all vendors, terms, and conditions. Additionally, given the scarcity of SLCGP funding, this statewide approach will benefit its most rural communities, which may lack the capacity to apply for grants independently or provide matching funds. Maine's intent to distribute shared services to local governments is consistent with other states' approaches to implementing the SLCGP.[13]

The State will communicate opportunities to participate in the SLCGP via MEMA's website, social media, and direct messaging services, while also engaging local government associations and organizations, including those representatives on the Planning Committee, to aid in promoting the opportunities. MEMA will also coordinate with state leads for the sixteen critical infrastructure sectors to leverage existing state and local partnerships to promote opportunities to participate in SLCGP. As SLCGP funds are finite, and eligibility is limited to organizations outlined in the NOFO, it may not be possible for all interested organizations to participate in the SLCGP offerings. Continuous refinement of the priorities will be accomplished by leveraging the aggregated information provided by participants of the NCSR, and other risk and vulnerability assessments coordinated by the Planning Committee.

[13] States share services as DHS cyber grants roll out

FUNDING & SERVICES

Risks

The State of Maine faces significant risk across the SLCGP required elements that are beyond the means of this grant, lack free or low-cost offerings at the federal level, and/or exceed the State’s ability to implement them. Some of this risk may be addressed through other initiatives or a continuance of the SLCGP resourced by both the federal and State government. Improving State and local governments’ awareness of the federal cybersecurity resources and services (Objective 2.2) may result in the implementation of additional best practices and address portions of the SLCGP required elements. However, absent dedicated resources, it will be challenging for State and local governments to implement these cybersecurity resources and services and achieve best practices.

ASSESS CAPABILITIES

To inform the Cybersecurity Plan, the Planning Committee distributed a survey to contacts representing local governments and school districts.

The survey questions were designed leveraging the elements highlighted in the SLCGP NOFO and validated by the Planning Committee. In addition, the survey was designed to be intuitive for participants without a technical background to complete it by not mandating a response to every single question, providing a response option for "I'm not sure," and linking to a list of Frequently Asked Questions and live support if needed. The survey collected demographic insights to ensure comprehensive participation from various types of organizations (county, municipality, and school district) and regions (respondents were asked which county/counties they perform services in), but responses remained anonymous to encourage candid feedback and perceived vulnerabilities from being attributed to specific organizations.

The survey was developed using an online form and distributed by email on 3/29/23 to nearly 900 contacts representing county commissioners, municipal officials, school district superintendents, and IT directors. The Survey Response Rate table depicts the 181 organizations representing eight counties, 79 municipalities, and 94 school districts that completed the survey prior to the deadline of 4/21/23. During the response window, all organizations received multiple email reminders and additional messaging to encourage survey participation was coordinated through partner agencies.

Survey Response Rate

	Organizations Surveyed	Organizations Responding	Response Rate
Counties	16	8	50%
Municipalities	483	79	16.4%
School Districts	278	94	33.8%
Total	**777**	**181**	**23.3%**

Survey Results: Demographic Insights

Organizations responding to the survey

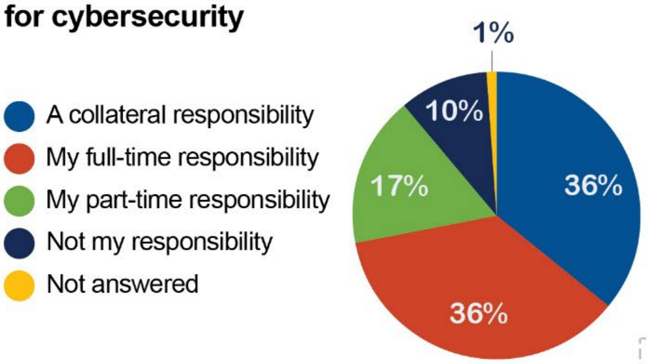
181

8 County

79 Municipality

94 School Districts

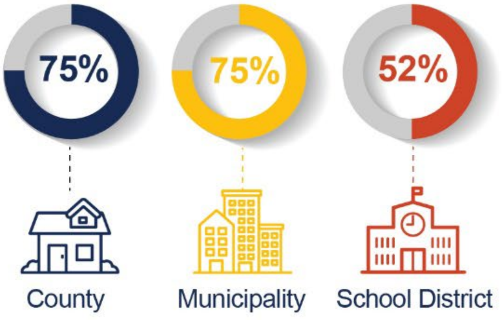
Organization has dedicated position for cybersecurity



Median number of personnel in organizations dedicated to cybersecurity

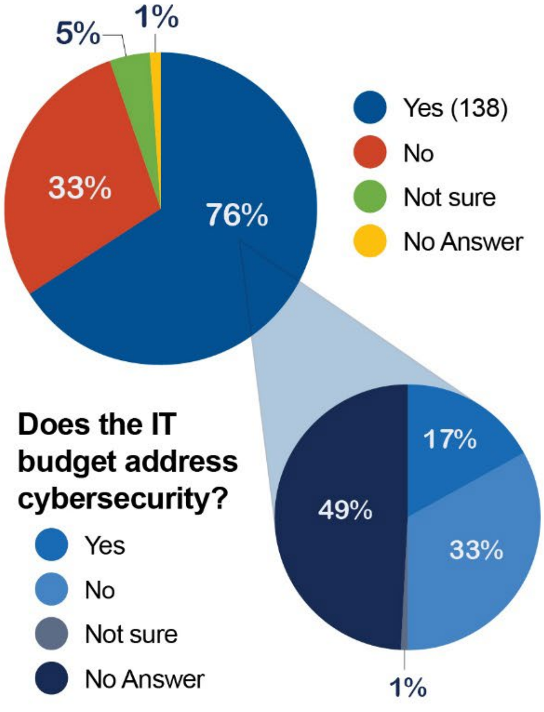
County	Municipality	School District
2	1	2

Percentage of organizations outsourcing cybersecurity responsibilities

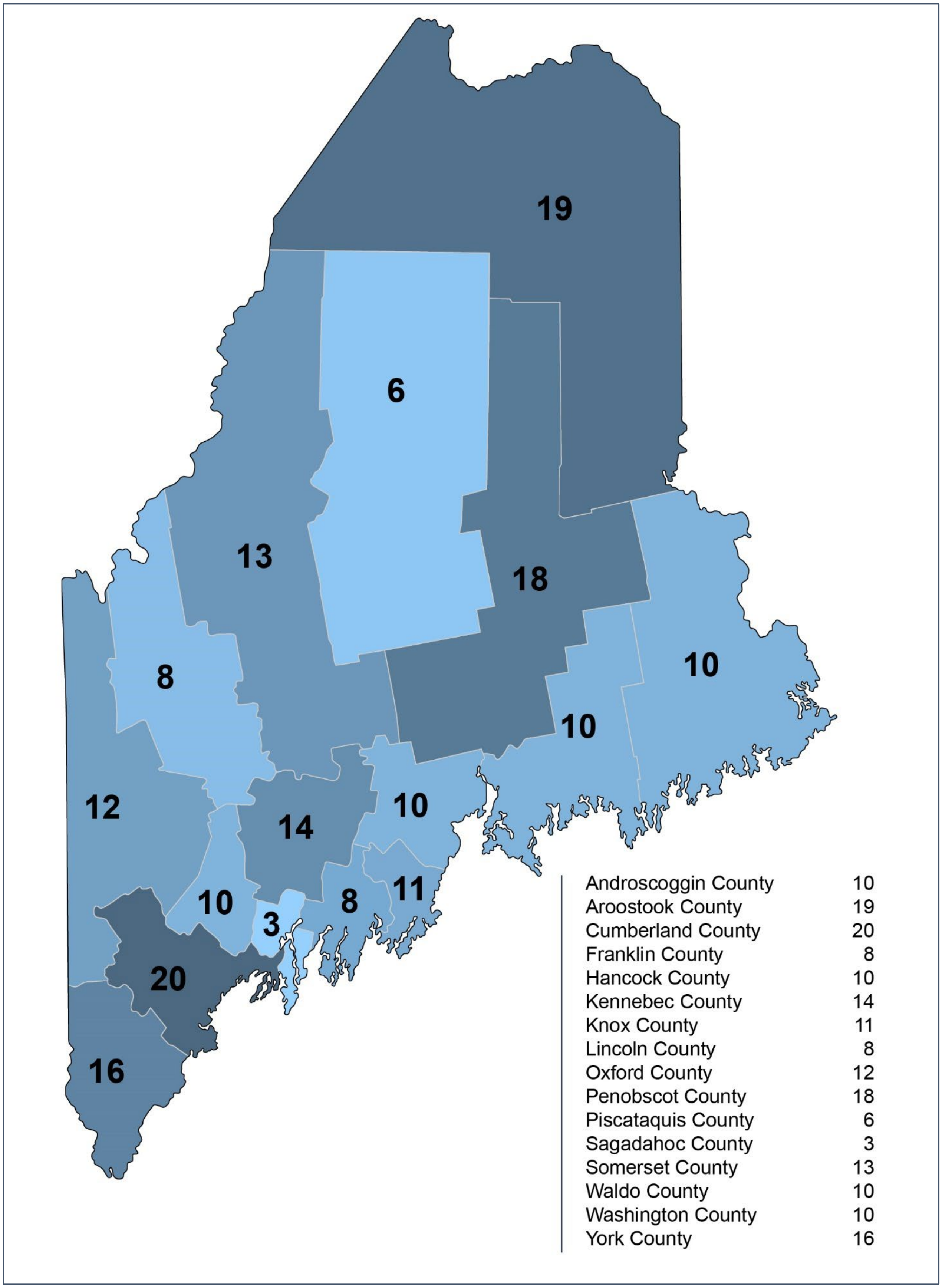


14% responding organizations experienced a cyber incident **within the last year**

Organization has an IT budget



Does the IT budget address cybersecurity?



Androscoggin County	10
Aroostook County	19
Cumberland County	20
Franklin County	8
Hancock County	10
Kennebec County	14
Knox County	11
Lincoln County	8
Oxford County	12
Penobscot County	18
Piscataquis County	6
Sagadahoc County	3
Somerset County	13
Waldo County	10
Washington County	10
York County	16

Figure 1: Count of Survey Responses by County

IMPLEMENTATION PLAN

Resource Overview and Timeline Summary

MaineIT and MEMA will provide the necessary resources to oversee grant administration of the SLCGP in Maine.[14] The anticipated timeline for implementation of the SLCGP is captured in the table below.

Timeline Summary	
Activity	**Date**
Fiscal Year 22	
Planning Committee and CISO/CIO adoption of the Cybersecurity Plan	September 2023
Submission of the Cybersecurity Plan to FEMA and CISA	September 2023
FY22 local consent forms due to MEMA	August – September 2023
CISA approval of the Cybersecurity Plan	October – December 2023 (Tentative)
Submission of projects and revised FY22 Investment Justifications to FEMA	Dates TBD, contingent upon Plan approval
FEMA releases FY22 funds	Dates TBD, contingent upon Plan approval
FY22 Grant agreements executed and projects funded – 45 days after release of funds by FEMA	Dates TBD, contingent upon Plan approval
Period of Performance for FY22 projects concludes	August 31, 2026
Fiscal Year 23	
MEMA submits Maine's FY23 Investment Justifications to FEMA	October 2023
FEMA releases FY23 funds	Dates TBD, contingent upon FEMA approval
FY23 Grant agreements executed and projects funded – 45 days after release of funds by FEMA	Dates TBD, contingent upon FEMA approval
Planning Committee and CISO/CIO submit an updated Cybersecurity Plan to FEMA and CISA for re-approval	September 2025 (within 2 years of initial approval)
Period of Performance for FY23 projects concludes	November 30, 2027

[14] Memorandum of Understanding between OIT and MEMA, dated May 2023

APPENDIX A: PROJECT SUMMARY WORKSHEET

Purpose: The **Project Summary Worksheet** is a list of cybersecurity projects that the entity plans to complete. Following the Cybersecurity Plan approval and follow-on coordination with local governments to refine scope, revised Investment Justifications and Project Worksheets will be submitted with updated project descriptions and budgets. The status column of the Project Summary Worksheet identifies whether projects are near-term (Phase 1) for SLCGP implementation, or long-term (Phase 2).

Project Summary Worksheet

Number	Project Name	Project Description	Related Required Element	Status	Priority	Project Type
1.1	Contact List	Produce a comprehensive set of contacts inclusive of the State and local partners to facilitate future outreach, training, and resource offerings.	11, 15, 16	Phase 1	High	Planning, Organization
2.1	Awareness Training	Provide centrally managed security awareness training for end users in qualifying entities.	8	Phase 1	High	Training
2.2	Cybersecurity Outreach	Increase practitioners' awareness and implementation of federally offered free and fee-based cybersecurity resources.	1, 2, 3, 4, 7, 8, 11, 12, 13	Phase 1	High	Training
3.1	Multifactor Authentication	Provide MFA services to qualifying entities to implement on their networks.	5a	Phase 1	High	Equipment
3.2	.gov migration	Provide a comprehensive service to qualifying entities to evaluate the capability of a .gov domain structure and support turnkey migration.	5g, 6	Phase 1	High	Equipment/Service
3.3	Endpoint Detection and Response	Provide an Endpoint Detection and Response service to qualifying entities to monitor threat activity.	1, 2	Phase 2	Medium	Equipment/Service
4.1	SLCGP Cybersecurity Plan	Maintain and refine the SLCGP Cybersecurity Plan.	14, 15, 16	Phase 1	High	Planning
4.2	Statewide Cybersecurity Planning	Develop and document roles and responsibilities for State and local governments during cybersecurity incident response.	11	Phase 2	Medium	Planning, Organization

APPENDIX B: METRICS

Throughout the duration of the SLCGP, the Planning Committee will measure progress against the goals and objectives in this Plan, which are also representative of the objectives and key elements included in the NOFO. Some of the projects and initiatives created may deliver near-term outcomes and have very granular metrics. Other initiatives included in the Plan are enduring and will evolve over time.

In addition to metrics that measure progress in reducing cyber risk in State and local government organizations, the Planning Committee and the SAA may also develop and maintain administrative, financial, and other related grant management metrics throughout the duration of the SLCGP.

Cybersecurity Program Metrics			
Program Objectives	**Program Sub-Objectives**	**Associated Metrics**	**Metric Description (Details, Source, Frequency)**
1.1 Produce a comprehensive set of contacts inclusive of the State and local partners in Maine to facilitate future outreach, training, and resource offerings.	1.1.1 Create an opt-in mechanism for organizations to receive SLCGP communications from the SAA.	• Number of organizations opting into SAA's SLCGP communications	MEMA (SAA) will produce a quarterly update on this metric
2.1. Provide centrally managed security awareness training for end users in local governments.	1.1.2. Raise awareness of the opt-in mechanism, through an awareness campaign.	• Number of organizations served by training • Increase in individuals' cybersecurity awareness measured by pre- or post-course assessments	The organization providing this training will produce a quarterly update on this metric in coordination with the MaineIT Security Governance and Training Officer and the SoS Director of Cybersecurity and Infrastructure Security
2.2. Increase practitioners' awareness and implementation of federally offered free and fee-based cybersecurity resources.	3.2.1. Conduct procurement of a vendor to implement training.	• Number of organizations contacted through outreach engagements • Number of organizations with MS-ISAC and EI-ISAC memberships • Number of organizations completing the NCSR	MEMA, in coordination with MaineIT and SoS will produce a quarterly update on this metric
3.1. Provide MFA services to qualifying entities to implement on their networks.	3.2.1. Conduct procurement of a vendor to implement MFA. 3.2.2. Onboard vendor. 3.3.2. Implement MFA.	• Number of organizations served	The organization providing this service will produce a quarterly update on this metric

Cybersecurity Program Metrics

Program Objectives	Program Sub-Objectives	Associated Metrics	Metric Description (Details, Source, Frequency)
3.2. Provide a comprehensive service to qualifying entities to evaluate the capability of a .gov domain structure and support turnkey migration.	3.2.1. Conduct procurement of a vendor to manage .gov migration services. 3.2.2. Onboard vendor. 3.3.2. Conduct .gov assessment and migration for qualifying entities.	• Number of local governments on the .gov domain structure	The organization providing this service will produce a quarterly update on this metric, detailing the number of .gov assessments and migrations completed
3.3. Provide an Endpoint Detection and Response (EDR) service to qualifying entities to monitor threat activity.	3.2.1. Conduct procurement of a vendor to manage EDR. 3.2.2. Onboard vendor. 3.3.2. Implement EDR.	• Number of organizations served • Number of threats identified and mitigated	The organization providing this service will produce a quarterly update on these metrics, detailing the EDR implementation and mitigated threats
4.1. Maintain and refine the SLCGP Cybersecurity Plan.	4.1.1. Refine and update the SLCGP Cybersecurity Plan.	• Future Plan approval from CISA	Email from CISA confirming approval of the Plan
4.2. Develop and document roles and responsibilities for State and local governments during cybersecurity incident response.	4.2.1. Develop and/or update state-wide plans which document roles and responsibilities. 4.2.2. Develop an incident response plan template for organizations to use to document roles and responsibilities, and guide response efforts.	• Number of organizations leveraging the incident response plan template	MEMA (SAA) will post the resource to its website

APPENDIX C: PLANNING COMMITTEE MEMBERS

Planning Committee Members		
Name	Title	Agency
Peter Rogers	Director	Maine Emergency Management Agency
Nicholas Marquis	Acting Chief Information Officer	Maine Office of Information Technology
Nathan Willigar	Chief Information Security Officer	Maine Office of Information Technology
Brian McDonald	Director, IT & Administration	Maine Municipal Association
Mike Dery	Information Technology Director	City of South Portland
John Forker	Chief Information Security Officer	University of Maine System
Beth Lambert	Director, Teaching and Learning	Maine Department of Education
Dave Simsarian	Director, Business Technology Solutions	Maine Department of Health and Human Services
Darren Woods	Chair/Director	Maine Emergency Management County Directors Council/Aroostook County Emergency Management Agency
Kathy Montejo	City Clerk & Registrar of Voters	City of Lewiston
Mark Toulouse	Former Division Chief, Finance & Administrative Services	Office of Attorney General
Shenna Bellows	Secretary of State	Department of the Secretary of State
Mathew Casavant	Sergeant	Department of Public Safety / Maine Information and Analysis Center
Steve Mallory	Director of Operations and Response	Maine Emergency Management Agency
Harry Lanphear	Administrative Director	Maine Public Utilities Commission
Brian Tarbuck	General Manager	Greater Augusta Utility District
Daisy Mueller	Former Critical Infrastructure Protection Officer	Maine Emergency Management Agency
Michael Steinbuchel	Colonel	Maine National Guard
Heather Perreault	Deputy Commissioner of Finance	Maine Department of Administrative and Financial Services
Core Team and Staff Members		
Charles Rote	Deputy Chief Information Security Officer	Maine Office of Information Technology
Natalie Haynes	Cybersecurity and Compliance Legal Analyst	Maine Office of Information Technology
James Chasse	Maine Learning Technology Initiative Technology Infrastructure Specialist	Department of Education
Andy Ouellette	Information Security Legal Analyst	Maine Office of Information Technology
Joe Legee	Deputy Director	Maine Emergency Management Agency
Emily Cook	Director of Communications	Department of the Secretary of State
Stephanie Buzzell	Homeland Security Grant Manager	Maine Emergency Management Agency
Amy Carole	Public Outreach Specialist	Maine Emergency Management Agency
Vanessa Corson	Public Information Officer	Maine Emergency Management Agency

APPENDIX D: ORGANIZATION ROLES AND RESPONSIBILITIES

State Agencies

Maine Office of Information Technology

MaineIT is the primary agency responsible to coordinate the State's cybersecurity efforts. Under the direction of the Chief Information Officer (CIO), MaineIT is responsible for:

- Providing IT services to 13,000+ Executive Branch employees, 14 cabinet-level departments, and smaller Executive Branch agencies.
- Providing network support for the Judicial Branch, Secretary of State, and Attorney General.
- Supporting citizens by maintaining the maine.gov web portal.
- Supporting public safety by maintaining the state radio communications network.

Maine Emergency Management Agency

MEMA performs essential coordination and communication roles during disasters, including cybersecurity incidents. MEMA leverages an all-hazards approach to the four phases of emergency management: preparedness, response, recovery, and mitigation. MEMA is also responsible for:

- Serving as the SAA for federal preparedness grants issued by the DHS, including the SLCGP.
- Providing guidance and assistance to municipal emergency managers and the 16 county emergency management agencies as outlined in State statute.
- Working proactively with stakeholders to increase resiliency through planning, training, exercise, and outreach.
- Identifying Critical Infrastructure and Key Resources (CIKR) within the state.
- Primary coordination of homeland security activities.
- Activating and managing the State Emergency Operations Center (SEOC).
- Assisting, as appropriate, in the restoration of communications and CIKR during disruptions.
- Requesting a State of Emergency Proclamation through the Governor's Office and coordinating any federal support for response and recovery.

Department of the Secretary of State

The Secretary of State oversees the Maine State Archives, the Bureau of Corporations, Elections and Commissions, and the Bureau of Motor Vehicles. As a department providing direct services to the citizens of Maine, the Department is a leader in efforts to enhance access to information and adoption of e-Government services. The Secretary of State's Office is responsible for:

- Promoting public trust by safeguarding vital government records.
- Authority to define and manage digital signatures for secure government functions.
- Safeguarding free, safe and secure elections including responsibility and helpdesk support for all election-related technology and election security
- Coordinating training of municipal clerks, registrars and agents for implementation of state and federal elections
- Providing audits and training of municipalities with regards to the joint provision of vehicle registration services and elections.
- Coordinating threat reports from local election officials
- Managing identity and licensing for Maine people
- Leveraging technology to improve efficiency and customer service.

Maine Information and Analysis Center

Under the command of the Maine State Police, the MIAC serves as Maine's fusion center. Through partnership with federal, state, county, local and tribal law enforcement agencies and the private sector, the MIAC provides real-time information to partners through the nationwide fusion center network. The MIAC is responsible for:

- Collecting, analyzing, and sharing intelligence (including cybersecurity threats) to enhance statewide situational awareness.
- Disseminating cybersecurity alerts using the Homeland Security Information Network (HSIN).
- Coordinating threat intelligence and information sharing with federal partners, including DHS, the Federal Bureau of Investigations (FBI), CISA, and the MS-ISAC.

Maine National Guard

The Adjutant General for the MENG serves as the Department of Veterans and Emergency Management Commissioner (overseeing several agencies, including MEMA) and as the Homeland Security Advisor for the State. The MENG fulfills federal responsibilities for cybersecurity in the military and a homeland role in Maine upon the governor's activation. If activated by the governor in the event of a cybersecurity incident, the MENG may provide incident coordination, technical support, and/or liaison support with U.S. Cyber Command or the National Security Agency. During all-hazard disasters and emergencies, the MENG participates in the SEOC activations as requested.

Maine Department of Education

The DOE supports school districts in their cybersecurity efforts through the Maine School Safety Center (MSSC) and the Maine Learning Technology Initiative (MLTI). The MSSC provides training, planning support and technical assistance to school districts in all-hazards planning and emergency management. The MLTI delivers a state-level holistic technology program available to schools and includes equipment and software acquisition, learning resources, technology support, and systematic monitoring and support.

Advisory Groups

Cybersecurity Advisory Council

Executive Order 25 establishes the Cybersecurity Advisory Council to strengthen the security and resiliency of the State's information technology infrastructure to protect against cybersecurity risks and ensure an effective cybersecurity communication chain to the Governor's Office.[15] The Council participates in activities to better understand the State's security threats and incidents and supports the development of statewide partnerships, policies and procedures, and recommendations to enhance cybersecurity.

SLCGP Planning Committee

In accordance with the requirements of the grant and in coordination with the SAA, the Cybersecurity Advisory Council has formed the SLCGP Planning Committee ("Planning Committee"). The Planning Committee ensured a whole-of-state approach was taken in developing this Plan to align with the unique needs and risk profiles of critical sectors throughout the state and provide cyber stakeholders with support and resources to defend against evolving cyber threats. The "Maine Cybersecurity Advisory Council SLCGP Planning Committee Charter" establishes the purpose, membership, and responsibilities of its members. A full list of members is provided in Appendix D.

Homeland Security Advisory Council

Established in Title 37-B of the Maine State Statute, the Homeland Security Advisory Council is comprised of representatives from several State agencies, advises the governor on the coordination of homeland security activities of state agencies, and recommends the most effective uses of Homeland Security Grant Program (HSGP) funds[16].

Individual Organizations

Each State and local government organization is responsible and primarily accountable to maintain its own cybersecurity program. The resources provided to individual organizations through the SLCGP do not fulfill their cybersecurity

[15] An Order Establishing the State of Maine Cybersecurity Advisory Council

[16] Maine Revised Statute, Title 37-B: Defense, Veterans and Emergency Management

responsibilities or supersede existing initiatives; rather, they are intended to augment individual organizations' resources to reduce cybersecurity risks.

Individual organizations which participate in the SLCGP will be encouraged to:

- Become members of the MS-ISAC and/or the EI-ISAC (as applicable), which are no-cost memberships.
- Sign up for CISA's Cyber Hygiene Vulnerability scanning program, a free service. This is a requirement from CISA for any grant subrecipients which receive services or funds through the SLCGP.
- Complete the NCSR annually.
- Participate in State-led cybersecurity assessments in future years as necessary.
- Gain familiarity with the many cybersecurity resources and services provided by CISA, MS-ISAC, EI-SAC, and the CIS.

APPENDIX E: ACRONYMS, GLOSSARY, AND REFERENCES

Acronyms

CIKR	Critical Infrastructure and Key Resources
CIO	Chief Information Officer
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
CSAT	Controls Self-Assessment Tool
CSET	Cyber Security Evaluation Tool
DHS	Department of Homeland Security
DOE	Department of Education
EDR	Endpoint Detection and Response
EI-ISAC	Elections Infrastructure Information Sharing and Analysis Center
FBI	Federal Bureau of Investigations
FEMA	Federal Emergency Management Agency
HSIN	Homeland Security Information Network
HTTPS	Hypertext Transfer Protocol Secure
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization
IT	Information Technology
MaineIT	Maine Office of Information Technology
MCC	Maine Cybersecurity Center
MEMA	Maine Emergency Management Agency
MENG	Maine National Guard
MFA	Multifactor Authentication
MIAC	Maine Information and Analysis Center
MICC	Maine Interoperable Communications Committee
MLTI	Maine Learning Technology Initiative
MS-ISAC	Multi-State Information Sharing and Analysis Center
MSSC	Maine School Safety Center
NCSR	Nationwide Cybersecurity Review
NDPC	National Domestic Preparedness Consortium
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NOFO	Notice of Funding Opportunity
SAA	State Administrative Agency
SCIP	State Interoperable Communications Plan

SEOC	State Emergency Operations Center
SoS	Secretary of State
SLCGP	State and Local Cybersecurity Grant Program
SPR	Stakeholder Preparedness Review
THIRA	Threat and Hazard Identification and Risk Assessment
UMS	University of Maine System

Glossary

Asset: An item of value to stakeholders. An asset may be tangible (e.g., a physical item such as hardware, firmware, computing platform, network device, or another technology component) or intangible (e.g., humans, data, information, software, capability, function, service, trademark, copyright, patent, intellectual property, image, or reputation).

Best Practice: A procedure that has been shown by research and experience to produce optimal results and that is established or proposed as a standard suitable for widespread adoption.

Capability: A combination of mutually reinforcing controls implemented by technical means, physical means, and procedural means. Such controls are typically selected to achieve a common information security or privacy purpose.

Cloud computing: A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Critical infrastructure: Systems and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. The federally designated critical infrastructure sectors are as follows: Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Facilities, Healthcare and Public Health, Information Technology, Nuclear, Transportation Systems, and Water and Wastewater Systems.[17]

Cybersecurity: Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Cybersecurity incident: An occurrence that (i) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (ii) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

Cybersecurity risk: An effect of uncertainty on or within information and technology. Cybersecurity risks relate to the loss of confidentiality, integrity, or availability of information, data, or information (or control) systems and reflect the potential adverse impacts to organizational operations (i.e., mission, functions, image, or reputation) and assets, individuals, other organizations, and the Nation.

Cyber threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via

[17] CISA Critical Infrastructure Sectors

unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat source to successfully exploit a particular information system vulnerability.

Data: A representation of information as stored or transmitted.

Endpoint detection and response: An endpoint (e.g., mobile phone, laptop, Internet-of-Things device) security solution that continuously monitors end-user devices to detect and respond to cyber threats like ransomware and malware.

Fusion center: A collaborative effort of two or more agencies that provide resources, expertise and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity.

Hardware: The material physical components of an information system.

Home rule: A principle of governance that implies that each level of government has a separate realm of authority. Therefore, state power should not infringe on the authority of local government in certain areas as dictated in the state constitution.

Information system: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Multifactor authentication: An authentication system that requires more than one distinct authentication factor for successful authentication. Multifactor authentication can be performed using a multifactor authenticator or by a combination of authenticators that provide different factors. The three authentication factors are something you know, something you have, and something you are.

Network: Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

Resilience: The ability to maintain the required capability in the face of adversity.

Resource: Asset used or consumed during the execution of a process.

Risk: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

Organization: A government state agency or, as appropriate, any of its operational elements.

Security: A condition that results from the establishment and maintenance of protective measures that enable an organization to perform its mission or critical functions despite risks posed by threats to its use of systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the organization’s risk management approach.

Software: Computer programs and associated data that may be dynamically written or modified during execution.

Threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Turnkey migration: A process that allows for the easy backup and migration of application and server configurations.

User: Individual or (system) process authorized to access an information system.

Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Reference List

CISA SLCGP Cybersecurity Plan Template: https://www.cisa.gov/state-and-local-cybersecurity-grant-program

CISA Cross-Sector Cybersecurity Performance Goals: https://www.cisa.gov/cross-sector-cybersecurity-performance-goals

DHS SLCGP NOFO (FY 2022): https://www.fema.gov/fact-sheet/department-homeland-security-notice-funding-opportunity-fiscal-year-2022-state-and-local

FEMA Preparedness Grants Manual (2023): https://www.fema.gov/sites/default/files/documents/fema_gpd-fy-23-preparedness-grants-manual.pdf

FEMA State and Local Cybersecurity Grant Program: https://www.fema.gov/grants/preparedness/state-local-cybersecurity-grant-program

Maine Cybersecurity Center: https://www.uma.edu/academics/programs/cybersecurity/cybersecurity-center/

Maine Cyber Range: https://www.uma.edu/academics/programs/cybersecurity/maine-cyber-range/

Maine Economic Development Strategy (2020-2029): https://www.maine.gov/decd/sites/maine.gov.decd/files/inline-files/DECD_120919_sm.pdf

Maine Learning Technology Initiative: http://www.maine.gov/doe/Learning/LTT/MLTI/2.0

MaineIT Business Continuity and Disaster Recovery Policy: https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/BusinessContinuityDisasterRecoveryPolicy.pdf

Maine Revised Statute, Title 37-B: Defense, Veterans and Emergency Management: https://legislature.maine.gov/statutes/37-B/title37-Bsec708.html

Memorandum of Understanding between OIT and MEMA (May 2023): *no link available*

Order Establishing the State of Maine Cybersecurity Advisory Council: https://www.maine.gov/future/sites/maine.gov.governor.mills/files/inline-files/EO 82 25.pdf

State of Maine Communication Interoperability Plan: https://www.maine.gov/mema/ema-community/communications/document-library

State of Maine Homeland Security Strategy (2023-2025): *no link available*

State of Maine Information Security Strategic Plan (2021-2026): *no link available*

Title 6 U.S.C. § 101(13): https://www.govinfo.gov/link/uscode/6/101

APPENDIX F: PLAN SIGNATURES

Original document is signed

Nicholas Marquis – Co-Chair
Acting State Chief Information Officer
Maine Office of Information Technology
State of Maine

Nathan Willigar – Co-Chair
State Chief Information Security Officer
Maine Office of Information Technology
State of Maine

Peter Rogers
Director
Maine Emergency Management Agency

John Forker
Chief Information Security Officer
University of Maine System

Beth Lambert
Director, Teaching and Learning
Maine Department of Education

Shenna Bellows
Maine Secretary of State

Sgt. Mathew Casavant
Maine Department of Public Safety
State Police

Colonel Michael Steinbuchel
Maine National Guard

Darren Woods
Director
Aroostook County Emergency Management Agency

Steven Mallory
Statewide Interoperability Coordinator
Maine Emergency Management Agency

Harry Lanphear
Administrative Director
Maine Public Utilities Commission

Brian Tarbuck
General Manager
Greater Augusta Utility District

Heather Perreault
Deputy Commissioner of Finance
Maine Department of Administrative and Financial Services

Brian McDonald
Director, IT and Administration
Maine Municipal Association

David Simsarian
Director, Business Technology Solutions
Maine Department of Health and Human Services

Mike Dery
IT Director
City of South Portland

Kathy Montejo
City Clerk and Registrar of Voters
City of Lewiston

APPENDIX G: RECORD OF CHANGES

Date	Approved By	Summary of Changes