



STATE OF NEW HAMPSHIRE STATE AND LOCAL



CYBERSECURITY GRANT PROGRAM (SLCGP) PLAN

Approved by State of New Hampshire SLCGP
Planning Committee
On 9 OCTOBER 2024

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LETTER FROM THE NEW HAMPSHIRE SLCGP PLANNING COMMITTEE 1

INTRODUCTION 2

 Vision and Mission 3

 SLGCP Cybersecurity Program Goals and Objectives..... 3

SLGCP CYBERSECURITY PLAN ELEMENTS 4

 Manage, Monitor, and Track 4

 Monitor, Audit, and Track..... 4

 Enhance Preparedness..... 4

 Assessment and Mitigation 4

 Best Practices and Methodologies..... 5

 Safe Online Services 6

 Continuity of Operations 6

 Cyber Threat Indicator Information Sharing..... 7

 Leverage CISA Services..... 7

 Information Technology and Operational Technology Modernization Review 7

 Cybersecurity Risk and Threat Strategies 8

 Rural Communities..... 8

FUNDING & SERVICES 8

 Distribution to Local Governments..... 8

ASSESS CAPABILITIES 9

IMPLEMENTATION PLAN..... 9

 Organization, Roles, and Responsibilities..... 9

 Resource Overview and Timeline Summary 10

METRICS 11

APPENDIX A: CYBERSECURITY PLAN CAPABILITIES ASSESSMENT..... 12

APPENDIX B: PROJECT SUMMARY WORKSHEET..... 16

APPENDIX C: ENTITY METRICS..... 17

LETTER FROM THE NEW HAMPSHIRE SLCGP PLANNING COMMITTEE

9 October 2024

Greetings,

The State and Local Cybersecurity Grant Program (SLCGP) Planning committee for New Hampshire is pleased to present the FFY 2024 (Years 3 and 4 of the program) New Hampshire SLCGP Cybersecurity Plan. This Plan represents the State of New Hampshire's continued commitment to improving cybersecurity through the SLCGP. The purpose of this plan is to meet the requirement of the current Federal Emergency Management Agency (FEMA), U.S. Department of Homeland Security (DHS) and Cyber and Infrastructure Security Agency (CISA) guidelines for the State and Local Cybersecurity Grant Program (SLCGP).

Representatives from cities, towns, and counties, rural, suburban, and urban; higher education and K-12 Public Education; public health and public safety are represented on the New Hampshire SLCGP Planning Committee and collaborated to approve the SLCGP Cybersecurity Plan with goals and objectives that meet program priorities and objectives found in the Notice of Funding Opportunity (NOFO). These goals and objectives focus on leveraging economies of scale to implement programs that directly benefit the represented entities on the SLCGP Planning Committee. The entire structure of the plan is specifically formatted to meet the required plan elements defined in the NOFO.



Denis Goulet
Chief Information Officer
Chairman, NH SLCGP Planning Committee

INTRODUCTION

The content of the plan follows the Cybersecurity Plan Template provided by the Notice of Funding Opportunity (NOFO) for the State and Local Cybersecurity Grant Program (SLCGP).

The Cybersecurity Plan is a strategic planning document for the grant's period of performance that contains the following components:

- **Vision and Mission:** Articulates the vision and mission of the SLCGP Planning Committee for improving cybersecurity resilience over the next one-to-three-years.
- **Organization, and Roles and Responsibilities:** Describes the current roles and responsibilities, and any governance mechanisms for cybersecurity within as well as successes, challenges, and priorities for improvement. This also includes a strategy for the cybersecurity program and the organization structure that identifies how the cybersecurity program is supported. In addition, this section includes governance that identifies authorities and requirements of the State of New Hampshire's cybersecurity program. The Cybersecurity Plan is a guiding document required by the SLCGP and does not create any authority or direction over any of the State of New Hampshire's local systems or agencies, or any branch of the New Hampshire State Government.
- **How feedback and input from local governments and associations was incorporated.** Describes how inputs from local governments as used to reduce overall cybersecurity risk across the eligible entity. This is especially important to develop a holistic cybersecurity plan.
- **Cybersecurity Plan Elements:** Outlines technology and operations needed to maintain and enhance resilience across the cybersecurity landscape.
- **Funding:** Describes funding sources and allocations to build cybersecurity capabilities within State of New Hampshire along with methods and strategies for funding sustainment and enhancement to meet long-term goals.
- **Implementation Plan:** Describes the State of New Hampshire's plan to implement, maintain, and update the Cybersecurity Plan to enable continued evolution of and progress toward the identified goals. The implementation plan must include the resources and timeline where practicable.
- **Metrics:** Describes how State of New Hampshire will measure the outputs and outcomes of the program across the entity.

This plan aligns with and/or references the following:

- [State Of New Hampshire – Department of Information Technology – Statewide Strategic Information Technology Plan – 2021-2025](#)
- [New Hampshire Information and Cybersecurity Policies and Procedures](#)
- [NH SLCGP Information](#)

Vision and Mission

This section describes the State of New Hampshire SLCGP Planning Committee’s vision and mission for improving cybersecurity through the SLCGP:

Vision:

Work as a “Whole of State Team” to implement projects that improve Cyber resilience and mitigate risk across the State of New Hampshire.

Mission:

Ensure SLCGP funding is used efficiently to improve cyber resilience, secure critical infrastructure and regulated data, and safeguard the privacy of New Hampshire residents, and those that do business with the state, municipalities, schools, and other local government entities.

SLGCP Cybersecurity Program Goals and Objectives

State of New Hampshire SLCGP Planning Committee goals and objectives include the following:

NH SLCGP Cybersecurity Program	
Program Goal	Program Objectives
1. Improve State and Local Entities’ capacity to implement best practices and methodologies to mitigate cybersecurity risk.	1.1 Improve and refine SLGCP Cybersecurity Plan and perform Program Management Functions.
	1.2 Implement Endpoint and Server Managed Detection and Response for High Value Targets (HVT) in 100% of NH School Administrative Units (Public K12s) for an initial period of 3 years.
	1.3 Implement Cybersecurity improvements for Community Drinking Water and Wastewater facilities (Public-Sector Owned and/or operated).

SLCGP CYBERSECURITY PLAN ELEMENTS

Manage, Monitor, and Track

At the State and Local Levels, entities should establish procedures that effectively control and restrict access to information assets to authorized users based on defined business and legal requirements (essentially, access will be limited to a “need-to-use” and/or “need-to-know” basis). Mechanisms will be implemented that provide for the control, administration, and tracking of access to, and the use of, information assets, as well as the protection of such assets from unauthorized or unapproved activity and/or destruction. The Executive Branch’s specific Policies to implement this Strategic Approach are documented in the [New Hampshire Information and Cybersecurity Policies and Procedures](#) and are also available for use by the other Branches of State Government and Local Government entities.

Monitor, Audit, and Track

Asset owners, asset custodians, and information security and privacy officers at the State and Local levels should:

- (a) Ensure the information assets under their purview are assessed for security and privacy risks and configured such that event logging is enabled to ensure an adequate level of situational awareness regarding potential threats to the confidentiality, integrity, availability, and privacy of agency information and information systems are identified and managed; and
- (b) Review and retain event logs in compliance with all applicable Local, State and Federal laws, regulations, executive orders, circulars, directives, internal agency and State of New Hampshire policies, and contractual requirements.

The Executive Branch’s specific Policies to implement this Strategic Approach are documented in the [New Hampshire Information and Cybersecurity Policies and Procedures](#) and are also available for use by the other Branches of State Government and Local Government entities.

Enhance Preparedness

State and Local Government Entities should implement continuous risk management processes that account for the identification, assessment, treatment, and monitoring of risks that can adversely impact their operations, information systems, and information. These processes will inform the exercise and execution of Incident Response Plans, Continuity of Operations Plans and the State Emergency Operation Plan. Lessons Learned from these exercises will be incorporated into future planning, inform organizational decisions, and demonstrate additional equipment and training needs. For members of the New Hampshire Public Risk Management Exchange (PRIMEX) assistance with this planning is readily available by request. The Executive Branch’s specific Policies to implement this Strategic Approach are documented in the [New Hampshire Information and Cybersecurity Policies and Procedures](#) and are also available for use by the other Branches of State Government and Local Government entities.

Assessment and Mitigation

All major systems and applications, and general support systems operated by or on behalf of State and Local Government entities should undergo security assessments to ensure adequate security and privacy controls

are implemented and risks are managed to acceptable levels throughout their lifecycles. Risk management processes including identifying, assessing, and addressing security and privacy risks at the inception of the project to build a system until the decommissioning of a system. These actions enable State and Local Government entities to maintain security and privacy of a system throughout its lifecycle. To aid in satisfying the ongoing assessment requirements, assessment results from the following sources can be used: continuous monitoring, audits and authorizations, and other system development life cycle activities. The Executive Branch's specific Policies to implement this Strategic Approach are documented in the [New Hampshire Information and Cybersecurity Policies and Procedures](#) and are available for use by the other Branches of State Government and Local Government entities.

Best Practices and Methodologies

The State of New Hampshire Executive Branch operates on the principle of "Baseline and Baseline-Plus" for security controls and Best Practices. The specifics of the Baseline and Baseline-Plus are summarized below.

BASELINE:

The Baseline is applied to all State-owned, leased, licensed, or managed information systems, system components, and system services and is derived from the controls defined by NIST Special Publication 800-171 R2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.

BASELINE PLUS:

Entities across the State Government have various legal, regulatory, and contractual compliance requirements based on their business services and operations, and the information they collect, store, process, and transmit. Some commonly applicable statutory and regulatory requirements include IRS Publication 1075, Safeguards for Protecting Federal Tax Returns and Return Information, Health Insurance Portability and Accountability Act (HIPAA), Minimum Acceptable Risk Standards for Exchanges, version 2.0 (MARS-E), Family Education Rights Privacy Act (FERPA), Payment Card Industry – Data Security Standards (PCI-DSS), Criminal Justice Information Services (CJIS), and others. To satisfy the control objectives for the above statutory and regulatory requirements, and to provide a uniform baseline across State entities that are subject to these levels of compliance, all State-owned, leased, licensed, or managed information systems, system components, and system services subject to the above are required to, at a minimum, implement Moderate level controls as defined by NIST Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations.

At the local level, many of the controls and best practices which are implemented, especially among the more than 500 Local entities who are members of the New Hampshire Public Risk Management Exchange (PRIMEX,) are based on the Center for Internet Security Critical Security Controls.

In either case, whether based on NIST Special Publications, or CIS Critical Security Controls, the following best practices are included and projects to implement will be considered over the life of the SLCGP: (a) implementation of multi-factor authentication, (b) implementation of enhanced logging, (c) encryption for data at rest and in transit, (d) eliminating use of unsupported/end of life software and hardware that are accessible from the Internet, (e) prohibition of use of known/fixed/default passwords and credentials, and (f) enabling the ability to reconstitute systems (backups).

NIST Principles

A detailed description of the application of NIST Principles and the CIS Critical Security Controls is provided in the preceding paragraph.

Supply Chain Risk Management

The State of New Hampshire requires Third Parties that do business with the State of New Hampshire Executive Branch to implement security and privacy controls derived from NIST 800-171R2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, and/or NIST 800-53R5, Security and Privacy Controls for Information Systems and Organizations, that align with the controls the State requires of itself and as documented in the [New Hampshire Information and Cybersecurity Policies and Procedures](#). To document compliance and inform risk-based decisions prior to procurement/contract actions, New Hampshire requires a thorough examination of third party risk as documented in this SOP: [Risk Management for Commercial Software and Cloud Hosting Environments](#). Additionally, the State prohibits the use of certain technologies as defined in the [NH Prohibited Technologies List](#).

Tools and Tactics

Tools and Tactics are addressed in the Cyber Threat Indicator Sharing section found later in this plan.

Safe Online Services

For Organizations eligible to receive funds under the SLCGP who have not previously migrated to the .gov domain, one of the fully funded projects is a turn-key solution, branded as .Gov in a Box to assist with this migration. Details on this program can be found here: [.GOV in a Box and Drinking Water Cybersecurity in a Box](#)

Continuity of Operations

State and Local Government entities should develop, implement, test, and maintain contingency plans to ensure continuity of operations for all information systems that deliver or support essential or critical functions on behalf of the State of New Hampshire or their respective Local Government Entity. Contingency planning is an important aspect of risk management. Ensuring availability for critical and essential systems and components allows agencies to meet its mandates that are dictated by statute, executive order, policy, or contract, and to ensure delivery of vital government services. For members of the New Hampshire Public Risk Management Exchange (PRIMEX) assistance with this planning is readily available by request. The Executive Branch's specific Policies to implement this Strategic Approach are documented in the [New Hampshire Information and Cybersecurity Policies and Procedures](#) and are also available for use by the other Branches of State Government and Local Government entities.

Workforce

Workforce recruitment and retention is a well-documented problem across the Nation in both the Public and Private Sector. State and Local Government entities are tied to archaic personnel policies and a unionized

workforce. However, once State and Local Government Entities recruit and hire employees, they should ensure that all users are made aware of the security and privacy risks associated with their roles and that users understand their responsibilities, as well as applicable laws, regulations, executive orders, circulars, policies, standards, and procedures related to the security and privacy of State information and systems. The Municipal Cyber Defense Program (MCDP) is a Public Private partnership between NH PRIMEX, the Atom Group, LLC, The Overwatch Foundation, and the State of New Hampshire that provides significant training and education to local government entities on these topics. More information on the MCDP can be found here: [NH MCDP](#)

Cyber Threat Indicator Information Sharing

The New Hampshire Information and Analysis Center (NHIAC) is a cooperative effort under the New Hampshire Department of Safety between the New Hampshire State Police and New Hampshire Homeland Security and Emergency Management. The New Hampshire Cyber Integration Center (NHIC) is also a partner with the NHIAC. The NHIAC and NHIC, in coordination with the Local and Regional CISA representative monitor information from a variety of open and classified sources, analyzes that information, and distribute information across State and Local entities. For Local members of the New Hampshire Public Risk Management Exchange (PRIMEX) threat data is available through the PRIMEX Cybersecurity Portal and advisories sent to the membership. Recipients of the SLCGP will also share information through their respective MS-ISAC indicator sharing efforts.

Department Agreements

Currently, there is no intent by the State of New Hampshire to expand any information sharing agreements.

Leverage CISA Services

Many Local Government entities take advantage of cybersecurity assessment services offered by CISA. This should continue and expand in the future. The Local/Regional CISA representative is very collaborative and accessible to State and Local Government entities and routinely coordinates with the membership of the New Hampshire Public Risk Management Exchange, New Hampshire Municipal Association, and other entities across the State. Additionally, the SLCGP recipients should enroll in Vulnerability Scanning and Web-Application Scanning as appropriate.

Information Technology and Operational Technology Modernization Review

The State of New Hampshire's strategic approach to ensure alignment between information technology and operational technology cybersecurity objectives is that although much of the funding comes from different sources to protect the totality of these systems, a distinction is not made between controls applied to information technology and operational technology as the convergence of the (formerly) two technologies is almost complete. SLCGP participants may also replace end of life/outdated equipment found at this convergence, e.g., Windows XP and/or Windows 7 Machines if equipment purchases are approved by the SLCGP Planning Committee at some point in the future. Current efforts by New Hampshire to address these critical vulnerabilities can be found here: [.GOV in a Box and Drinking Water Cybersecurity in a Box](#)

Cybersecurity Risk and Threat Strategies

The NH SLCGP Planning Committee should use this plan and operate under their approved charter to develop and coordinate strategies and projects to address cybersecurity risks and cybersecurity threats with other organizations, including consultation with local governments and associations of local governments. Specifically, the committee includes representatives from the New Hampshire Municipal Association and the New Hampshire Association of Counties along with the New Hampshire Public Risk Management Exchange to continuously solicit and receive input and feedback from their respective members.

Rural Communities

Rural communities are assured adequate access to projects under the SLCGP by virtue of their representation on the planning committee and outreach activities that will be done by the Planning Committee as a whole and individual members of the Planning Committee.

FUNDING & SERVICES

The State of New Hampshire SLCGP Planning Committee intends to focus on 3 new efforts to strengthen cybersecurity across the State. These efforts include:

- Improve and refine the SLCGP Cybersecurity Plan and manage all years approved projects in execution.
- Implement Endpoint and Server Managed Detection and Response for High Value Targets (HVT) in 100% of NH School Administrative Units for an initial 3-year period (Public K12s.)
- Cybersecurity Improvements to Community Drinking Water and Wastewater Systems (Public-Sector owned and/or operated).

These efforts are detailed in **Appendix B: Project Summary Worksheet**

NOTE: All approved projects from FFY2022 and FFY2023 are still in execution across the State of New Hampshire

Distribution to Local Governments

The State of New Hampshire intends to use at least 80%, and most likely more, of the funding received through SLCGP to deliver services and capabilities to local government entities as described in **Appendix B: Project Summary Worksheet**. As approved (unanimously) by the NH SLCGP Planning Committee, the State of New Hampshire **WILL NOT** provide sub-grants or direct pass through of funds as part of this program. This approach, including ensuring that 25% of the Grant Funding is received as services to rural areas meets the requirement in the State and Local Cybersecurity Improvement Act: e.2.B.xvi. Individual local and rural recipients will provide local consent as part an integrated online process when they apply for the services.

ASSESS CAPABILITIES

The New Hampshire SLCGP Planning Committee used Appendix A, the Cybersecurity Plan Capabilities Assessment to assess and document capabilities for the cybersecurity plan elements included in this plan.

IMPLEMENTATION PLAN

Organization, Roles, and Responsibilities

At the State Level, there are four individuals with primary responsibility and accountability under the Law for providing and maintaining the information technology infrastructure, including all aspects of cybersecurity for their respective branch of Government. For the Executive Branch of State Government, the senior individual is the Commissioner of the Department of Information Technology (Referred to as the State CIO assisted by the Chief Information Security Officer (CISO.) For the Legislative Branch of State Government, this individual is the Chief Operating Officer of the General Court of New Hampshire. For the Judicial Branch of State Government, this individual is the Chief Information Officer within the Administrative Office of the Courts. The State Chief Information Security Officer reports to the State CIO. Additionally, there are IT Leaders and ISOs in various other State organizations depending on their size and complexity.

These individuals routinely collaborate and coordinate through two entities established by statute, The Information Technology (IT) Council, and the Cybersecurity Advisory Committee (CAC.)

Resource Overview and Timeline Summary

The following information is provided to meet the requirements in the State and Local Cybersecurity Improvement Act: e.2.E. and the NOFO.

This plan was coordinated with the NH CISA Cybersecurity Advisor on 1 OCTOBER 2024.

The Planning Committee approved the projects and spending levels documented in this plan on 9 OCTOBER 2024 per the Committee Charter.

Voting Members of the Planning Committee	
Goulet, Denis	State of New Hampshire, Chief Information Officer (CIO)
Weeks, Ken	State of New Hampshire, Chief Information Security Officer (CISO)
Bouchard, Rod	County of Cheshire, Assistant County Administrator
Buxton, Robert	Director, NH Homeland Security and Emergency Management
Byrnes, Margaret	NH Municipal Association, Executive Director
Casey, Cori	NH PRIMEX, Risk Manager
Dias, John	Town of Merrimack, IT Director
Fortier, Jean	City of Manchester, IT Director
Lavoie, Steve	NH Department of Safety, Assistant Commissioner
Nudd, Tom	University System of New Hampshire, Chief Information Security Officer (CISO)
Olstad, Josh	Oyster River Cooperative School District, Director of Information Technology
Pfaff, Terry	The General Court of New Hampshire, Chief Operating Officer (COO)
Rae, Brian	Town of Goffstown, IT Director
Seaton, Matthew	Administrative Office of the Courts, Chief Information Officer (CIO)
Smith, Glen	City of Laconia, Director of Finance
Trumble, Tom	Merrimack County, IT Director
Wieters, David	NH DHHS, Information Services Director
Yasenchock, Dr. David	University System of New Hampshire, Director of Cyber GRC/Faculty
CISA NH Cybersecurity Advisor	
Rossi, Rick	NH Cybersecurity Advisor
Planning Committee Support / SAA	
Aulson, Sean	SLCGP Program Manager
Bresnahan, Janice	Grants Manager
Chapman, Kelly	Grants Manager and New Hampshire SAA
Schelb, Douglas	Deputy CISO

The State of New Hampshire intends to request the following financial resources to implement the Cybersecurity Plan for FFY2024:

NH Allocation / NOFO	%	Match Requirement	Amount of Match	TOTAL AMOUNT
\$3,808,572.00	1.35%	30%	\$1,632,246.00	\$5,440,810.00
			After 5% M&A	\$5,168,777.00 For Projects

The match requirement is authorized in State of New Hampshire Operating funds for this grant year.

METRICS

New Hampshire - Cybersecurity Program Metrics			
Program Goal	Program Objectives	Associated Metrics	Metric Description (Details, source, frequency)
1. Improve State and Local Entities capability and capacity to adopt and use best practices and methodologies to enhance cybersecurity	1.1 Improve and Refine SLGCP Cybersecurity Plan and execute approved projects from all FFYs.	Plan approved by CISA.	Email from CISA confirming approval of plan.
	1.2 Implement Endpoint and Server Managed Detection and Response for High Value Targets (HVT) in 100% of NH School Administrative Units for 3 years. (Public K12s)	Number of SAU's with Endpoint and Server Managed Detection and Response for HVTs deployed and operating.	Integer, Report from Vendor, quarterly. % of total SAUs = X /139.
	1.3 Cybersecurity Improvements to Community Drinking Water and Wastewater Systems (Public owned/operated)	Number of Community Water Systems serviced.	Integer, Report from vendor, quarterly.

APPENDIX A: CYBERSECURITY PLAN CAPABILITIES ASSESSMENT

COMPLETED BY: State of New Hampshire CISO and approved by the NH Cybersecurity Planning Committee (CPC)				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	Incomplete implementation across the totality of the State and Local Government entities.	Foundational	2,3	
2. Monitor, audit, and track network traffic and activity	Incomplete implementation across the totality of the State and Local Government entities.	Foundational	2,3	
3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts	Incomplete implementation across the totality of the State and Local Government entities.	Fundamental	1,2,3	
4. Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk	Incomplete implementation across the totality of the State and Local Government entities. Different Processes used by State entities vice PRIMEX members and other Local Entities	Fundamental	1,2,3	
5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST)				
a. Implement multi-factor authentication	Incomplete implementation across the totality of the State and Local Government entities.	Fundamental	3	
b. Implement enhanced logging	Incomplete implementation across the totality of the State and Local Government entities.	Foundational	2,3	
c. Data encryption for data at rest and in transit	Based on standard configurations of Microsoft and Network Devices this is addressed	Intermediary	3	
d. End use of unsupported/end of life software and hardware that are accessible from the Internet	Incomplete implementation across the totality of the State and Local Government entities.	Foundational	2,3	

COMPLETED BY: State of New Hampshire CISO and approved by the NH Cybersecurity Planning Committee (CPC)				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) (If applicable – as provided in Appendix B)	Met
e. Prohibit use of known/fixed/default passwords and credentials	Incomplete implementation across the totality of the State and Local Government entities.	Foundational	2,3	
f. Ensure the ability to reconstitute systems (backups)	Incomplete implementation across the totality of the State and Local Government entities.	Intermediary	None under this program	
g. Migration to the .gov internet domain	Incomplete across the eligible entity	Advanced	Completed funding in previous FFY 22 and 23	
6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain	Incomplete across the eligible entity	Advanced	2,3	
7. Ensure continuity of operations including by conducting exercises	Different processes are used across the various State and Local Government entities. Some are managed services, provided through PRIMEX and some are inherent in State process and Procedure	Intermediary	Previously funded in FFY 2023	
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)	Different processes are used across the various State and Local Government entities. Some are managed services, provided through PRIMEX and some are inherent in State process and Procedure	Intermediary	3	
9. Ensure continuity of communications and data networks in the event of an incident involving communications or data networks	Pretty solid at the State Level and for Local First Responders, but less than Advanced for many other local entities.	Intermediary	2,3	

COMPLETED BY: State of New Hampshire CISO and approved by the NH Cybersecurity Planning Committee (CPC)				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) (If applicable – as provided in Appendix B)	Met
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 performance of information systems within the jurisdiction of the eligible entity	Incomplete implementation across the totality of the State and Local Government entities.	Fundamental	2,3	
11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department	Will stick with current process and arrangement. No intent to expand information sharing agreements.	Intermediary	None under this program	
12. Leverage cybersecurity services offered by the Department	NOFO requires organizations receiving funding from the grant take MS-ISAC NCSR (membership/services paid by CISA) and CISA Vuln Scanning and Web App Scanning.	Foundational	2,3	
13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives	Replacement of end of life/end of support equipment used at the convergence of IT/IO systems.	Fundamental	2,3	
14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats	This plan contributes to this required element	Advanced	1,2,3	

COMPLETED BY: State of New Hampshire Cybersecurity Planning Committee (CPC)				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) (If applicable – as provided in Appendix B)	Met
15. Ensure rural communities have adequate access to, and participation in plan activities	Inherent in the program administration. Apart from 2 Cities, all local entities in NH are rural.	Advanced	2,3	
16. Distribute funds, items, services, capabilities, or activities to local governments	New Hampshire has a mature SAA that routinely manages FEMA/DHS Grant programs. New Hampshire will ONLY deliver shared services to locals. There will be no pass-through funding as part of New Hampshire’s SLCGP.	Advanced	1,2,3	

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**.

State of New Hampshire SLCGP Projects							
Rank	1. Project Name	2. Project Description	3. Related Required Element # from APPENDIX A.	4. Cost	5. Status	6. Priority	7. Project Type
1	FFY2024-1: NH Statewide Cybersecurity Plan Refinement, Maintenance, Reporting, and Metrics Analysis	Additional planning by Cybersecurity Planning Committee to refine Cybersecurity Plan Submission for subsequent FYs as well as analysis and reporting of program metrics. The Program Manager also facilitates intake of requests and enrollment of local entity for services.	1,2,3,4,14,16	\$300,000.00	Ongoing	High	Plan
2	FFY2024-2 Managed Detection and Response Implementation for NH (Public) K12 High Value Targets for 3 years	Implement Endpoint and Server Managed Detection and Response for High Value Targets (HVT) in 100% of NH School Administrative Units (Public K12s) Leverage NH Statewide Contract for CROWDSTRIKE Falcon Complete for 3 years.	1,2,3,4,5b,5d,5e,6,9,10,12,13,14,15,16	\$3,600,000.00	Future	High	Equip & Train
3	FFY2024-3 Cybersecurity Improvements to (Public) Community Drinking Water and Wastewater Systems	Modernize/Harden (or perform initial fielding and installation) of hardware, tools, and connectivity from the Water System Operator’s Interface Device and the SCADA control unit of the Community Drinking Water and/or Wastewater Systems (Public-Sector Owned or Operated Systems). Continue an ongoing effort. NH CISA Cybersecurity Advisor is already embedded in this project performing assessments.	1,3,4,5a,5b,5c,5d,5e,6,8,9,10,12,13,14,15,16	\$1,268,777.00	Ongoing	High	Equip & Train

APPENDIX C: ENTITY METRICS

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

Cybersecurity Plan Metrics			
Planning Goal	Plan Objectives	Associated Metrics	Metric Description (Details, source, frequency)
1. The State of New Hampshire has an approved Cybersecurity Plan that meets the SLCGP requirements as defined in the NOFO	1.1 Draft the Plan	Draft Plan exists in Document Library	CISO confirms Draft Plan is in Document Library
	1.2 Committee Approves Plan	Signed Letter by CIO	Committee Meeting Minutes
	1.3 Submit the Plan to CISA	Confirmation of Receipt	Email from CISA
	1.4 CISA Approves Plan	Statement of Approval	Email from CISA
2. Receive Funding from SLCGP	2.1 Funding received to Execute approved projects	Receipt of funds	Accept and Expend approval from Governor and Council
3. Execute Procurement Process for Each Approved Project	3.1 Execute approved projects	Projects are invoiced and paid	Financial Reporting via SAA
	3.2 Closeout approved projects	Projects are terminated or renewed	Financial Reporting via SAA
4. Process services for Local Entities and Rural areas that request inclusion	4.1 Enroll Local Entities in Services	Number of entities enrolled in each approved project	Financial Reporting via SAA
5. Review, Revise and Update Plan for next FY as required.	5.1 Repeat Objectives for Goal 1 for subsequent FY	See Goal 1	See Goal 1.