STATE OF RHODE ISLAND CYBERSECURITY PLAN

September 2023

Approved by State of Rhode Island Cybersecurity Planning Committee on 8 September 2023
Version 1.0

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LETTER FROM STATE OF RHODE ISLAND CYBERSECURITY PLANNING COMMITTEE

Greetings,

The State of Rhode Island (SoRI) cybersecurity planning committee is pleased to present to you the 2023 State of Rhode Island Cybersecurity Plan (RICSP). The RICSP represents the State of Rhode Island's commitment to support continuous maturation of the cybersecurity posture of the state and our local municipalities. In addition, this plan meets the requirement of the current U.S. Department of Homeland Security guidelines for the State and Local Cybersecurity Grant Program (SLCGP).

Representatives from the State of Rhode Island governing body/represented bodies with the SoRI cybersecurity planning committee collaborated to develop this RICSP with actionable and measurable goals and objectives that have champions identified to ensure completion. These goals and objectives focus on 1) *the mitigation of identified cybersecurity risks*, 2) *the adoption of zero trust principles and architecture,* 3) *promoting a cyber aware culture across state and local government*. This approach is designed to support the State of Rhode Island in planning for new technologies and navigating the ever-changing cybersecurity landscape. They also incorporate the SLCGP required plan elements.

As we continue to mature cybersecurity, we remain dedicated to improving our resilience among disciplines and across jurisdictional boundaries. With help from cybersecurity practitioners, we will achieve the goals set forth in the RICSP and become a model for cyber resilience.

Sincerely,

Brian Tardiff
State of Rhode Island Chief Digital Officer / Chief Information Officer
Chair of RI Cybersecurity Planning Committee
Department of Administration, Enterprise Technology Strategy and Services

Nathan Loura
Co-Chair of RI Cybersecurity Planning Committee
State of Rhode Island Chief Information Security Officer
Department of Administration, Enterprise Technology Strategy and Services

INTRODUCTION

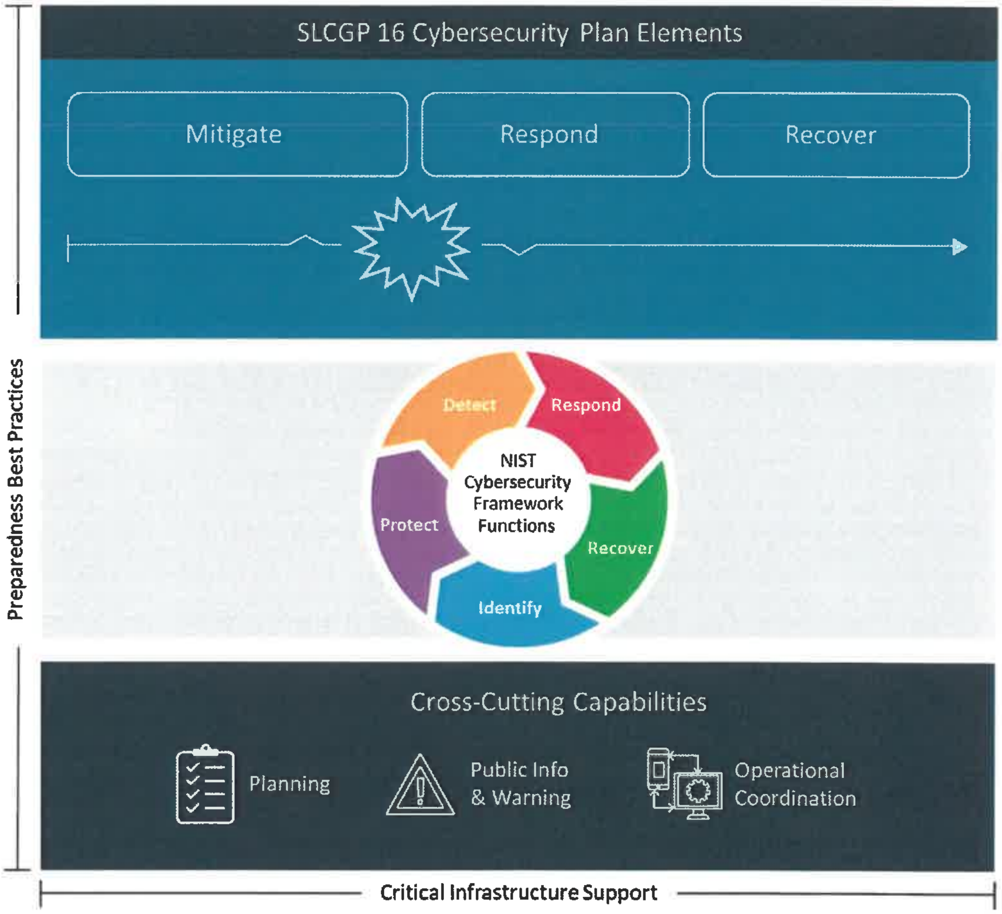
The RICSP is a three-year strategic planning document that contains the following components:

- **Vision and Mission:** Articulates the vision and mission for improving cybersecurity resilience interoperability 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 the State of Rhode Island 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 SoRI cybersecurity program. The RICSP is a guiding document and does not create any authority or direction over any of the State of Rhode Island's or local systems or agencies.
- **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 State of Rhode Island. This is especially important to develop a holistic cybersecurity plan.
- **RICSP 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 the State of Rhode Island along with methods and strategies for funding sustainment and enhancement to meet long-term goals.

- **Implementation Plan:** Describes the State of Rhode Island's plan to implement, maintain, and update the RICSP 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 the State of Rhode Island will measure the outputs and outcomes of the program across the State of Rhode Island.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework[1], included in Figure 1, helps guide key decision points about risk management activities through various levels of an organization from senior executives to business and process level, as well as implementation and operations.

Figure 1: Achieving Cyber Resilience Through Comprehensive Cybersecurity Plans


SLCGP 16 Cybersecurity Plan Elements
Mitigate
Respond
Recover
Preparedness Best Practices
Detect
Respond
NIST Cybersecurity Framework Functions
Protect
Recover
Identify
Cross-Cutting Capabilities
Planning
Public Info & Warning
Operational Coordination
Critical Infrastructure Support

[1] https://www.nist.gov/cyberframework/getting-started

Vision and Mission

Vision:

Make cybersecurity programmatic throughout Rhode Island state and local government to protect critical systems, data, and services.

Mission:

Develop, coordinate, drive, and maintain the cross-functional efforts necessary for Rhode Island state and local government to effectively manage cybersecurity risk. This will be achieved through strategic and tactical investments in the people, processes, and technology required to build a sustainable statewide cybersecurity program.

Cybersecurity Program Goals and Objectives

The State of Rhode Island Cybersecurity goals and objectives include the following:

Cybersecurity Program	
Program Goals	**Program Objectives**
1. Increase the resilience of the information systems supporting the health, safety, and security of Rhode Island's constituents.	1.1: Strategies to implement Zero Trust Architecture
	1.2: Strategies for Disaster Recovery operations
	1.3: Third party risk management
2. Manage statewide cybersecurity risk through defined and measured information technology and operational technology program, project, and vendor governance.	2.1: Application rationalization and cloud adoption strategies
	2.2: Software and hardware management (SAM/HAM)
	2.3: Information Technology Service Management Framework Implementation
3. Govern and protect the statewide shared data ecosystem.	3.1: Statewide, Secure Data Mesh Architecture
	3.2: Data security and categorization
	3.3: Privileged Access Management
	4.1: Security awareness training, using an equity lens for outreach and curriculum

Program Goals	Program Objectives
4. Create a statewide culture of digital literacy and cyber awareness through a sustained and equitable education and awareness program.	4.2: Statewide cybersecurity workforce development strategy, with a focus on increasing diversity, especially racial and ethnic diversity, in the workforce
	4.3: Statewide digital literacy training program, in multiple languages
5. Mature the cyber hygiene of the state and local municipality technology ecosystems.	5.1: Enhanced Governance, Risk and Compliance capabilities
	5.2: Statewide Cybersecurity Threat Information Sharing across all municipalities
	5.3: Improved Cybersecurity Incident response capabilities across all municipalities

CYBERSECURITY PLAN ELEMENTS

Manage, Monitor, and Track

A primary goal of this plan is to manage statewide cybersecurity risk through defined and measured information technology (IT) and operational technology (OT) program, project, and vendor governance. This includes the adoption and adherence to IT Service Management frameworks designed to manage IT / OT throughout its lifecycle, ensuring that end of life hardware or software are not in use through the adoption of hardware and software asset management tools.

Monitoring, mitigation, and reporting of vulnerabilites across the state's IT / OT environment is one fo the most critical components to reducing the state's overall risk posture. Municipalities will be encouraged to select and deploy / mature technologies that will automate the vulnerability management process.

Third party vulnerability management must be executed as the adoption of "X"as a Service is more widely adopted across state and local government entities. This management must include contract general terms and conditions that identify vulnerability management service level agreements (SLA) and penalities for violations of contractual SLA's.

Third party vulnerabilty and risk management must also include review of contractually mandated System and Organizational Controls (SOC) audit reports and reporting of corrective action plans by contracted third parties. The deployment of governance, risk and compliance solutions can assist in this effort and should be prioritized.

Monitor, Audit, and Track

The state has deployed network monitoring services via MS-ISAC Albert sensors, Security Incident Event Management (SIEM), third-party information security continuous monitoring, and extended detection and response (XDR). Municipalities should leverage CISA and MS-ISAC services where available / applicable to enhance network monitoring capabilities, as well as make targeted investments in the deployment of SIEM solutions on-premises or in the cloud by leveraging existing state contracts or Master Purchasing Agreements (MPA's).

Internet Service Provider (ISP) contracts with the state and municipalities should include network monitoring and reporting services, DOS / DDOS protection, as well as DNS security when available.

The state plans to expand centralized monitoring and reporting capabilities through investment in the growth of the capacity and capabilities of the state's Fusion center as the hub for statewide cybersecurity and threat intelligence ingestion and reporting.

Enhance Preparedness

SoRI will engage with CISA and RIEMA resources to plan and execute tabletop exercises of the state's Major Cybersecurity Incident Response Plan (MCIRP). These tabletop exercises will include members of the SLCGP planning committee and municipalities to better measure response capabilities across the state. The state's yearly Threat Hazard Identification Risk Assessment (THIRA) and Stakeholder Preparedness Report (SPR) surveys will be referenced in development of the tabletop exercises to ensure alignment and maturity measurement against the planning, organization, training, and exercise (POTE) capability target goals.

Tabletop lessons learned will be used to plan and execute actions to further the maturity of the state and local government overall readiness to respond to and mitigate cybersecurity incidents, including those impacting CIKR.

Assessment and Mitigation

SoRI state and local government entities will continue to adopt the assessment services provided by CISA as well as leveraging the existing state and federal auditing mechanisms and contracted external third-party assessors to identify, document, and develop corrective action plans (CAP) and plan of action and milestones (POAM) to execute the mitigation of threats and vulnerabilities resulting in the reduction of overall cybersecurity risk. Assessment and mitigation planning will include the mandate of SOC audits for critical cloud hosted infrastructure, platforms, and applications.

Information security continuous monitoring (ISCM) is essential to the automation of identification and remediation of critical vulnerabilities and malware. Client based technologies such as endpoint detection and response (EDR), XDR, with planned enhancement to a governance, risk, and compliance (GRC) platform for third party risk management are vital components of the RICSP to resolve identified vulnerabilities aligned to CISA BOD 22-01 guidance.

Best Practices and Methodologies

NIST Special Publication 800-207, Zero Trust Architecture (ZTA) will be referenced as SoRI develops the strategy to architect and deploy ZTA and Secure Access Service Edge (SASE) throughout state and local government entities. This will include strategies for opportunities for the adoption of the various ZTA approaches and SASE technologies and principles such as:

- ZTA using enhanced identity governance, which includes:
    - Multi-factor authentication (MFA)
    - Prohibit use of known/fixed/default passwords and credentials
    - Privileged Access Management

  - Enhanced logging
  - Authoritative guidelines for use of service processes acting on behalf of users
- ZTA using network infrastructure segmentation and software defined perimeters, which includes:
  - Software Defined Wide Area Network (SD-WAN)
  - Cloud Access Security Broker (CASB)
  - Network micro-segmentation
  - Firewall as a Service (FWaaS)
  - Security Incident and Event Management (SIEM)

NIST Principles

SoRI has adopted the NIST Cybersecurity Framework (CSF), NIST Risk Management Framework (RMF), and NIST 800-53 Rev. 5 Security and Privacy Controls, which the SoRI Security and Risk Management Program are built upon. This adoption is reflected in the library of the SoRI Division of Enterprise Technology Strategy and Services policies, procedures, and IT systems planning, configurations, deployments, and operations.

In accordance with the vision of this plan, it is the intent of the SLCGP planning committee and its members to promulgate adoption of these frameworks by the municipalities to achieve a common baseline of policy and controls to provide for ease of assessment of maturity and cybersecurity capabilities that can be improved through strategic planning and investment. This adoption will guide critical, programmatic improvements such as:

- Data encryption for data at rest and in transit
- End use of unsupported/end of life software and hardware that are accessible from the Internet
- Ensure the ability to reconstitute systems (backups)
- Third party and supply chain risk management
- Vulnerability management
- Identity and access management
- Audits and assessments
- Cybersecurity awareness and training

Supply Chain Risk Management

The state will reference NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations. and implement municipality cyber supply chain risk management (C-SCRM) for IT and OT with active leadership from the IT Vendor Management Office (VMO) within the Division of Enterprise Technology Strategy and Services, with support from with SoRI legal, procurement, and enterprise architecture leads to ensure that a holistic, organizational risk management process is executed.

state and local government should leverage the state's centralized IT VMO, master purchasing agreements (MPA's) and procurement methodologies that have been designed to mitigate global supply chain risks through the inclusion of robust IT general terms and conditions in service and product procurements and renewals, cybersecurity insurance requirements for vendors of IT products and services, and sound IT project governance executed through the product or service lifecycle.

Tools and Tactics

The SoRI CISO, as the primary representative for MS-ISAC within the state, will leverage MS-ISAC SOC services when appropriate to request tactics, techniques, and procedures (TTP's) of suspected and identified malicious activity targeting SoRI entities to share threat intelligence and promote the use of MS-ISAC SOC and incident response services when needed.

The intent of the state is to scale threat intelligence reporting of adversary TTP's to municipalities and potentially impacted state and local government entities as threat intelligence is received through expansion of the state's Fusion center analysis and reporting capabilities through increased adoption of CISA, MS-ISAC, and third-party threat intelligence solutions.

Safe Online Services

A full adoption of the CISA .gov domain services by all state eligible entities is within the goals and objectives of this plan. There are currently 23 of 39 municipalities within SoRI on the .gov domain. It is within the scope and intent of this plan to migrate the remaining municipalities to operate on the .gov domain.

A focused effort to ensure the proper adoption of encryption of data in transit and at rest for all state and local government business systems and interconnected vendor systems will ensue, including the full adoption of HTTPS for all state and local websites.

Continuity of Operations (COOP)

A programmatic method for the testing of state and local government continuity of operations and disaster recovery (DR) plans for critical systems should be executed often. Inclusion of cybersecurity events and incidents in regularly scheduled tabletop exercises for COOP and DR must occur to define gaps in COOP capabilities and define plans for improvement.

Architecture review and testing of back-ups and restoration should occur regularly for mission critical systems to identify and plan for the mitigation of gaps in the plan and the organizations' ability to execute the plan. This includes a review of the competency and capacity of the staff supporting COOP and disaster recovery operations.

Power and network redundancy and resiliency should be assessed and included in any exercise of COOP plans with gaps identified and any integrations or dependencies with CIKR infrastructure identified.

The adoption of cloud services for modernization of IT / OT should be prioritized to maximize the enhanced COOP and DR benefits that cloud type services provide versus physical, on-premises infrastructure that often cannot easily be recovered or restored.

Tools that accommodate consolidated storage of state and local COOP and DR plans should be explored to better facilitate and expedite coordinated response activities.

Workforce

In alignment with this plan's goals and objectives, developing a workforce with increased cybersecurity competencies will be pursued. It is our intent to leverage the National Initiative for Cybersecurity Education (NICE) at the state level to integrate cybersecurity training components into job descriptions for the state information technology and cybersecurity workforces. SoRI ETSS will lead this effort and support the adoption of the NICE Workforce Framework statewide through coordination with the SLCGP and assistance from the SoRI Division of Human Resources.

We will propose projects within the scope of this grant program to execute training and training programs for workforce roles across the state that are responsible for the protection of critical systems, infrastructure, and data. Through this plan, we will work to ensure that employee cyber hygiene and awareness programs are implemented by state and local government entities.

As a member of the SoRI SLCGP planning committee, the RI National Guard is an active participant and supporter of the Air and Space Forces CyberPatriot youth cyber education program and will seek to continue to expand adoption of this program across the state's high school and middle school populations.

Continuity of Communications and Data Networks

SoRI has a documented Information Technology Sector Specific Plan (SSP) as an annex to the Rhode Island Critical Infrastructure Program Plan, managed by RIEMA. This IT SSP highlights the key stakeholders (public and private) responsible or accountable for the resilience and continuity of operations of data networks and critical IT systems across the state.

The state also has a documented Major Cybersecurity Incident Response Plan that details how key state agencies will respond to, mitigate, and recover cybersecurity incidents impacting state or local government systems and infrastructure. This plan will be exercised in the fall of 2023, with lessons learned documented and any investments needed to enhance resiliency identified. Municipality participation will be encouraged to identify any critical gaps in resiliency capabilities at the local level.

Assess and Mitigate Cybersecurity Risks and Threats to Critical Infrastructure and Key Resources (CIKR)

The SLCGP planning committee has members from various CIKR sectors and will rely upon those sector representatives to present projects to the committee that directly align with sector specific risk mitigation strategies.

Sector Specific Plans (SSPs) maintained by RIEMA for each of the CIKR sectors within the state will be referenced in the proposal of projects to the SLCGP committee. A focus on improving the resilience of the CIKR systems and infrastructure is an objective of this plan and will be tracked and reported accordingly.

The state's yearly Threat Hazard Identification Risk Assessment (THIRA) and Stakeholder Preparedness Report (SPR) surveys will be referenced in development of the tabletop exercises to ensure alignment and maturity measurement against the planning, organization, training, and exercise (POTE) capability target goals especially as related to CIKR.

Cyber Threat Indicator Information Sharing

The state currently leverages the Rhode Island State Police managed Fusion center as the cyber threat information clearing house. Recently passed legislation mandates the reporting of cybersecurity incidents and a process to enable these new reporting requirements is in active development. All existing resources and opportunities to leverage technology to enhance this reporting will occur, to include the adoption of managed services if feasible.

We will actively explore opportunities to grow our threat ingestion, hunting, analysis, and sharing capabilities within the scope of this plan through consolidation of threat intelligence sources (MS-ISAC, EI-ISAC, FBI, DoD, CISA, private industry, etc..), and dissemination of relevant cybersecurity threat information to state and local government entities through investments in the deployment of tools, staff augmentation and training, and process automation where possible.

Leverage CISA Services

The State of Rhode Island has an active and engaging relationship with our CISA state cybersecurity advisor, who has engaged with and either completed or has assessments scheduled for 12 of 39 of SoRI municipalities, with interest for execution of an assessment from 7 more. It is our intent and recommendation to continue to leverage the CISA assessment capabilities as well as the full suite of technical references and resources available. SoRI is also an active participant in MS - ISAC, EI – ISAC and leverages Albert Sensor services at the state and higher education.

A CISA led Cyber Storm exercise is scheduled for execution in late September 2023 to assess the RI Major Cybersecurity Incident Response Plan. As municipality and state cybersecurity maturity increases, further adoption, and utilization of CISA services will occur.

Information Technology and Operational Technology Modernization Review

In alignment with plan goal 2, Manage statewide cybersecurity risk through defined and measured information technology and operational technology program, project, and vendor governance; IT / OT inventory and rationalization should be executed by portfolio owners across state and local entities.

Maintaining an IT / OT inventory will enable systems owners to develop strategies for modernization that priortize risk mitigation through selection and implementation of secure, scalable, and sustainable IT / OT solutions with a goal of technology modernization through adoption of modern cloud, hosted, and virtual solutions across the IT / OT ecosystems. The IT / OT systems associated with CIKR should be prioritized for modernization by state and local government.

ETSS will share portfolio and project governance best practices with municipalites and leverage state policy and enterprise archtiecture principles to support IT / OT modernization strategy development.

Cybersecurity Risk and Threat Strategies

SoRI ETSS will develop strategy with associated policy that incorporates applicable state and local regulation, the core functions of NIST Cyber Security Framework, and align with the NIST Risk Management Framework to address cybersecurity risks and cybersecurity threats. These strategies and policies will be socialized to all with local governments and associations of local governments within their jurisdiction, neighboring entities, territories, and Tribal governments (as applicable), or members of an ISAC; and state partnerships to help unify risk management into a common impact and likelihood projection enabling the sharing of best practice mitigations and actionable understating of supply chain risk.

Once strategies are socialized, a continuous monitoring program will be matured to ensure risks are identified, categorized, and prioritized across all assets and third-party organizations in the supply chain. The state can follow with the execution of cost-effective remediation while sharing continuous improvement consultation to all with local governments and associations of local governments within their jurisdiction, neighboring entities, territories, and Tribal governments (as applicable), or members of an ISAC, and state partnerships. The state can also reduce systemic risks by effectively integrating risk-management practices, human-focused cyber hygiene, and secure engineering solutions delivered in a seamless and transparent process to our workforce and constituents using an equity lens.

Rural Communities

Rural areas represent 30% of the SLCGP planning committee and are critical in the construct of the RICSP. The RI SLCGP planning committee, through coordinated outreach with the Rhode Island League of Cities and Towns, and the Rhode Island Cybersecurity Advisor (CISA) will assist rural areas in participation of the SLCGP and relevant projects through guidance, assessment, and planning as required to realize the

SLCGP 25% funding objectives for rural areas. The review of projects will also include the Centers for Disease Control and Prevention (CDC) Social Vulnerability Index (SVI) SVI Interactive Map (cdc.gov) for municipalities as a consideration for prioritization of investment.

Municipality	Type	Pop. (2020)	Rural vs. Urban
Barrington	Town	17,153	RURAL
Bristol	Town	22,493	RURAL
Burrillville	Town	16,158	RURAL
Central Falls	City	22,583	RURAL
Charlestown	Town	7,997	RURAL
Coventry	Town	35,688	RURAL
Cranston	City	82,934	URBAN
Cumberland	Town	36,405	RURAL
East Greenwich	Town	14,312	RURAL
East Providence	City	47,139	RURAL
Exeter	Town	6,460	RURAL
Foster	Town	4,469	RURAL
Glocester	Town	9,974	RURAL
Hopkinton	Town	8,398	RURAL
Jamestown	Town	5,559	RURAL
Johnston	Town	29,568	RURAL
Lincoln	Town	22,529	RURAL
Little Compton	Town	3,616	RURAL
Middletown	Town	17,075	RURAL
Narragansett	Town	14,532	RURAL
Newport	City	25,163	RURAL
New Shoreham	Town	1,410	RURAL
North Kingstown	Town	27,732	RURAL
North Providence	Town	34,114	RURAL
North Smithfield	Town	12,588	RURAL
Pawtucket	City	75,604	URBAN
Portsmouth	Town	17,871	RURAL
Providence	City	190,934	URBAN
Richmond	Town	8,020	RURAL
Scituate	Town	10,384	RURAL
Smithfield	Town	22,118	RURAL
South Kingstown	Town	31,931	RURAL
Tiverton	Town	16,359	RURAL
Warren	Town	11,147	RURAL
Warwick	City	82,823	URBAN
Westerly	Town	23,359	RURAL
West Greenwich	Town	6,528	RURAL
West Warwick	Town	31,012	RURAL

Woonsocket	City	43,240	RURAL
State Population 2020 census		**1,097,379**	

FUNDING & SERVICES

The State of Rhode Island will provide subawards to municipalities for projects that align with the program goals and objectives within this plan. Each municipality has varied levels of cybersecurity maturity and the intent of the state plan is to leverage the SLCGP to approve and fund projects that provide each municipality the opportunity to achieve a higher level of sustainable cybersecurity maturity. State master purchasing agreements and existing cybersecurity contracts and pricing agreements can be leveraged by participating municipalities. Opportunities for funding for services and solutions that can be deployed across multiple municipalities will be prioritized.

Distribution to Local Governments

Distribution of funding for cybersecurity projects will be executed by RIEMA to ensure compliance with the guidelines of the SLCGP through a subaward funding model.

Proposals for projects will be submitted by the participating entities to the SLCGP planning committee through the SoRI ETSS for evaluation of alignment with the RICSP goals and objectives. Once approved by a majority vote by the SLCGP planning committee, projects funding will be distributed with the matching component issued through the SoRI Division of Enterprise Technology Strategy and Services for award year 2023.

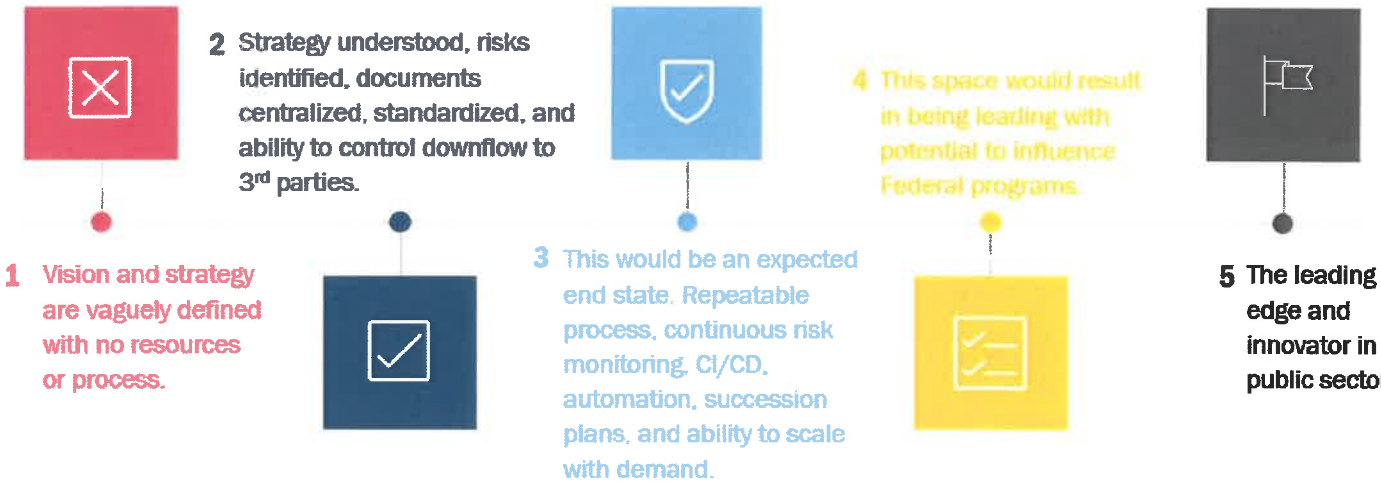
In a strategic effort to maximize participation by municipalities that historically lack funding for cybersecurity maturity efforts, SoRI has budgeted the matching component for award year 2023, and the CDO / CIO intends to request additional budget in the following years to accommodate the SLCGP matching requirement.

The existing processes for grant funding issuance as managed by RIEMA will be used for the distribution of funds to municipalities upon approval of projects by the SLCGP planning committee.

ASSESS CAPABILITIES

The SoRI CISO will lead initiatives to enhance the capability to assess and project maturity of cybersecurity programs for the state agencies with expansion to include local governments and associations of local governments within their jurisdiction, neighboring entities, territories, and Tribal governments (as applicable).

The approach to assessment will be to incorporate the requirements outlined within H.R. 3138 and applicable state and local regulations as the strategic layer of the Cybersecurity Defense Strategy and measure in a 5-tier maturity model. The tiered maturity model will range from a level 1 rating as the lowest level of maturity, with level 5 indicating the most mature defined as leading edge and the lead innovator in the public sector.



1 Vision and strategy are vaguely defined with no resources or process.

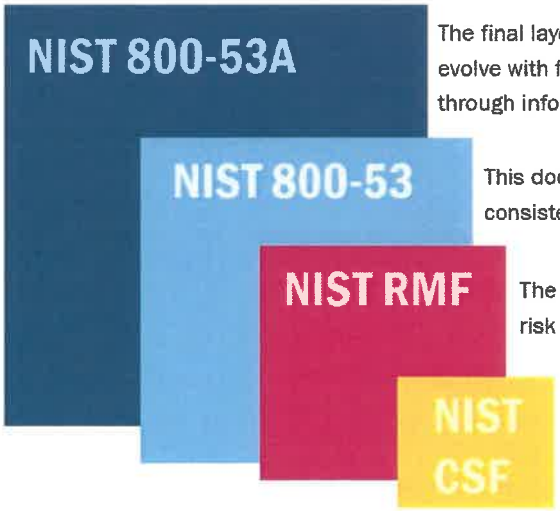
2 Strategy understood, risks identified, documents centralized, standardized, and ability to control downflow to 3rd parties.

3 This would be an expected end state. Repeatable process, continuous risk monitoring, CI/CD, automation, succession plans, and ability to scale with demand.

4 This space would result in being leading with potential to influence Federal programs.

5 The leading edge and innovator in the public sector.

The measurement supporting the maturity model will be the adoption of the control stack with a sustained and repeatable continuous monitoring program. These metrics will be assessed foundationally using the CISA Cyber Performance Goals (CPG) based on the NIST CSF for self-assessment with evolution to assessment of more mature programs against NIST 800-53A grounded in risk impact baseline with intention for standard as a unified assessment framework between SoRI, local governments and associations of local governments within their jurisdiction, neighboring entities, Territories, and Tribal governments (as applicable). Maturity progress post self-assessments are intended to be substantiated by a neutral third party if requested by an authorizing official from local governments and associations of local governments within their jurisdiction, neighboring entities, territories, and Tribal governments (as applicable).



The final layer is the continuous monitoring to ensure impact baselines risks are mitigated and evolve with future technology. This layer includes other baselines and best practices fed through information sharing and threat intelligence cooperation throughout the SoRI.

This document provides controls to with defined guidance and standards to implement consistent protections in alignment with a unified impact baseline for the SoRI.

The Risk Management Framework provides a disciplined 7-step approach to mitigate risk throughout the lifecycle to standardize the approach throughout the SoRI.

The Cybersecurity Framework outlines the 5 core functions: Recover, Identify, Protect, Detect, and Respond. Foundational assessment with the CISA Cyber Performance Goals Checklist (CPGs).

Implementation Plan

Organization, Roles, and Responsibilities

Each goal and its associated objectives have a timeline with a target completion date, and one or more owners that will be responsible for overseeing and coordinating its completion. Accomplishing goals and objectives will require support and cooperation from numerous individuals, groups, or agencies, and may be added as formal agenda items for review during regular governance body meetings.

The SoRI Division of Enterprise Technology Strategy and Services led by the CDO / CIO, will ensure proper project governance is applied to all approved projects. The SLCGP planning committee will review project updates during regular governance body meetings and provide timely reporting of project completion and success as mandated by this grant program.

RIEMA will track and report grant spending of SLCGP funds with support from the ETSS IT financial management office as needed.

Overall risk measurement and project success criteria will be managed by the SLCGP planning committee and led by the SoRI Chief Information Security Officer (CISO).

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

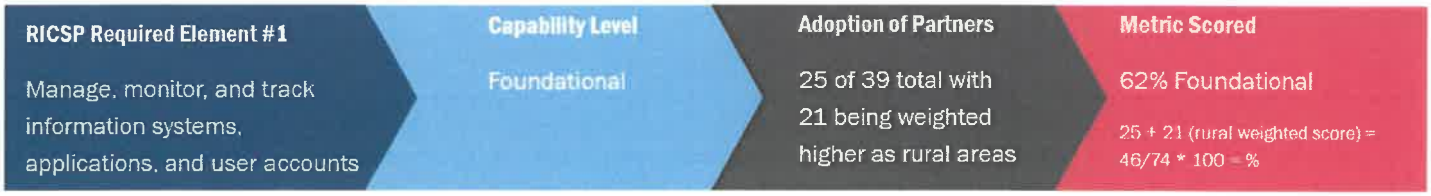
Resource Overview and Timeline Summary

Projects approved by the SoRI SLCGP planning committee are aligned with a corresponding SLCGP program goal, objectives, and SLCGP required elements. The efforts are assigned to one or more responsible owners with oversight by SoRI ETSS. The SoRI CISO will oversee and coordinate project execution as the designee from ETSS, as achieving these goals and objectives will necessitate multilateral support and coordination between the SoRI, local governments and associations of local governments within their jurisdiction, neighboring entities, territories, and Tribal governments (as applicable).

Formal agenda items will be identified for review during SoRI SLCGP planning committee meetings to facilitate effective progress tracking. In compliance with the State and Local Cybersecurity Improvement Act: e.2.E, the Plan documents the essential resources across the tables in APPENDIX A, B, and C. which provide a projected timeline for each project, whenever feasible to satisfy the requirements outline within the act.

METRICS

Throughout the implementation of the RICSP, the SoRI ETSS Team remains dedicated to assessing our local partners progress in achieving the RICSP objectives and the SLCGP overall goals. The CISO will provide oversight to evaluate the advancement against the program objectives outlined in this plan, ensuring they align with the essential elements specified in the RICSP's funding opportunity. The metrics will be framed within the 'capability level' selected in APPENDIX A for all 'Cybersecurity Plan Required Elements' measured in adoption by the total number of local governments and associations of local governments within their jurisdiction, neighboring entities, territories, and Tribal governments (as applicable) with an added weight for rural communities.



RICSP Required Element #1

Manage, monitor, and track information systems, applications, and user accounts

Capability Level

Foundational

Adoption of Partners

25 of 39 total with 21 being weighted higher as rural areas

Metric Scored

62% Foundational

25 + 21 (rural weighted score) = 46/74 * 100 = %

While some initiatives within the plan may have varying durations, spanning multiple years, or operating continuously, our team remains accountable for overseeing progress tracking. This responsibility involves using meaningful metrics defined in the example above and reporting method using the sample table below to accurately assess the RICSP progress and achievements made by the SoRI, local governments and associations of local governments within their jurisdiction, neighboring entities, territories, and Tribal governments (as applicable).

Sample Table - Cybersecurity Plan Metrics

Sample Program Objectives	Sample Program Sub-Objectives	Sample Associated Metrics	Sample Metric Description (details, source, frequency)
1. Increase the resilience of the information systems supporting the health, safety, and security of Rhode Island's constituents.	1.1 Strategies to implement Zero Trust Architecture foundations are developed with the stand up of a Zero Trust Center of Excellence (CoE) within ETSS and drafting of a CoE Charter accessible to all state and local agencies with their associated partners.	**Metric Base:** Scope of each municipal assets identified in planning have completed all tasks for effort. Expected rate for municipality to be considered complete is at least 85% assets that have all tasks completed. Percentage is calculated as: assets completed/assets total = *100 **Adoption Baselines:** Minimum acceptance of % of all municipalities calculated with scoring equation based on baseline of Appendix A Foundational – 65%+ Fundamental – 60%+ Intermediary – 50%+ Advanced – 40%+	Metrics data collected by ETSS and League of Cities and Town designees quarterly. Metric % is calculated based on "Metrics" section scoring equation and emailed to RIEMA SAA for input to IW and PW Sheets.

APPENDIX A: SAMPLE CYBERSECURITY PLAN CAPABILITIES ASSESSMENT

By taking the following actions, the State of Rhode Island will demonstrate that their cybersecurity plan incorporates the required assessment relating to the Cybersecurity Plan Required Elements. Ensure that the assessment incorporates a State of Rhode Island-wide perspective. It also links any line items from the project summary worksheet that will help to establish, strengthen, or further develop our cybersecurity capabilities.

Eligible entities can use the "EVAL" column as a self-assessment tool in conjunction with the CISA CPGs Checklist[1]. Entities with newly initiated programs could use this spreadsheet to track the status of their cybersecurity planning efforts. Similarly, entities with advanced programs could use this worksheet to evaluate their current cybersecurity plan using "Yes, No, Partial, or N/A."

[1] *https://www.cisa.gov/sites/default/files/2023-03/cisa_cpg_checklist_v1.0.1_final.pdf*

COMPLETED BY STATE OF RHODE ISLAND				FOR ASSESSOR
Cybersecurity Plan Required Elements	Brief Description of Current Capabilities of SLTT within the Eligible State of Rhode Island	Select capability level from: Foundational Fundamental Intermediary Advanced	Project # (s) *(If applicable – as provided in Appendix B)*	Met
1. Manage, monitor, and track information systems, applications, and user accounts	A layered defense strategy using Active Directory to control user identities and entitlements. Information systems and applications are tracked throughout the lifecycle via an IT PMO function.	Foundational	TBD	
2. Monitor, audit, and track network traffic and activity	Use of a cloud based SIEM providing centralized repository and correlated log monitoring for deviations in user and hardware activity.	Foundational	TBD	
4. Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk	ETSS currently has a vulnerability management system that can identify, score risk, and associate CVEs to flaws within software and hardware components with installed agents. These vulnerabilities are reported to responsible parties for remediation and tracking of completion.	Foundational	TBD	

5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST)	Unified policy has been drafted and published requiring update and substantiated with a defined document hierarchy with standards supporting policy, procedures supporting standards, and guidelines supporting procedures.	Fundamental	TBD	🟥
a. Implement multi-factor authentication	ETSS has implemented MFA required to access network resources	Fundamental	TBD	🟥
b. Implement enhanced logging	ETSS operates a central logging system with SIEM capability to correlate activities based on engineered content for alerting SOC personnel to a deviation in expected behavior.	Intermediary	TBD	🟥
c. Data encryption for data at rest and in transit	Encryption on endpoints and networking devices have modes enabled to enforce standard FIPS 140-2	Intermediary	TBD	🟥
d. End use of unsupported/end of life software and hardware that are accessible from the Internet	ETSS completes reviews with associated initiatives to mitigate risk of EOS/EOL assets with under development program to automate monitoring with use of service catalog capabilities within the ITSM application.	Intermediary	TBD	🟥
e. Prohibit use of known/fixed/default passwords and credentials	GPOs are enabled to enforce password criteria outlined in policy that also restricts common and easily guessed passwords.	Foundational	TBD	🟥
f. Ensure the ability to reconstitute systems (backups)	ETSS identifies RPO and RTO for critical systems with back-ups to satisfy requirement.	Fundamental	TBD	🟥
g. Migration to the .gov internet domain	SoRI has moved all agencies to the .gov and policy defines this domain service as only authorized.	Foundational	TBD	🟥
7. Ensure continuity of operations including continuity of communications and data networks in the event of an incident involving communications or data networks by conducting exercises	SoRI completes quarterly BCDR exercise to test capability to return to operation using ‘warm site’. ETSS also sponsors and participates within cyber and emergency preparedness exercises with Federal Agencies and Public Safety Partners.	Foundational	TBD	🟥

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)	Will require assessment to understand complexity of the various capabilities within the	Foundational	TBD	
9. 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 State of Rhode Island	Projects to mitigate to applications that would provide platforms to register then project internal and supply chain risks and identify then prioritize vulnerabilities for remediation with automated capabilities have begun. These efforts will allow for standard documentation, artifacts of exceptions, automated remediation, and best practices that can be scaled to the local municipalities and Tribal partners to effectively and continuously resolve open threats	Foundational	TBD	
10. Enhance capabilities to share cyber threat indicators and related information between the eligible State of Rhode Island and the Department	Enhancements to threat intelligence integration to SIEM ability has been initiated to allow for better visibility of potentially malicious IOCs that can be broadcast via MS-ISAC membership and growing local municipality and Tribal relationships.	Foundational	TBD	
11. Leverage cybersecurity services offered by the SoRI and Federal Agencies	ETSS has forged a partnership with local CISA, FEMA, and RIEMA partners to leverage offered capabilities and adopt unified best practices. These leveraged services, memberships, or resources defined as required within *"FY23 Notice of Funding Opportunity Appendix F: Required, Encouraged, and Optional Services, Memberships, and Resources"*	Intermediary	TBD	
12. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information	ETSS is the standard bearer within the SoRI to provide policy and associated unified baselines developed under NIST guidance to adopt across all agencies and accessible to local partners.	Fundamental	TBD	

technology and operational technology cybersecurity objectives				🟥
13. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats	The office of the CISO develops strategy, maintains a risk register, and roadmaps to identify and mitigate threats in alignment with the NIST RMF.	Foundational	TBD	🟥
14. Ensure rural communities have adequate access to, and participation in plan activities	CDO/CIO for SoRI has enacted a committee comprised of all agencies, local governments, and associations of local governments within their jurisdiction, neighboring entities, territories, and Tribal governments to allow for equitable voice for all constituents.	Foundational	TBD	🟥
15. Distribute funds, items, services, capabilities, or activities to local governments	Chair has been confirmed with identified local and Tribal representatives with charter to allow oversight and ability to approve use of funds by the identified parties.	Foundational	TBD	🟥

APPENDIX B: PROJECT SUMMARY WORKSHEET

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

1.	2. Project Name	3. Project Description	4. Related Required Element #	5. Cost	6. Status	7. Priority	8. Project Type
TBD	Local Municipality Baseline Assessment	Project to assess municipalities within the SLCGP within the CISA CPG, assess potential technology requirements, and gather expected user counts and license requests	1 - 15	N/A	Future	High	Plan/Organize
TBD	Implement MFA	Provide services to implement MFA across all assets under scope of local municipalities	2,5	TBD	Future	Medium	Equip
TBD	Cybersecurity Fundamental Training	Expand access to LMS for current cybersecurity training to all municipalities and provide OLIS resources to help provide equity access	8,11,14	TBD	Future	High	Train
TBD	RI Cyber Collective Tabletop	Plan and complete a large-scale cybersecurity tabletop exercise with full municipality participation	4,5,7,8	TBD	Future	High	Plan/Exercise
TBD	.gov migration	Migrate remaining municipalities to .gov that are currently not on domain	2,5,9,12, 13,15	TBD	Ongoing	Medium	Train/Equip
TBD	Modernize Security perimeter	Provide managed FW services option to all municipalities to modernize and unify network and protection services across whole of state	2,5,8,9,11,12, 13,15	TBD	Future	Medium	Plan/Equip
TBD	Whole of State extended detection and response	Provide managed EDR or XDR solution to enhance protection, monitoring, and detection of endpoint assets within municipalities	2,5,8,9,11,12, 13,15	TBD	Future	High	Plan/Train/Equip
TBD	Whole of State Intelligence Fusion	Integrate all municipalities into the RI Fusion center and MS-ISAC to stitch information and physical threat domains into actionable intelligence	2,5,8,9,11,12, 13,15	TBD	Future	High	Plan/Train/Equip

APPENDIX C: STATE OF RHODE ISLAND METRICS

The below table reflects the goals and objectives the SoRI cybersecurity planning committee has established with actionable taskings metrics can be built to and reported on to convey the progress of the SLCGP program.

Cybersecurity Plan Metrics			
Program Goal	Program Objectives	Associated Metrics (Based on Selected Capability Level in Appendix A)	Metric Description (Details, Source, Frequency)
Increase the resilience of the information systems supporting the health, safety, and security of Rhode Island's constituents.	1.1 Strategies to implement Zero Trust Architecture foundations are developed with the stand up of a Zero Trust Center of Excellence (CoE) within ETSS and drafting of a CoE Charter accessible to all state and local agencies with their associated partners.	TBD – requires scoping of assets from local municipalities for current baseline to be completed under plan requirements 11-15 and Row 1 entry in Appendix B	Metrics data collected by ETSS and League of Cities and Town designees quarterly. Metric % is calculated based on "Metrics" section scoring equation and emailed to SAA (RIEMA) for input to IW and PW Sheets.
	1.2 Strategies for Disaster Recovery operations are developed within ETSS and accessible to all state and local agencies with their associated partners for assitance with drafting their specifc plans.	TBD – requires scoping of assets from local municipalities for current baseline to be completed under plan requirements 11-15 and Row 1 entry in Appendix B	Metrics data collected by ETSS and League of Cities and Town designees quarterly. Metric % is calculated based on "Metrics" section scoring equation and emailed to SAA (RIEMA) for input to IW and PW Sheets.
	1.3 Third party risk management foundational program is established to assess vendor programs to a unified baseline with risks identified and informing decision on relationship. Program should also establish an annual reassessment of current third parties and identification of their fourth parties or sub processors.	TBD – requires scoping of assets from local municipalities for current baseline to be completed under plan requirements 11-15 and Row 1 entry in Appendix B	Metrics data collected by ETSS and League of Cities and Town designees quarterly. Metric % is calculated based on "Metrics" section scoring equation and emailed to SAA (RIEMA) for input to IW and PW Sheets.
Manage statewide cybersecurity risk through defined and	2.1 Application rationalization and cloud adoption strategies foundations are developed with the stand up of a Cloud	TBD – requires scoping of assets from local municipalities for current	Metrics data collected by ETSS and League of Cities and Town designees quarterly. Metric %

Program Goal	Program Objectives	Associated Metrics (Based on Selected Capability Level in Appendix A)	Metric Description (Details, Source, Frequency)
measured information technology and operational technology program, project, and vendor governance.	Center of Excellence (CoE) within ETSS and drafting of a CoE Charter accessible to all state and local agencies with their associated partners.	baseline to be completed under plan requirements 11-15 and Row 1 entry in Appendix B	is calculated based on “Metrics” section scoring equation and emailed to SAA (RIEMA) for input to IW and PW Sheets.
	2.2 Software and hardware management (SAM/HAM) capabilities are built within the ETSS ITSM tool with guides for best practice available to all state and local agencies with their associated partners.	TBD – requires scoping of assets from local municipalities for current baseline to be completed under plan requirements 11-15 and Row 1 entry in Appendix B	Metrics data collected by ETSS and League of Cities and Town designees quarterly. Metric % is calculated based on “Metrics” section scoring equation and emailed to SAA (RIEMA) for input to IW and PW Sheets.
	2.3 Information Technology Service Management Framework Implementation is established built upon NIST CSF, RMF, and 800-53 controls with guidance for best practice available to all state and local agencies with their associated partners.	TBD – requires scoping of assets from local municipalities for current baseline to be completed under plan requirements 11-15 and Row 1 entry in Appendix B	Metrics data collected by ETSS and League of Cities and Town designees quarterly. Metric % is calculated based on “Metrics” section scoring equation and emailed to SAA (RIEMA) for input to IW and PW Sheets.
Govern and protect the statewide shared data ecosystem.	3.1 Statewide, Secure Data Mesh Architecture is implemented to share acquired data among all agencies through the pre-k to retirement lifecycle with defined IAM and data classification-based protections.	TBD – requires scoping of assets from local municipalities for current baseline to be completed under plan requirements 11-15 and Row 1 entry in Appendix B	Metrics data collected by ETSS and League of Cities and Town designees quarterly. Metric % is calculated based on “Metrics” section scoring equation and emailed to SAA (RIEMA) for input to IW and PW Sheets.
	3.2 Data security and categorization is established to classify data from public and sensitive data types like Federal Tax Information (FTI), Personally Identifiable Information (PII), and Personal Health Information (PHI).	TBD – requires scoping of assets from local municipalities for current baseline to be completed under plan requirements 11-	Metrics data collected by ETSS and League of Cities and Town designees quarterly. Metric % is calculated based on “Metrics” section scoring equation and emailed to SAA

Program Goal	Program Objectives	Associated Metrics (Based on Selected Capability Level in Appendix A)	Metric Description (Details, Source, Frequency)
		15 and Row 1 entry in Appendix B	(RIEMA) for input to IW and PW Sheets.
	3.3 Privileged Access Management program that identifies privileged and administrator accounts to enforce MFA and enhanced monitoring of activities with guidance for best practice available to all state and local agencies with their associated partners.	TBD – requires scoping of assets from local municipalities for current baseline to be completed under plan requirements 11-15 and Row 1 entry in Appendix B	Metrics data collected by ETSS and League of Cities and Town designees quarterly. Metric % is calculated based on "Metrics" section scoring equation and emailed to SAA (RIEMA) for input to IW and PW Sheets.
Create a statewide culture of digital literacy and cyber awareness through a sustained and equitable education and awareness program.	4.1 Security awareness training, using an equity lens for outreach and curriculum to cover topics most impactful to protection of constituent data and tiered development paths for colleagues with guidance for best practice available to all state and local agencies with their associated partners.	TBD – requires scoping of assets from local municipalities for current baseline to be completed under plan requirements 11-15 and Row 1 entry in Appendix B	Metrics data collected by ETSS and League of Cities and Town designees quarterly. Metric % is calculated based on "Metrics" section scoring equation and emailed to SAA (RIEMA) for input to IW and PW Sheets.
	4.2 Statewide cybersecurity workforce development strategy, with a focus on increasing diversity, especially racial and ethnic diversity, in the workforce	TBD – requires scoping of assets from local municipalities for current baseline to be completed under plan requirements 11-15 and Row 1 entry in Appendix B	Metrics data collected by ETSS and League of Cities and Town designees quarterly. Metric % is calculated based on "Metrics" section scoring equation and emailed to SAA (RIEMA) for input to IW and PW Sheets.
	4.3 Statewide digital literacy training program, in multiple languages with guidance for best practice available to all state and local agencies with their associated partners.	TBD – requires scoping of assets from local municipalities for current baseline to be completed under plan requirements 11-15 and Row 1 entry in Appendix B	Metrics data collected by ETSS and League of Cities and Town designees quarterly. Metric % is calculated based on "Metrics" section scoring equation and emailed to SAA (RIEMA) for input to IW and PW Sheets.

Program Goal	Program Objectives	Associated Metrics (Based on Selected Capability Level in Appendix A)	Metric Description (Details, Source, Frequency)
Mature the cyber hygiene of the state and local municipality technology ecosystems.	5.1 Enhanced Governance, Risk and Compliance capabilities using a unified platform built upon NIST CSF, RMF, and 800-53 controls with guidance for best practice available to all state and local agencies with their associated partners.	TBD – requires scoping of assets from local municipalities for current baseline to be completed under plan requirements 11-15 and Row 1 entry in Appendix B	Metrics data collected by ETSS and League of Cities and Town designees quarterly. Metric % is calculated based on "Metrics" section scoring equation and emailed to SAA (RIEMA) for input to IW and PW Sheets.
	5.2 Statewide Cybersecurity Threat Information Sharing across all municipalities leveraging ETSS, CISA, and MS-ISAC capabilities with guidance for best practice available to all state and local agencies with their associated partners.	TBD – requires scoping of assets from local municipalities for current baseline to be completed under plan requirements 11-15 and Row 1 entry in Appendix B	Metrics data collected by ETSS and League of Cities and Town designees quarterly. Metric % is calculated based on "Metrics" section scoring equation and emailed to SAA (RIEMA) for input to IW and PW Sheets.
	5.3 Improved Cybersecurity Incident response capabilities across all municipalities with a unified reporting plan from local level to state and external agencies as needed with guidance for best practice available to all state and local agencies with their associated partners.	TBD – requires scoping of assets from local municipalities for current baseline to be completed under plan requirements 11-15 and Row 1 entry in Appendix B	Metrics data collected by ETSS and League of Cities and Town designees quarterly. Metric % is calculated based on "Metrics" section scoring equation and emailed to SAA (RIEMA) for input to IW and PW Sheets.

APPENDIX D: ACRONYMS

Acronym	Definition
JCTF	Joint Cyber Task Force – statewide cyber incident response and awareness organization led by the Rhode Island State Police
SLCGP	State and Local Cybersecurity Grant Program
ETSS	Enterprise Technology Strategy and Services – the Rhode Island Executive branch information technology and cybersecurity division
CDO / CIO	Chief Digital Officer / Chief Information Officer – Director of ETSS
CISO	Chief Information Security Officer
CISA	Cybersecurity and Infrastructure Security Agency
SoRI	State of Rhode Island
RIEMA	Rhode Island Emergency Management Agency
C-SCRM	Cyber Supply Chain Risk Management
CIKR	Critical Infrastructure and Key Resources
NIST	National Institute of Standards and Technology
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework
NIST RMF	National Institute of Standards and Technology Risk Management Framework
BOD	Binding Operational Directives
H.R. 3138	H.R.3138 - State and Local Cybersecurity Improvement Act
CPG	Cyber Performance Goals
RICSP	Rhode Island Cybersecurity Plan
SIEM	Security Incident and Event Monitoring
SOC	Security Operations Center
FIPS 140-2	Federal Information Processing Standard 140 -2
EOS	End of Service
RPO	Recovery Point Objective
RTO	Recovery Time Objective
BCDR	Business Continuity and Disaster Recovery
EOL	End of Life

Acronym	Definition
ITSM	Information Technology Service Management
GPOs	Group Policy Objects
FEMA	Federal Emergency Management Agency
CoE	Center of Excellence
IAM	Identity and Access Management
FTI	Federal Tax Information
PII	Personally Identifiable Information
PHI	Personal Health Information
NOFO	Notice of Funding Opportunity
IJ	Grant Investment Justification Form
PW	Grant Project Worksheet Form
SAA	State Administrative Agency