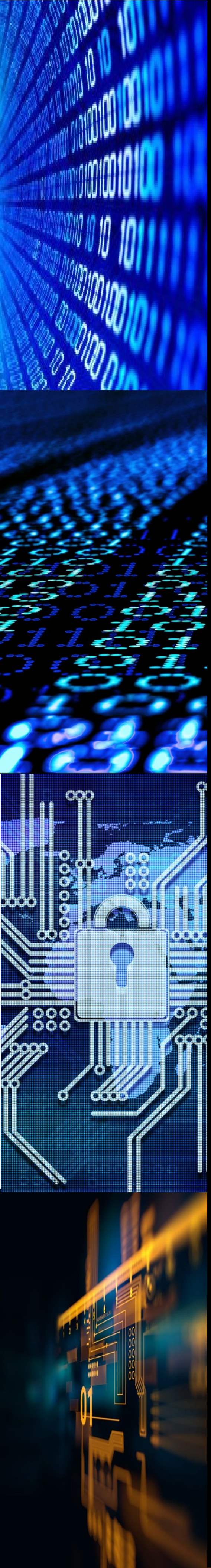


COMMONWEALTH OF PUERTO RICO CYBERSECURITY PLAN

Sensitive/confidential information removed for security purposes.

September 2023

Approved by Puerto Rico Innovation and Technology Service (PRITS) and the Puerto Rico Cybersecurity Planning Committee on September 26, 2023
Version 1.0

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

TABLE OF CONTENTS 2
Letter from the Cybersecurity Planning Committee 4
Introduction 5
Vision and Mission 7
Cybersecurity Program Goals and Objectives 7
Cybersecurity Plan Elements 16
Manage, Monitor, and Track 17
Monitor, Audit, and Track 17
Enhance Preparedness 18
Assessment and Mitigation 19
Best Practices and Methodologies 19
Safe Online Services 21
Continuity of Operations 21
Workforce 22
Continuity of Communications and Data Networks 23
Protect Critical Infrastructure and Key Resources 23
Cyber Threat Indicator Information Sharing 24
Leverage CISA Services 24
Information Technology and Operational Technology Modernization Review 25
Cybersecurity Risk and Threat Strategies 25
Rural Communities 26
Distribution to Local Governments 26
Funding and Services 26
Assess Capabilities 27
Implementation Plan 27
Organization Roles and Responsibilities 28
Feedback From Municipalities 29
Resource Overview and Timeline Summary 30
Metrics 31
Appendix A: Cybersecurity Plan Capabilities Assessment 32
Appendix B: Project Summary Worksheet 39
Appendix C: ENTITY METRICS 42
Appendix D: Acronyms 50

LIST OF TABLES

Table 1 Cybersecurity Program Goals & Objectives 9
Table 2 Cybersecurity Program Goals & Objectives by SLCGP Required Elements Summary Matrix 10
Table 3 Individual Action Items supporting Cybersecurity Program Goals & Objectives 15
Table 4 FY 2022 SLCGP Funding 26
Table 5 Required Element-based Capabilities Assessment Questions 32
Table 6 Capabilities Assessment Results 34
Table 7 Project Summary Worksheet 39
Table 8 Entity Metrics 42
Table 9 Acronyms 50

LIST OF FIGURES

Figure 1 Achieving cyber resilience through comprehensive cybersecurity planning 6
Figure 2 Summary of the sixteen required cybersecurity elements 16
Figure 3 Capabilities Assessment process 27
Figure 4 Structure of the PR SLCGP Cybersecurity Planning Committee 28
Figure 5 Collaboration between the PR SLCGP Cybersecurity Planning Committee, PRITS & SAA, and other entities 29
Figure 6 Feedback cycle for the Cybersecurity Plan 29
Figure 7 Puerto Rico Municipalities responding to the Capabilities Assessment 29

LETTER FROM THE CYBERSECURITY PLANNING COMMITTEE

Greetings,

The Puerto Rico Cybersecurity Planning Committee is pleased to present the 2023 Commonwealth of Puerto Rico Cybersecurity Plan. The Cybersecurity Plan represents Puerto Rico's continued commitment to improving cybersecurity and supporting our Commonwealth, as well as cybersecurity practitioners across our municipalities. In addition, this Cybersecurity Plan meets the requirement of the current U.S. Department of Homeland Security (DHS) guidelines for the State and Local Cybersecurity Grant Program (SLCGP).

Representatives from the Commonwealth of Puerto Rico collaborated with the Cybersecurity Planning Committee to develop and update the Cybersecurity Plan with actionable and measurable goals and objectives to ensure completion. These goals and objectives focus on fostering and increasing collaboration between the Government of Puerto Rico (GPR) and the municipalities, to mature cybersecurity practices across Puerto Rico and strengthen our cybersecurity posture using sustainable and scalable solutions. They are designed to support the Commonwealth of Puerto Rico in planning for new technologies, navigating the ever-changing cybersecurity landscape, and incorporating the SLCGP required plan elements.

As we continue our efforts, we must remain dedicated to improving our cybersecurity resilience across jurisdictional boundaries. With help from practitioners at GPR and the municipalities, we will work to achieve the goals set forth in the Cybersecurity Plan and become a model for other states and territories.

Sincerely,

Antonio Ramos Guardiola
Chief Technology Officer and Puerto Rico Planning Committee Chair
Government of Puerto Rico

INTRODUCTION

The Cybersecurity Plan is a two-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 two years.
- **Organization, Roles, and Responsibilities:** Describes the current roles and responsibilities, and any governance mechanisms for cybersecurity within the Commonwealth of Puerto Rico 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 the requirements of the Commonwealth of Puerto Rico's cybersecurity program. The Cybersecurity Plan is a guiding document and does not create any authority or direction over the Commonwealth of Puerto Rico, GPR agencies, or municipalities.
- **How feedback and input from local governments and associations was incorporated:** Describes how inputs from local governments (i.e., municipalities) are 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 the Commonwealth of Puerto Rico, along with methods and strategies for funding sustainment and enhancement to meet long-term goals.
- **Implementation Plan:** Describes the Commonwealth of Puerto Rico'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 the Commonwealth of Puerto Rico will measure the outputs and outcomes of the program across the entity.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)[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.

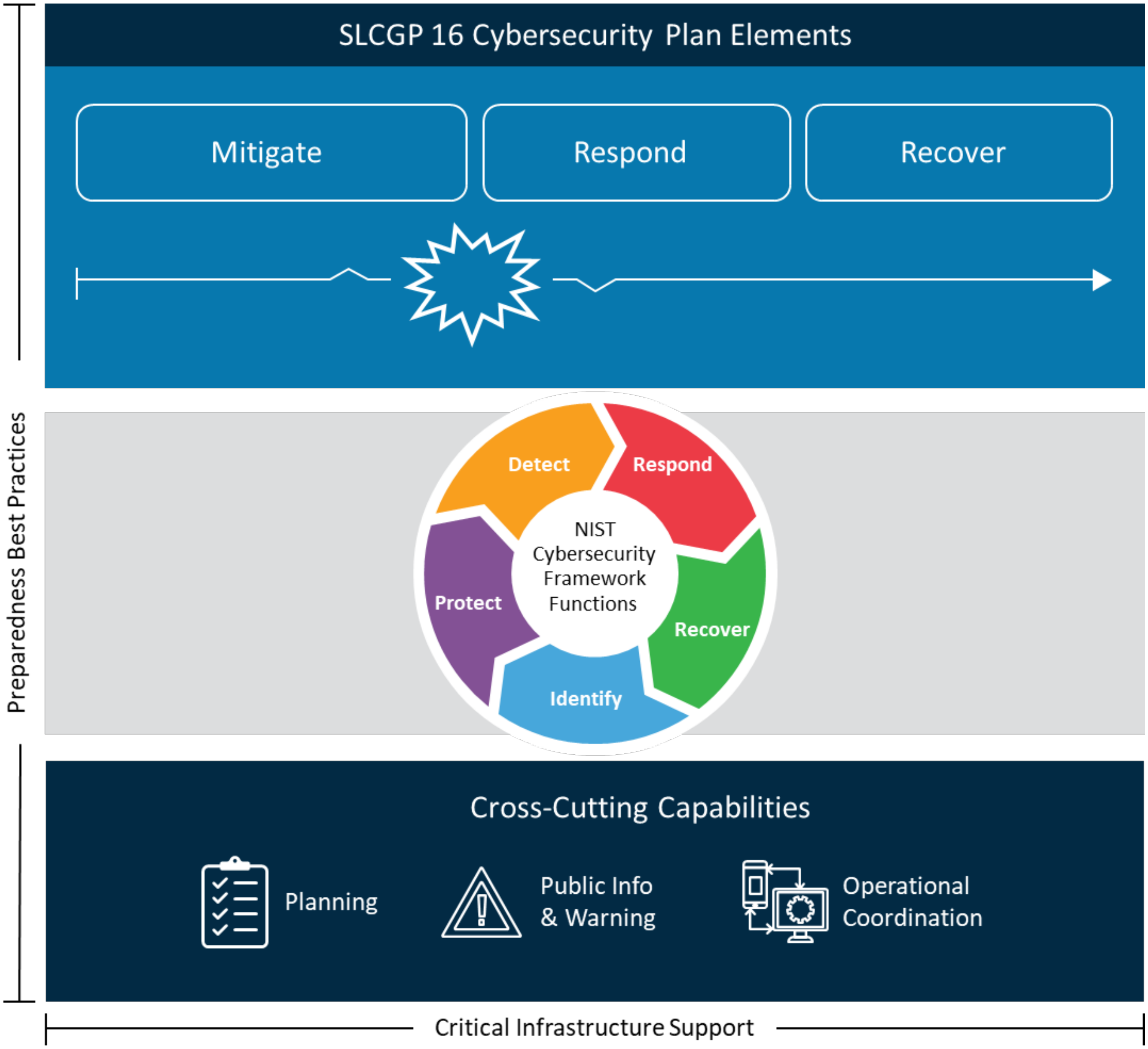

SLCGP 16 Cybersecurity Plan Elements
Mitigate
Respond
Recover
Preparedness Best Practices
Detect
Respond
NIST Cybersecurity Framework Functions
Protect
Recover
Identify
Cross-Cutting Capabilities
Planning
Public Info & Warning
Operational Coordination
Critical Infrastructure Support

Figure 1 Achieving cyber resilience through comprehensive cybersecurity planning

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

Vision and Mission

This section describes the Commonwealth of Puerto Rico's vision and mission for improving cybersecurity:

Vision:

Establish a robust, dynamic, and resilient cybersecurity environment, safeguarding both the infrastructure and systems of the Commonwealth of Puerto Rico and the personal data of its citizens, while promoting economic growth and societal progress.

Mission:

To proactively design, implement, and maintain cutting-edge cybersecurity measures that prioritize the protection of the Commonwealth of Puerto Rico's infrastructure and its citizens' data. Through collaboration, continuous learning, and innovation, we aim to foster a secure digital landscape that bolsters economic and social prosperity, fully capitalizing on emerging technologies as an engine for progress.

Cybersecurity Program Goals and Objectives

The Cybersecurity Planning Committee has defined long-term goals to support and implement the Cybersecurity Plan, address identified cybersecurity gaps, and improve the cybersecurity posture across all branches of the Commonwealth of Puerto Rico. Each of the five (5) goals and their supporting objectives aligns to one (1) or more of the required, applicable cybersecurity plan elements outlined in the SLCGP Notice of Funding Opportunity (NOFO) and described in the next section. The Planning Committee utilized a strategic approach in collaboration with PRITS, other GPR agencies, and local jurisdictions (i.e., the municipalities) and considered the results of the Capabilities Assessment to further refine the goals and objectives of the Cybersecurity Plan. The following table outlines the Cybersecurity Plan's goals and associated objectives, which will guide the selection of cybersecurity investment projects and activities. (One or more SLCGP Required Elements that directly align to a cybersecurity program objective are also specifically noted next to that objective.)

Commonwealth of Puerto Rico Cybersecurity Program Goals & Objectives		
Goals	**Objectives**	
Goal 1 – Establish centralized cybersecurity governance, policies & standards, and recommended baselines for cybersecurity and resilience across Puerto Rico.	1.1	Continue, enhance, and expand the Cybersecurity Planning Committee to involve and meet the cybersecurity needs of an increasing number of stakeholders. *(SLCGP Required Elements 14 & 15)*
	1.2	Develop and promulgate a cybersecurity framework based on industry leading practices, such as the NIST CSF. *(SLCGP Required Elements 5 & 14)*

Commonwealth of Puerto Rico Cybersecurity Program Goals & Objectives

Goals	Objectives
	1.3 Develop, test, and enhance cyber incident response and business continuity plans, processes, and procedures. *(SLCGP Required Elements 3, 5, 7 & 9)*
Goal 2 – Understand cybersecurity posture and continually assess risk to entities across Puerto Rico.	2.1. Perform continual, comprehensive, and periodic (e.g., annual) cyber risk assessments. *(SLCGP Required Elements 10 & 14)*
	2.2. Maintain complete inventories of IT and operational technology (OT) hardware and software owned or operated by or on behalf of government entities. *(SLCGP Required Element 1)*
	2.3. Continually assess government entities' cybersecurity maturity and identify areas for enhancement. *(SLCGP Required Elements 4 & 10)*
	2.4. Obtain CISA Cyber Hygiene assessments across external government networks and web applications. *(SLCGP Required Elements 4 & 12)*
	2.5. Perform recurring vulnerability scans of internal and external networks, systems, and applications. *(SLCGP Required Elements 4)*
Goal 3 – Protect citizen data, secure digital public services, and enhance the resilience of critical infrastructure throughout Puerto Rico.	3.1. Migrate all remaining and appropriate government domains to the .gov Internet domain. *(SLCGP Required Elements 5 & 6)*
	3.2. Upgrade or replace outdated, end-of-life, and unsupported software. *(SLCGP Required Elements 1, 5 & 13)*
	3.3. Establish effective software patch management processes. *(SLCGP Required Elements 1 & 4)*
	3.4. Implement architectural measures and controls to protect data at rest and in transit from unauthorized access and use. *(SLCGP Required Element 5)*
	3.5. Enhance identity and access management, particularly for administrative and other privileged accounts. 3.5.1. Implement strong password policies and controls. 3.5.2. Require Multi-Factor Authentication (MFA) for public services and government accounts. *(SLCGP Required Elements 5 & 6)*
	3.6. Implement and enhance system and network logging and monitoring capabilities. *(SLCGP Required Elements 2 & 5)*
Goal 4 – Cultivate Puerto Rico's government cybersecurity workforce through education, training, and partnerships.	4.1. Adopt and leverage the NICE Framework (i.e., Workforce Framework for Cybersecurity) to build and enhance cyber workforce development, training, and retention programs. *(SLCGP Required Element 8)*
	4.2. Continually deliver cybersecurity awareness training to all government personnel, including simulated phishing

Commonwealth of Puerto Rico Cybersecurity Program Goals & Objectives	
Goals	**Objectives**
	campaigns targeting specific users. *(SLCGP Required Element 8)*
	4.3. Develop and provide specialized, role- and skills-based cybersecurity training for cyber, IT, and OT teams. *(SLCGP Required Element 8)*
	4.4. Establish a cybersecurity mentorship program between students and cyber & IT professionals. *(SLCGP Required Element 8)*
Goal 5 – Promote a secure cyberculture throughout Puerto Rico.	5.1. Develop and launch cyber awareness and education initiatives for businesses, educational institutions, and citizens. *(SLCGP Required Element 8)*
	5.2. Establish and enhance public-private partnerships aimed at improving cybersecurity across Puerto Rico. *(SLCGP Required Elements 11, 12 & 14)*

Table 1 Cybersecurity Program Goals & Objectives

The following table provides a summary matrix of Cybersecurity Program Goals and Objectives by the associated SLCGP Required Elements addressed.

		REQUIRED ELEMENTS BEING ADDRESSED															
Goal	**Objective**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16***
1 – *Establish centralized cybersecurity governance, policies & standards, and recommended baselines for cybersecurity and resilience across Puerto Rico.*	1.1														■	■	▨
	1.2					■									■		▨
	1.3			■		■		■		■							▨
2 – *Understand cybersecurity posture and continually assess risk to entities across Puerto Rico.*	2.1										■				■		▨
	2.2	■															▨
	2.3				■						■						▨
	2.4				■								■				▨
	2.5				■												▨
3 – *Protect citizen data, secure digital public services, and enhance the resilience of critical infrastructure throughout Puerto Rico.*	3.1					■	■										▨
	3.2	■				■								■			▨
	3.3	■			■												▨
	3.4					■											▨
	3.5					■	■										▨
	3.6		■			■											▨
4 – *Cultivate Puerto Rico's government cybersecurity workforce through education, training, and partnerships.*	4.1								■								▨
	4.2								■								▨
	4.3								■								▨

		REQUIRED ELEMENTS BEING ADDRESSED															
Goal	**Objective**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16***
	4.4								■								▨
5 – *Promote a secure cyberculture throughout Puerto Rico.*	5.1								■								▨
	5.2											■	■		■		▨
		**As documented in the FY 2022 SLCGP NOFO, the Commonwealth of Puerto Rico is exempted from the minimum 80% local govt. (and min. 25% rural area) pass-through requirement; therefore, required element # 16 also does not apply to Puerto Rico.*															

Table 2 Cybersecurity Program Goals & Objectives by SLCGP Required Elements Summary Matrix

To achieve Puerto Rico's cybersecurity program goals and objectives, a comprehensive set of more tactical and operational action items aligned to each objective are required. Such action items specifically identify and briefly describe the activities to be performed and that work in combination to accomplish each associated objective. Table 3 below provides the entire portfolio of action items for each objective that ultimately roll up to each of the five (5) cybersecurity program goals. These action items will be overseen by the Planning Committee, with management and implementation support provided by PRITS, other GPR agencies, the municipalities, and other stakeholders.

Action Items Supporting Cybersecurity Program Goals & Objectives		
Goals	**Objectives**	**Action Items**
Goal 1 – Establish centralized cybersecurity governance, policies & standards, and recommended baselines for cybersecurity and resilience across Puerto Rico.	1.1 Continue, enhance, and expand the Cybersecurity Planning Committee to involve and meet the cybersecurity needs of an increasing number of stakeholders.	▪ Continue to support and update the Planning Committee on SLCGP projects and other government cybersecurity initiatives. ▪ Expand the Planning Committee to include additional agency and municipal members. ▪ Build and launch focused sub-committees, as needed.
	1.2 Develop and promulgate a cybersecurity framework based on industry leading practices, such as the NIST CSF.	▪ Map policies, procedures, and controls with the NIST CSF to ensure alignment of current policies and standards with industry leading guidance. ▪ Address identified gaps through projects and initiatives. ▪ Provide training on NIST CSF implementation.
	1.3 Develop, test, and enhance cyber incident response and business continuity plans, processes, and procedures.	▪ Identify government entities with existing cyber incident response plans, business continuity plans, IT disaster recovery plans, and standard recovery processes. ▪ Establish a standardized reporting format for entities to submit information on their plans and processes. ▪ Create a repository to document existing plans and processes. ▪ Identify gaps or deficiencies in existing plans or processes.

Action Items Supporting Cybersecurity Program Goals & Objectives		
Goals	**Objectives**	**Action Items**
		▪ Assist government entities in developing new or enhancing existing cyber incident response plans, business continuity plans, IT disaster recovery plans, etc. ▪ Coordinate and facilitate incident response and recovery exercises (e.g., tabletop testing, simulation, fail-over, data backups) with government entities, as well as suppliers, third-party providers, and other stakeholders. ▪ Update cyber incident response plans, business continuity plans, IT disaster recovery plans, etc., based on results and lessons learned from incident response and recovery exercises
Goal 2 – Understand cybersecurity posture and continually assess risk to entities across Puerto Rico.	2.1 Perform continual, comprehensive, and periodic (e.g., annual) cyber risk assessments.	▪ Conduct risk scanning across systems and infrastructure. ▪ Categorize risks based on criticality and exploitability. ▪ Prioritize remediation efforts based on potential business impact.
	2.2 Maintain complete inventories of IT and operational technology (OT) hardware and software owned or operated by or on behalf of government entities.	▪ Deploy automated discovery tools and configuration management database. ▪ Establish procedures for maintaining accurate hardware and software inventories during changes. ▪ Integrate asset hardware and software inventories into the vulnerability management program.
	2.3 Continually assess government entities' cybersecurity maturity and identify areas for enhancement.	▪ Collaborate with government entities to evaluate their cybersecurity maturity levels. ▪ Identify and prioritize capability gaps requiring improvement. ▪ Develop strategic roadmaps to enhance cybersecurity maturity.
	2.4 Obtain CISA Cyber Hygiene assessments across external government networks and web applications.	▪ Onboard government entities for applicable CISA cyber assessment services. ▪ Develop and implement procedures to remediate identified vulnerabilities and weaknesses. ▪ Track improvements to security posture over time.
	2.5 Perform recurring vulnerability scans of internal and external networks, systems, and applications.	▪ Utilize CISA Cyber Hygiene scanning services for public-facing systems and to complement government entities' own vulnerability scanning.

Action Items Supporting Cybersecurity Program Goals & Objectives		
Goals	**Objectives**	**Action Items**
		▪ Prioritize remediation efforts based on risk level.
Goal 3 – Protect citizen data, secure digital public services, and enhance the resilience of critical infrastructure throughout Puerto Rico.	3.1 Migrate all remaining and appropriate government domains to the .gov Internet domain.	▪ Inventory existing government websites, web applications, and online content operating outside the .gov domain. ▪ Educate on the benefits of transitioning to the .gov domain. ▪ Encourage and support government entities in developing a transition plan to the .gov domain and provide support throughout the process. ▪ Assist in submitting .gov domain requests for eligible services, creating a deployment schedule and migration process. ▪ Incentivize entities that have transitioned to the .gov domain by providing additional support to enhance their cybersecurity posture.
	3.2 Upgrade or replace outdated, end-of-life, and unsupported software.	▪ Ensure end-of-life (EOL) status is captured in hardware and software inventories and ensure security tools can identify EOL h/w and s/w. ▪ Develop a phased plan to upgrade or replace outdated technology. ▪ Mitigate vulnerabilities and implement compensating controls associated with unsupported but unreplaceable systems.
	3.3 Establish effective software patch management processes.	▪ Ensure patch status is captured in software inventory. ▪ Establish patch management policies and procedures. ▪ Implement patch management tools. ▪ Standardize patch testing, validation, deployment, and monitoring processes.
	3.4 Implement architectural measures and controls to protect data at rest and in transit from unauthorized access and use.	▪ Identify and classify all data requiring protection. ▪ Encrypt data at rest, in transit, and in non-production (e.g., test) environments using robust encryption methods. ▪ Ensure compliance with encryption standards and protocols. ▪ Implement encryption or masking solutions and associated staff training. ▪ Establish an immutable backup infrastructure to ensure data integrity and rapid recovery of critical data.

Action Items Supporting Cybersecurity Program Goals & Objectives		
Goals	**Objectives**	**Action Items**
	3.5 Enhance identity and access management, particularly for administrative and other privileged accounts. 3.5.1. Implement strong password policies and controls. 3.5.2. Require Multi-Factor Authentication (MFA) for public services and government accounts.	▪ Update policies to mandate password complexity and expiration standards. ▪ Configure and test password complexity protocols in a controlled environment to ensure compatibility and operability. ▪ Implement phased roll-out of enhanced password controls, starting with critical systems. ▪ Use monitoring tools to track and report password-related events, such as password changes or account lockouts. ▪ Explore new authentication methods (e.g., federation/single sign-on) for citizen-facing applications. ▪ Inventory public services and government accounts. ▪ Integrate MFA across systems, starting with critical applications. ▪ Update policies to expand MFA requirements beyond administrators. ▪ Educate users on MFA importance and proper usage.
	3.6 Implement and enhance system and network logging and monitoring capabilities.	▪ Deploy enhanced logging, Security Information and Event Management (SIEM), and analytics tools. ▪ Develop alerts and use cases tailored to system and network environments. ▪ Perform daily reviews of system and network events for anomalies. ▪ Define and document incident response procedures based on system and network alerts and associated analysis.
Goal 4 – Cultivate Puerto Rico's government cybersecurity workforce through education, training, and partnerships.	4.1 Adopt and leverage the NICE Framework (i.e., Workforce Framework for Cybersecurity) to build and enhance cyber workforce development, training, and retention programs.	▪ Engage with and establish a partnership with NICE Framework leadership at NIST. ▪ Develop and provide education and training on the NICE Framework to GPR agencies and municipalities. ▪ Leverage the NICE Framework to develop tailored work roles for adopting organizations, as well as associated knowledge and skill statements for those roles.
	4.2 Continually deliver cybersecurity awareness training to all government personnel, including simulated	▪ Identify workforce cybersecurity knowledge gaps.

Action Items Supporting Cybersecurity Program Goals & Objectives		
Goals	**Objectives**	**Action Items**
	phishing campaigns targeting specific users.	▪ Develop a tailored cybersecurity awareness curriculum. - Schedule training via in-person and online platforms. - Incorporate real-world examples and case studies into training. - Monitor progress and completion of training through a learning management system. ▪ Assess awareness training effectiveness through quizzes, surveys, and/or feedback. ▪ Develop phishing training templates mimicking common attacks. - Target users across roles to evaluate susceptibility to phishing. - Provide additional cybersecurity awareness training to users susceptible to phishing.
	4.3 Develop and provide specialized, role- and skills-based cybersecurity training for cyber, IT, and OT teams.	▪ Identify cybersecurity knowledge and skill requirements for specific roles within cyber, IT, and OT teams using the NICE Framework. ▪ Develop cybersecurity training aligned with roles and responsibilities. ▪ Provide specialized and hands-on training and simulations. ▪ Encourage continuous learning and professional development. ▪ Evaluate training effectiveness through assessments, practical exercises, and feedback.
	4.4 Establish a cybersecurity mentorship program between students and cyber & IT professionals.	▪ Define clear objectives and expectations for the mentorship program. ▪ Establish partnerships with educational institutions to identify students interested in cybersecurity careers. ▪ Pair students with experienced cyber & IT professionals. ▪ Encourage regular meetings and knowledge transfer between cyber & IT professionals and students. ▪ Provide mentees with hands-on exposure and experience with real-world cybersecurity challenges. ▪ Evaluate the success of the mentorship program.

Action Items Supporting Cybersecurity Program Goals & Objectives		
Goals	**Objectives**	**Action Items**
Goal 5 – Promote a secure cyberculture throughout Puerto Rico.	5.1 Develop and launch cyber awareness and education initiatives for businesses, educational institutions, and citizens.	▪ Identify target audiences, including higher education, the private sector, and the public. ▪ Develop tailored curricula and education & training materials. ▪ Establish delivery mechanisms (e.g., in-person sessions, webinars, online courses, awareness campaigns). ▪ Assess the effectiveness of initiatives through quizzes, surveys, and/or feedback.
	5.2 Establish and enhance public-private partnerships aimed at improving cybersecurity across Puerto Rico.	▪ Identify potential partners in the federal government, state & local government, industry, and academia. ▪ Establish formal partnerships and information-sharing agreements. ▪ Regularly engage in sharing cybersecurity knowledge, expertise, best practices, threat indicators, and lessons learned. ▪ Participate in joint exercises and drills to improve cyber incident response capabilities. ▪ Develop a cybersecurity communications plan for Puerto Rico. ▪ Disseminate cybersecurity policies, guidelines, and best practices. ▪ Encourage prompt reporting of cybersecurity incidents and concerns. ▪ Foster a culture of continuous cybersecurity learning and improvement. ▪ Engage organizations in promoting cybersecurity as a business priority.

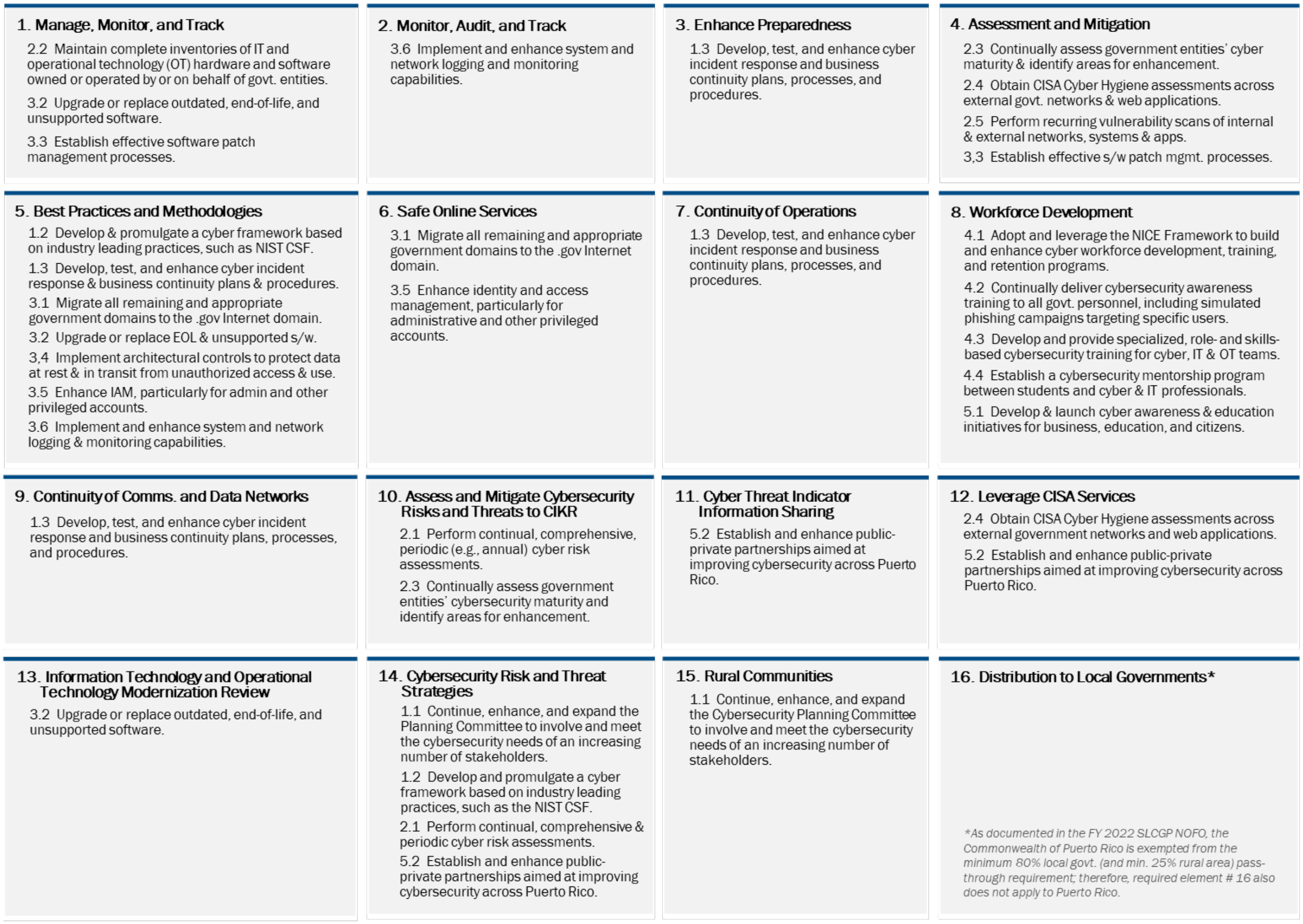
Table 3 Individual Action Items supporting Cybersecurity Program Goals & Objectives

CYBERSECURITY PLAN ELEMENTS

This section describes Puerto Rico's existing capabilities, as applicable, for meeting each of the sixteen (16) required cybersecurity elements. Further, the Cybersecurity Planning Committee's strategic approach towards assisting entities (e.g., GPR agencies, municipalities) in implementing and/or addressing existing gaps in meeting the required elements is also addressed in this section of the Plan.

The implementation approach for each cybersecurity element is designed to align with leading practices such as the NIST CSF and the Cybersecurity and Infrastructure Security Agency's (CISA) Cross-Sector Cybersecurity Performance Goals (CPGs). Each of the required elements is also supported by one or more associated program objectives (except for required element # 16 for which, as described further below, Puerto Rico is exempted in the SLCGP NOFO).

The cybersecurity program objectives are intended to guide future cyber investments and projects aimed at helping entities across Puerto Rico implement a corresponding required element(s). The following graphic (Figure 2) summarizes each of the sixteen required cybersecurity elements and associated program objectives for achieving intended outcomes. (This diagram essentially provides the inverse view as that presented in Table 1 and further demonstrates the strong interconnection and mutually supportive nature between the cybersecurity program goals and objectives and the required elements.)



1. Manage, Monitor, and Track

2.2 Maintain complete inventories of IT and operational technology (OT) hardware and software owned or operated by or on behalf of govt. entities.

3.2 Upgrade or replace outdated, end-of-life, and unsupported software.

3.3 Establish effective software patch management processes.

2. Monitor, Audit, and Track

3.6 Implement and enhance system and network logging and monitoring capabilities.

3. Enhance Preparedness

1.3 Develop, test, and enhance cyber incident response and business continuity plans, processes, and procedures.

4. Assessment and Mitigation

2.3 Continually assess government entities' cyber maturity & identify areas for enhancement.

2.4 Obtain CISA Cyber Hygiene assessments across external govt. networks & web applications.

2.5 Perform recurring vulnerability scans of internal & external networks, systems & apps.

3,3 Establish effective s/w patch mgmt. processes.

5. Best Practices and Methodologies

1.2 Develop & promulgate a cyber framework based on industry leading practices, such as NIST CSF.

1.3 Develop, test, and enhance cyber incident response & business continuity plans & procedures.

3.1 Migrate all remaining and appropriate government domains to the .gov Internet domain.

3.2 Upgrade or replace EOL & unsupported s/w.

3,4 Implement architectural controls to protect data at rest & in transit from unauthorized access & use.

3.5 Enhance IAM, particularly for admin and other privileged accounts.

3.6 Implement and enhance system and network logging & monitoring capabilities.

6. Safe Online Services

3.1 Migrate all remaining and appropriate government domains to the .gov Internet domain.

3.5 Enhance identity and access management, particularly for administrative and other privileged accounts.

7. Continuity of Operations

1.3 Develop, test, and enhance cyber incident response and business continuity plans, processes, and procedures.

8. Workforce Development

4.1 Adopt and leverage the NICE Framework to build and enhance cyber workforce development, training, and retention programs.

4.2 Continually deliver cybersecurity awareness training to all govt. personnel, including simulated phishing campaigns targeting specific users.

4.3 Develop and provide specialized, role- and skills-based cybersecurity training for cyber, IT & OT teams.

4.4 Establish a cybersecurity mentorship program between students and cyber & IT professionals.

5.1 Develop & launch cyber awareness & education initiatives for business, education, and citizens.

9. Continuity of Comms. and Data Networks

1.3 Develop, test, and enhance cyber incident response and business continuity plans, processes, and procedures.

10. Assess and Mitigate Cybersecurity Risks and Threats to CIKR

2.1 Perform continual, comprehensive, periodic (e.g., annual) cyber risk assessments.

2.3 Continually assess government entities' cybersecurity maturity and identify areas for enhancement.

11. Cyber Threat Indicator Information Sharing

5.2 Establish and enhance public-private partnerships aimed at improving cybersecurity across Puerto Rico.

12. Leverage CISA Services

2.4 Obtain CISA Cyber Hygiene assessments across external government networks and web applications.

5.2 Establish and enhance public-private partnerships aimed at improving cybersecurity across Puerto Rico.

13. Information Technology and Operational Technology Modernization Review

3.2 Upgrade or replace outdated, end-of-life, and unsupported software.

14. Cybersecurity Risk and Threat Strategies

1.1 Continue, enhance, and expand the Planning Committee to involve and meet the cybersecurity needs of an increasing number of stakeholders.

1.2 Develop and promulgate a cyber framework based on industry leading practices, such as the NIST CSF.

2.1 Perform continual, comprehensive & periodic cyber risk assessments.

5.2 Establish and enhance public-private partnerships aimed at improving cybersecurity across Puerto Rico.

15. Rural Communities

1.1 Continue, enhance, and expand the Cybersecurity Planning Committee to involve and meet the cybersecurity needs of an increasing number of stakeholders.

16. Distribution to Local Governments*

**As documented in the FY 2022 SLCGP NOFO, the Commonwealth of Puerto Rico is exempted from the minimum 80% local govt. (and min. 25% rural area) pass-through requirement; therefore, required element # 16 also does not apply to Puerto Rico.*

Figure 2 Summary of the sixteen required cybersecurity elements

Manage, Monitor, and Track

Required Element #1

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

The Government of Puerto Rico, through PRITS, recently started implementing an Endpoint Detection and Response (EDR) service in partnership with the .
This EDR initiative aims to monitor, protect, and manage GPR agencies' user devices and servers. It is a comprehensive solution for all GPR agencies, tailored to existing cyber risks and the need to safeguard government endpoints' confidentiality, integrity, and availability.

The endpoint monitoring and management services include 24/7/365 monitoring of GPR devices by the Security Operations Center (SOC) in New York State. This monitoring service complements the PRITS SOC's existing monitoring coverage as follows:

- PRITS SOC: (working hours)
- SOC: 24x7

The Cybersecurity Planning Committee will coordinate with GPR/PRITS to define and establish standards for government entities to manage, monitor, track, and approve assets (applications and systems) and user accounts. In addition, the Committee will seek to invest in solutions or tools to assist entities with managing assets throughout their lifecycle.

The following cybersecurity program objectives align with and support the accomplishment of this SLCGP required element:

- Program Objective 2.2: Maintain complete inventories of IT and operational technology (OT) hardware and software owned or operated by or on behalf of government entities.
- Program Objective 3.2: Upgrade or replace outdated, end-of-life, and unsupported software.
- Program Objective 3.3: Establish effective software patch management processes.

Alignment to Leading Practices:

CPG:

- *1.5 Separating User and Privilege Accounts*
- *1.7 Revoking Credentials for Departing Employees*
- *2.1 Hardware and Software Approval Process*
- *2.3 Asset Inventory*

NIST CSF:

- *ID.AM-1*
- *ID.AM-2*
- *PR.AC-4*

Monitor, Audit, and Track

Required Element #2

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

PRITS has implemented several cybersecurity projects aimed at centralizing, streamlining, and monitoring cybersecurity alerts for critical networks and systems of the Government of Puerto Rico. One of these projects was the construction and implementation of the Puerto Rico Cyber Command Center (PRC3), which includes the PRITS SOC.

Leading practices will be leveraged to enable government entities to standardize monitoring capabilities to detect potential cyber threats and events. Network and user monitoring capabilities will be enhanced to allow government entities to holistically understand threats within their networks.

The following cybersecurity program objective aligns with and supports the accomplishment of this SLCGP required element:

- Program Objective 3.6: Implement and enhance system and network logging and monitoring capabilities.

Alignment to Leading Practices:

CPG:

- *8.2 Detecting Relevant Threats and TTPs*

NIST CSF:

- *DE.CM-1*
- *DE.CM-3*

Enhance Preparedness

Required Element #3

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

The PRC3's PRITS SOC was constructed and implemented with the vision to eventually serve as the one-stop-shop for performing 24/7/365 threat monitoring, cybersecurity risk assessments, incident response (IR), intelligence sharing, and vulnerability scanning.

The following cybersecurity program objective aligns with and supports the accomplishment of this SLCGP required element:

- Program Objective 1.3: Develop, test, and enhance cyber incident response and business continuity plans, processes, and procedures.

Alignment to Leading Practices:

***CPG*:**

- *6.2 Supply Chain Incident Reporting*
- *7.2 Incident Response (IR) Plans*

NIST CSF:

- *PR.IP-7*
- *PR.IP-9*
- *PR.IP-10*

Assessment and Mitigation

Required Element #4

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

The Cybersecurity Planning Committee will establish a vulnerability management and threat mitigation framework to provide entities (e.g., GPR agencies and municipalities) with guidelines based on leading practices. Additionally, the Planning Committee will oversee the adoption of required CISA Cyber Hygiene services.

The following cybersecurity program objectives align with and support the accomplishment of this SLCGP required element:

- Program Objective 2.3: Continually assess government entities' cybersecurity maturity and identify areas for enhancement.
- Program Objective 2.4: Obtain CISA Cyber Hygiene assessments across external government networks and web applications.
- Program Objective 2.5: Perform recurring vulnerability scans of internal and external networks, systems, and applications.
- Program Objective 3.3: Establish effective software patch management processes.

Alignment to Leading Practices:

CPG:

- *5.1 Mitigating Known Vulnerabilities*
- *6.3 Supply Chain Vulnerability Disclosure*

NIST CSF:

- *DE.CM-8*
- *ID.RA-1*
- *RS.MI-2*
- *RS.MI-3*

Best Practices and Methodologies

Required Element #5

Ensure that the state or local governments within the state adopt and use best practices and methodologies to enhance cybersecurity, discussed further below. The following cybersecurity best practices under required element 5 must be included in each eligible entity's Cybersecurity Plan:

- *Implement multi-factor authentication.*
- *Implement enhanced logging.*
- *Data encryption for data at rest and in transit.*
- *End use of unsupported/end-of-life software and hardware that are accessible from the Internet.*
- *Prohibit the use of known/fixed/default passwords and credentials.*
- *Ensure the ability to reconstitute systems (backups).*
- *Migration to the .gov internet domain.*

PRITS established the *Standards for Cybersecurity V1.2* for GPR agencies. By virtue of Law 75-2019, these policies and standards apply to all executive branch agencies and their employees that use or access any information technology resource of the GPR. . Currently, municipalities are not subject to these policies and standards. The Standards for Cybersecurity V1.2 require:

- MFA for:

- Data encryption:
    - Necessary controls (e.g., encryption) must be implemented to ensure the confidentiality of sensitive data at rest and in transit on unsecured networks (e.g., Internet, wireless networks).
    - Remote connections to the GPR network must only be made through a virtual private network (VPN) for any official use and when work-related tasks are required.
    - Confidential information (e.g., PHI, PII) must not be left exposed or unprotected under any circumstances. It must be encrypted in all its states (e.g., in transit and at rest).
- Passwords:

Leading cybersecurity practices and methodologies, such as those recommended by the NIST CSF and CISA CPGs, will be adopted to standardize cybersecurity capabilities, enhance cybersecurity posture across Puerto Rico, and manage and protect the IT assets and infrastructure of all entities (e.g., GPR agencies, municipalities).

The following cybersecurity program objectives align with and support the accomplishment of this SLCGP required element:

- Program Objective 1.2: Develop and promulgate a cybersecurity framework based on industry leading practices, such as the NIST CSF.
- Program Objective 1.3: Develop, test, and enhance cyber incident response and business continuity plans, processes, and procedures.
- Program Objective 3.1: Migrate all remaining and appropriate government domains to the .gov Internet domain.
- Program Objective 3.2: Upgrade or replace outdated, end-of-life, and unsupported software.
- Program Objective 3.4: Implement architectural measures and controls to protect data at rest and in transit from unauthorized access and use.
- Program Objective 3.5: Enhance identity and access management, particularly for administrative and other privileged accounts.
    - Sub-Objective 3.5.1. Implement strong password policy and controls.
    - Sub-Objective 3.5.2. Require Multi-Factor Authentication (MFA) for public services and government accounts.

Alignment to Leading Practices:

CPG:

- *1.2 Changing Default Passwords*
- *1.3 Multi-Factor Authentication (MFA)*
- *1.4 Minimum Password Strength*
- *1.6 Unique Credentials*
- *3.1 Log Collection*
- *3.2 Secure Log Storage*
- *3.3 Strong and Agile Encryption*
- *3.4 Secure Sensitive Data*
- 7.3 System Back Ups

- Program Objective 3.6: Implement and enhance system and network logging and monitoring capabilities.

Safe Online Services

Required Element #6

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

PRITS understands the importance of using the .gov domain and has been promoting safe online services in Puerto Rico by encouraging both municipalities and GPR agencies to migrate to .gov, where appropriate. Almost all GPR agencies are either currently using the .gov domain or are migrating to it.

PRITS and the Planning Committee will coordinate with entities throughout Puerto Rico to assess their use and the trustworthiness of their hosted online services, encourage eligible and appropriate entities (e.g., municipalities) to migrate to the .gov domain and promote safe online services.

The following cybersecurity program objectives align with and support the accomplishment of this SLCGP required element:

- Program Objective 3.1: Migrate all remaining and appropriate government domains to the .gov Internet domain.
- Program Objective 3.5: Enhance identity and access management, particularly for administrative and other privileged accounts.
  - Sub-Objective 3.5.1. Implement strong password policy and controls.
  - Sub-Objective 3.5.2. Require Multi-Factor Authentication (MFA) for public services and government accounts.

Continuity of Operations

Required Element #7

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

All GPR agencies have a continuity plan in place in the event of a disaster (e.g., hurricane).

NIST CSF:

- *PR.IP-4*
- *PR.IP-10*
- *ID.SC-5*
- *RS.RP-1*
- *RS.IM-1*
- *RS.IM-2*

Plans, processes, procedures, and recommended tools and services for enabling continuity of operations will be developed and shared with entities (e.g., GPR agencies and municipalities) to help reduce the impact and disruption of a cybersecurity incident. Additionally, response and recovery exercises will be conducted to practice responding to a major cybersecurity incident, and associated plans, processes, and procedures updated post-exercise.

The following cybersecurity program objective aligns with and supports the accomplishment of this SLCGP required element:

- Program Objective 1.3: Develop, test, and enhance cyber incident response and business continuity plans, processes, and procedures.

Workforce

Required Element #8

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

The Government of Puerto Rico conducts annual cybersecurity awareness training in conjunction with National Cybersecurity Awareness Month (NCSAM) each October to help bolster the knowledge, skills, and abilities of GPR personnel.

PRITS developed the Guide for Employees About Cyber Security V1.1 to instruct new and existing GPR employees on their roles and responsibilities to help prevent incidents that put information handled by the GPR at risk. This guidance applies to all GPR agencies and their employees who use or access any information technology resource of PRITS or any other GPR agency. Each GPR employee is required to read this manual upon hire and to acknowledge they received the guidance and will comply with it.

Additionally, PRITS has a recruitment plan for its cyber workforce that establishes required roles and levels according to the cyber tasks to be performed and the skills needed for each position. However, this plan is currently not mapped to the NICE Framework.

The Cybersecurity Planning Committee will coordinate with PRITS, other GPR agencies, the municipalities, etc., to adopt the National Initiative for Cybersecurity Education (NICE) Framework to identify and mitigate gaps in their cyber workforces and training, as well as to establish effective cyber workforce education and training standards. The Planning Committee and PRITS will also collaborate with higher education to help ensure cybersecurity educational programs at colleges and universities are aligned with the cybersecurity knowledge and skills defined in the NICE Framework to help meet the cyber needs of government (and private sector) entities across Puerto Rico.

The following cybersecurity program objectives align with and support the accomplishment of this SLCGP required element:

- Program Objective 4.1: Adopt and leverage the NICE Framework (i.e., Workforce Framework for Cybersecurity) to build and enhance cyber workforce development, training, and retention programs.
- Program Objective 4.2: Continually deliver cybersecurity awareness training to all government personnel, including simulated phishing campaigns targeting specific users.
- Program Objective 4.3: Develop and provide specialized, role- and skills-based cybersecurity training for cyber, IT, and OT teams.
- Program Objective 4.4: Establish a cybersecurity mentorship program between students and cyber & IT professionals.
- Program Objective 5.1: Develop and launch cyber awareness and education initiatives for businesses, educational institutions, and citizens.

Alignment to Leading Practices:

CPG:

- *4.3 Basic Cybersecurity Training*
- *4.4 OT Cybersecurity Training*

NIST CSF:

- *PR.AT-1*
- *PR.AT-2*

Continuity of Communications and Data Networks

Required Element #9

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

Communications and data networks will be fortified to help improve communications resiliency and continuity capabilities across entities (e.g., PRITS, other GPR agencies and municipalities). Collaboration between these entities will help identify weaknesses, dependencies, and opportunities to mature and protect communications and data networks.

The following cybersecurity program objective aligns with and supports the accomplishment of this SLCGP required element:

- Program Objective 1.3: Develop, test, and enhance cyber incident response and business continuity plans, processes, and procedures.

Alignment to Leading Practices:

NIST CSF:

- *PR.PT-4*
- *PR.PT-5*

Protect Critical Infrastructure and Key Resources

Required Element #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 state.

The Government of Puerto Rico maintains a list of critical infrastructure based on an annual strategic infrastructure review required by FEMA.

Identifying all Critical Infrastructure and Key Resources (CIKR) will be a Commonwealth-wide approach to assist entities (e.g., GPR agencies and municipalities) to understand better their risk landscape and where to enhance cybersecurity capabilities for CIKR. This will enable these entities to implement measures to identify potential cyber risks and threats, evaluate their impact, and take steps to ensure the availability and reliability of CIKR.

The following cybersecurity program objectives align with and support the accomplishment of this SLCGP required element:

- Program Objective 2.1: Perform continual, comprehensive, and periodic (e.g., annual) cyber risk assessments.
- Program Objective 2.3: Continually assess government entities' cybersecurity maturity and identify areas for enhancement.

Alignment to Leading Practices:

NIST CSF:

- *ID.RA-5*
- *ID.RA-6*
- *ID.AM-5*
- *ID.BE-4*
- *DE.AE-2*
- *DE.AE-4*
- *ID.RM-3*

Cyber Threat Indicator Information Sharing

Required Element #11

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

PRITS currently receives threat advisories and CISA alerts and advisories. These threat advisories are triaged by PRITS and then distributed across the GPR agencies.

Cyber threat indicator sharing will be promoted, enabled, and enhanced within and throughout Puerto Rico through engagement with GPR agencies, municipalities, CISA, the MS-ISAC, etc. Cyber threat indicator sharing enables PRITS to obtain and share threat intelligence to enhance other GPR agencies' and municipalities' cybersecurity detection and response capabilities.

The following cybersecurity program objectives align with and support the accomplishment of this SLCGP required element:

- Program Objective 5.2: Establish and enhance public-private partnerships aimed at improving cybersecurity across Puerto Rico.

Alignment to Leading Practices:

CPG:

- *5.2 Vulnerability Disclosure/ Reporting*
- *7.1 Incident Reporting*

NIST CSF:

- *ID.RA-2*

Leverage CISA Services

Required Element #12

Leverage cybersecurity services offered by the Department (See NOFO Appendix G for additional information on CISA resources and required services and membership).

In 2022, the Government of Puerto Rico completed the Nationwide Cybersecurity Review (NCSR).

The Cybersecurity Planning Committee and PRITS will guide the adoption of required CISA services while also encouraging GPR agencies and municipalities to participate in other recommended CISA services, memberships, and resources to assist them in better understanding their cybersecurity posture and reducing their cyber risk.

The following cybersecurity program objectives align with and support accomplishment of this SLCGP required element:

- Program Objective 2.4: Obtain CISA Cyber Hygiene assessments across external government networks and web applications.
- Program Objective 5.2: Establish and enhance public-private partnerships aimed at improving cybersecurity across Puerto Rico.

Information Technology and Operational Technology Modernization Review

Required Element #13

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

The Cybersecurity Planning Committee and PRITS will lead and encourage GPR agencies and municipalities to perform information technology (IT) and operational technology (OT) modernization reviews to identify areas where new solutions (e.g., cloud services, artificial intelligence) can be adopted to improve operations, enhance security, reduce costs, and/or proactively phase out legacy and unsupported systems across both IT and OT.

The following cybersecurity program objective aligns with and supports the accomplishment of this SLCGP required element:

- Program Objective 3.2: Upgrade or replace outdated, end-of-life, and unsupported software.

Cybersecurity Risk and Threat Strategies

Required Element #14

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

The Planning Committee and PRITS will coordinate and work with other GPR agencies and municipalities to develop an overarching cybersecurity risk strategy. Once completed, this strategy will be made available to all entities in Puerto Rico so that all GPR agencies and municipalities uniformly understand and consistently manage cyber risks. The strategy will provide a standardized process for GPR agencies and municipalities to identify, assess, and mitigate cyber threats, vulnerabilities, and associated risks.

The following cybersecurity program objectives align with and support the accomplishment of this SLCGP required element:

- Program Objective 1.1: Continue, enhance, and expand the Cybersecurity Planning Committee to involve and meet the cybersecurity needs of an increasing number of stakeholders.
- Program Objective 1.2: Develop and promulgate a cybersecurity framework based on industry leading practices, such as the NIST CSF.

- Program Objective 2.1: Perform continual, comprehensive, and periodic (e.g., annual) cyber risk assessments.
- Program Objective 5.2: Establish and enhance public-private partnerships aimed at improving cybersecurity across Puerto Rico.

Alignment to Leading Practices:

NIST CSF:

- *ID.RM-1*

Rural Communities

Required Element #15

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

The Cybersecurity Planning Committee and PRITS will continue to provide outreach and build collaborative relationships with rural municipalities throughout Puerto Rico so that these communities also have full access to, can participate in, and benefit from cybersecurity items, services, capabilities, and activities implemented leveraging SLCGP funding. Rural municipalities will be fully included and are intended to benefit from all planning and implementation efforts for achieving cybersecurity program goals and objectives and meeting the required elements.

Additionally, the following cybersecurity program objective aligns with and supports accomplishment of this SLCGP required element:

- Program Objective 1.1: Continue, enhance, and expand the Cybersecurity Planning Committee to involve and meet the cybersecurity needs of an increasing number of stakeholders.

Distribution to Local Governments

Required Element #16

Distribute funds, items, services, capabilities, or activities to local governments.

As documented in the FY 2022 SLCGP NOFO, the minimum 80% local government pass-through (including the minimum 25% rural area pass-through) requirement does *not* apply to the Commonwealth of Puerto Rico.

FUNDING AND SERVICES

The Commonwealth of Puerto Rico State has been awarded $2,491,949 in federal SLCGP funding for FY 2022 as displayed in the following table:

Table 4 FY 2022 SLCGP Funding

FY 2022 SLCGP Funding			
Anticipated Federal Funding Release	Federal Allocation	Puerto Rico State Share	Total FY 2022 Award
October 2023	$2,491,949	$0	$2,491,949

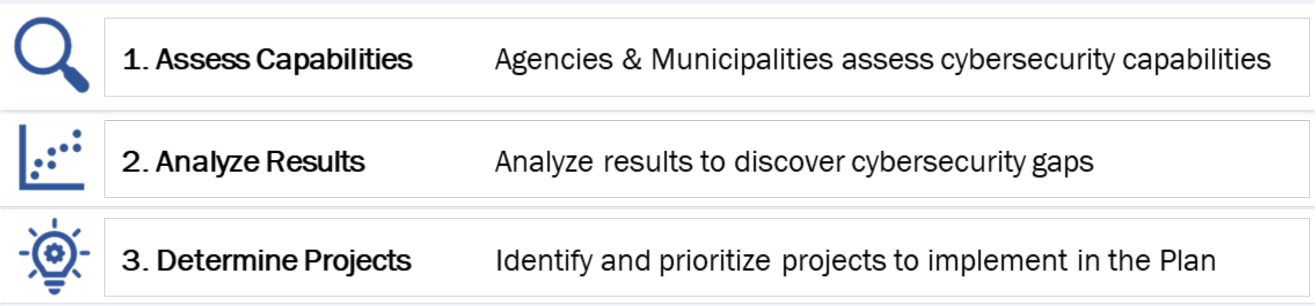
As documented in the FY 2022 grant award package, Puerto Rico is *not* required to match the federal award with any amount of non-Federal funds.

In addition to the grant funding that will be received through the SLCGP, PRITS will work to identify and obtain additional funds to sustain cybersecurity initiatives and investments described in this Plan upon conclusion of all grant years' periods of performance and exhaustion of available SLCGP grant funding.

Projects planned for investment leveraging FY 2022 SLCGP funding are identified, along with a description, cost, status, priority, etc. for each project in "Appendix B: Project Summary Worksheet." Prospective projects initially targeted to utilize FY 2023 SLCGP grant funds are also included in Appendix B but with individual project costs marked as "TBD."

ASSESS CAPABILITIES

An initial cybersecurity Capabilities Assessment was conducted with participating entities (GPR agencies and municipalities) to determine cybersecurity gaps and maturity levels against the required plan elements. It was conducted through a self-assessment that allowed each entity to 1) confirm whether it performs each of the required elements; and, if so, 2) its maturity level in performing such elements. The Capabilities Assessment provided an initial baseline of GPR agency and municipality maturity versus the required elements while also enabling identification of initial SLCGP-funded projects for inclusion in the Puerto Rico Cybersecurity Plan in advance of plan submission to CISA. The results of the assessment were used to identify, prioritize, and select investment projects to address cybersecurity gaps and needs.

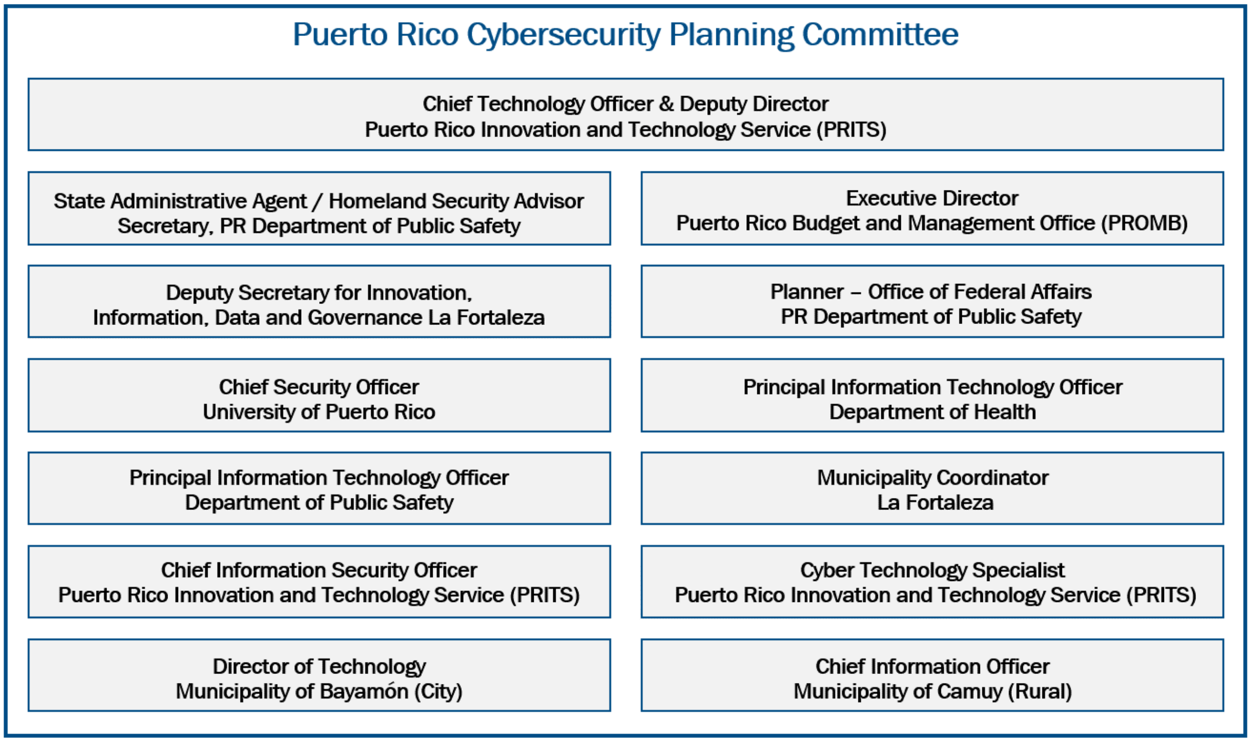


1. Assess Capabilities	Agencies & Municipalities assess cybersecurity capabilities
2. Analyze Results	Analyze results to discover cybersecurity gaps
3. Determine Projects	Identify and prioritize projects to implement in the Plan

Figure 3 Capabilities Assessment process

IMPLEMENTATION PLAN

The Puerto Rico Cybersecurity Planning Committee has been tasked with the development and maintenance of the SLCGP Cybersecurity Plan to help improve the cybersecurity posture of entities across Puerto Rico. The Committee has defined roles and responsibilities to implement the Cybersecurity Plan and metrics to measure progress towards implementing the Plan. The graphic below (Figure 4) illustrates the composition of the Planning Committee.



Puerto Rico Cybersecurity Planning Committee

Chief Technology Officer & Deputy Director
Puerto Rico Innovation and Technology Service (PRITS)

State Administrative Agent / Homeland Security Advisor
Secretary, PR Department of Public Safety

Executive Director
Puerto Rico Budget and Management Office (PROMB)

Deputy Secretary for Innovation,
Information, Data and Governance La Fortaleza

Planner – Office of Federal Affairs
PR Department of Public Safety

Chief Security Officer
University of Puerto Rico

Principal Information Technology Officer
Department of Health

Principal Information Technology Officer
Department of Public Safety

Municipality Coordinator
La Fortaleza

Chief Information Security Officer
Puerto Rico Innovation and Technology Service (PRITS)

Cyber Technology Specialist
Puerto Rico Innovation and Technology Service (PRITS)

Director of Technology
Municipality of Bayamón (City)

Chief Information Officer
Municipality of Camuy (Rural)

Figure 4 Structure of the PR SLCGP Cybersecurity Planning Committee

Organization Roles and Responsibilities

The Puerto Rico Innovation and Technology Service, or PRITS, was established by Law 75 on July 25, 2019. PRITS fundamentally aims to nurture a resilient, agile, and efficient government, all while prioritizing transparency in its operations. PRITS directly oversees the development of projects that promote effective integration of technology within governmental management. The establishment and maintenance of secure cyber environments across Puerto Rico's governments and other critical entities has been identified as a top priority by PRITS. To comprehensively address this challenge, PRITS has undertaken a proactive initiative to assess, understand, and fortify the cybersecurity defenses of government agencies, municipalities, and the broader community. This initiative is carried out with the support of the SLCGP.

The Cybersecurity Planning Committee developed the Plan and identified cybersecurity services and activities for addressing potential cyber threats. Representatives from local entities assisted the Committee by providing input on the status of their cybersecurity capabilities and key security concerns through the Capabilities Assessment and while participating in Committee activities. Going forward, PRITS and the Planning Committee will continue to update the Cybersecurity Plan to ensure that goals, objectives, and investment projects continue to address the highest priority cybersecurity risks and the needs of entities across Puerto Rico.

PRITS is responsible for coordination and implementation of the services and activities identified in the Plan. PRITS will collaborate with other GPR agencies and the municipalities to ensure a comprehensive and coordinated approach to accomplishing cybersecurity initiatives and investment projects.

The Planning Committee will work with PRITS and the State Administrative Agency (SAA) to apply for and allocate grant funding for investment projects, oversee the implementation of those projects, and periodically report on financial and project performance to FEMA/CISA.

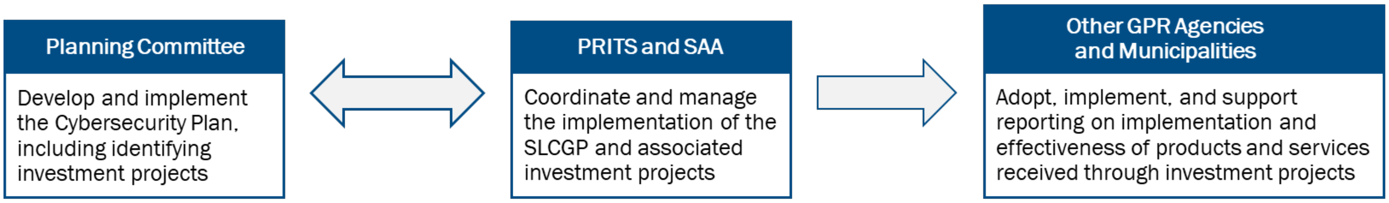

Planning Committee
Develop and implement the Cybersecurity Plan, including identifying investment projects
PRITS and SAA
Coordinate and manage the implementation of the SLCGP and associated investment projects
Other GPR Agencies and Municipalities
Adopt, implement, and support reporting on implementation and effectiveness of products and services received through investment projects

Figure 5 Collaboration between the PR SLCGP Cybersecurity Planning Committee, PRITS & SAA, and other entities

Feedback From Municipalities

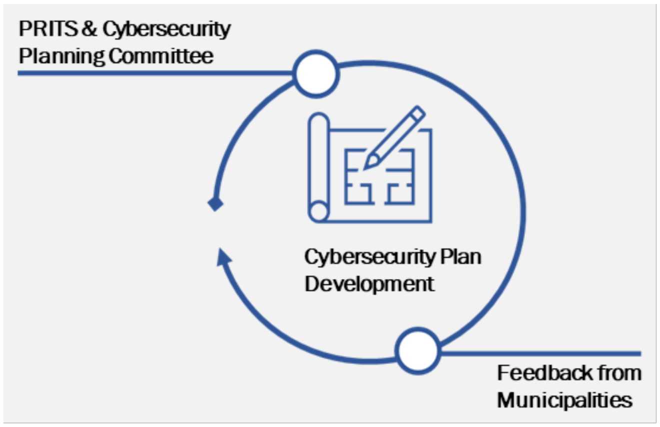

PRITS & Cybersecurity Planning Committee
Cybersecurity Plan Development
Feedback from Municipalities

Figure 6 Feedback cycle for the Cybersecurity Plan

The Cybersecurity Planning Committee actively reached out to, involved, and solicited feedback from the local government jurisdictions in Puerto Rico (i.e., the municipalities) to develop the Cybersecurity Plan and identify investment projects to address cybersecurity risks and threats. Participating municipalities provided feedback and input throughout the development of the Cybersecurity Plan, including and notably the City of Bayamón. The Director of IT for the City of Bayamón is also a member of the Planning Committee.

As detailed in "Appendix A: Cybersecurity Plan Capabilities Assessment," a significant percentage (37%) of municipalities responded to the Capabilities Assessment. The assessment results also constitute valuable, direct feedback on the current cybersecurity maturity and needs of many municipalities across the island. As depicted in Figure 7 below, Capabilities Assessment responses also include substantial representation of both rural (21 out of 64) and larger/non-rural (8 out of 14) municipalities that are also geographically distributed throughout Puerto Rico.

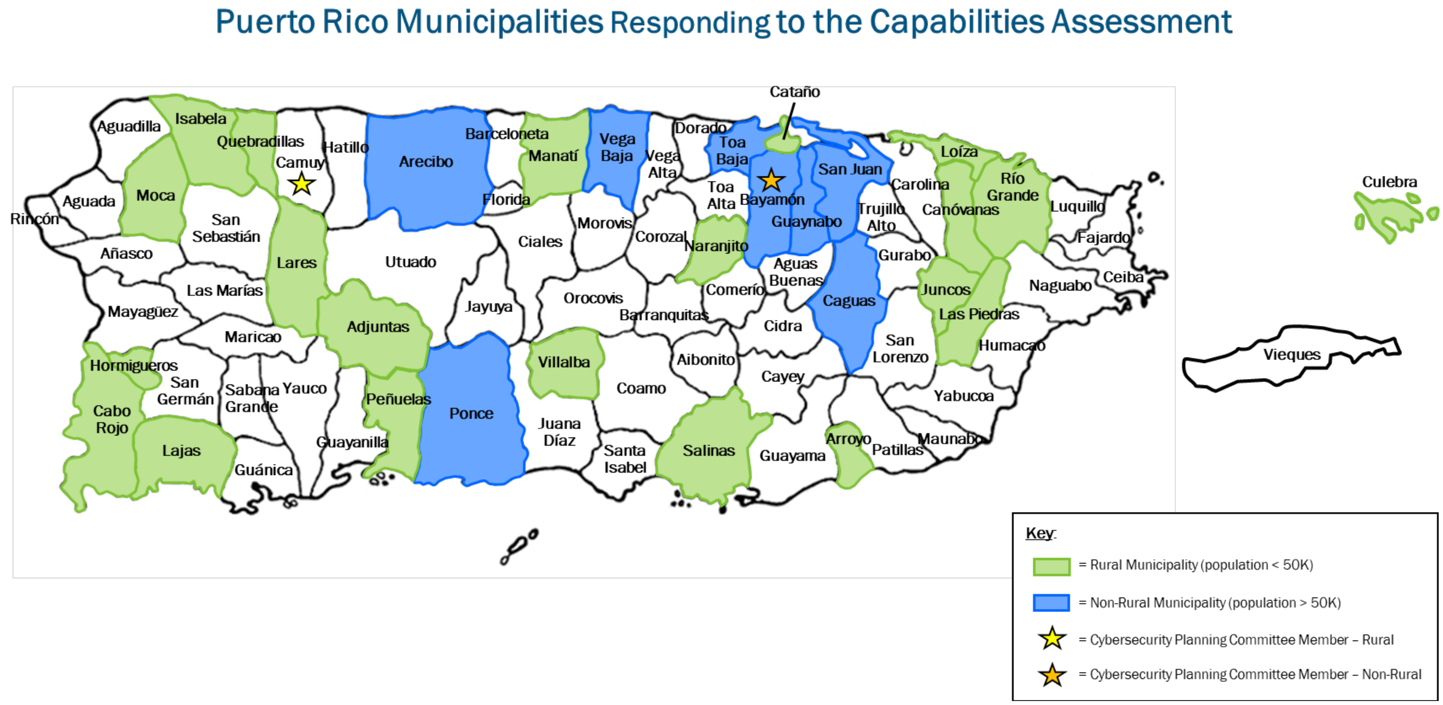


Figure 7 Puerto Rico Municipalities responding to the Capabilities Assessment

Larger municipalities, with more mature cybersecurity programs–like the City of Bayamon–are also helping to lead the way for enhancing the cybersecurity of other, often smaller municipalities in Puerto Rico. Several of these larger municipalities are benchmarking their cybersecurity performance according to a set of leading cybersecurity practices. This strategy is intended to help less cyber mature municipalities in Puerto Rico benchmark and measure their own security efforts according to leading cybersecurity practices as well as in comparison to their peers. The smaller municipalities can then continually assess their cybersecurity performance over time according to the benchmarks set by the larger municipalities.

The larger municipalities are developing improvement plans that will not only provide security benefits within their own city's cyber boundaries but also throughout different parts of the island. This will help standardize policies, prioritize cyber risk reduction strategies, and, if needed, help advocate for stronger cybersecurity measures at all levels of government. Cyberattacks are increasing at an alarming rate and targeting U.S. government entities, with no regard to size, location, or agency type. In response to these increasing threats, Puerto Rico's municipalities are taking aggressive steps to improve their network and system security.

In addition to the two municipalities directly included in the Cybersecurity Planning Committee, Bayamón and Camuy, representatives from the remaining municipalities will continue to collaborate with the Planning Committee and PRITS to help implement the Cybersecurity Plan and associated projects. Additionally, the Planning Committee will collaborate with the following local government groups:

- Association of Mayors
- Federation of Mayors

Collaboration with municipalities and local towns through existing organizations such as Conexion Laboral and the Information Systems Consortium, has helped to establish a baseline understanding of municipalities' current cybersecurity posture and informed how GPR would like to collaborate with local governments moving forward. Puerto Rico plans to enhance collaboration amongst its municipalities through the expansion of existing consortiums and/or the development of new local government associations.

Resource Overview and Timeline Summary

The Cybersecurity Planning Committee identified necessary resources and a timeline for implementing and achieving the Plan goals and objectives over the next two to three years. A summary of investment projects can be found in "Appendix B: Project Summary Worksheet."

The Commonwealth of Puerto Rico Cybersecurity Planning Committee understands that, upon CISA approval, the Cybersecurity Plan is required to be resubmitted for CISA review and approval within two years and then annually thereafter. In between these required, periodic resubmissions to CISA, the Planning Committee will also review the Cybersecurity Plan for any necessary, substantive changes that may be needed and will revise the Plan accordingly. As investment projects are completed, resulting in mitigation of risks, closure of identified capability gaps, and achievement of initially targeted program objectives, new projects will be selected that address additional and potentially new program objectives. Further, as the Cybersecurity Plan is a "living, breathing" strategy for cybersecurity and cyber risk reduction across Puerto Rico, it is anticipated that project priorities will shift with the changing cybersecurity landscape and as determined by continual cyber risk assessments performed over time (e.g., annual NCSR).

METRICS

The Puerto Rico Cybersecurity Planning Committee has developed metrics to measure progress towards implementing the Cybersecurity Plan and reducing cybersecurity threats and risks. The metrics are designed to help stakeholders understand Puerto Rico's progress towards achieving its cybersecurity program goals and objectives.

Table 8 in “Appendix C: Entity Metrics” outlines the program goals, objectives, associated metrics, and metric descriptions that the Commonwealth of Puerto Rico has established for measuring its progress in implementing its Cybersecurity Plan.

APPENDIX A: CYBERSECURITY PLAN CAPABILITIES ASSESSMENT

The Commonwealth of Puerto Rico began its capabilities assessment approach by developing an intuitive survey instrument based on the required elements directly applicable to prospective respondents of the assessment. Entities invited to participate in the capabilities assessment included all 121 GPR agencies and all 78 municipalities throughout Puerto Rico. The response rate was excellent for each entity type, with 32% of all GPR agencies and 37% of the municipalities responding to the survey.

The five (5) required elements rated as the lowest maturity across all entities include:

1. Workforce Development and adoption of the NICE Framework
2. Leveraging CISA Services (e.g., Cyber Hygiene Services, NCSR)
3. Best Practices and Methodologies – Data encryption for data at rest and in transit
4. Information Technology & Operational Technology Modernization Review
5. Best Practices and Methodologies – Implementing enhanced logging

The five (5) required elements rated as the lowest maturity across GPR agencies include:

1. Workforce Development and adoption of the NICE Framework
2. Best Practices and Methodologies – Data encryption for data at rest and in transit
3. Information Technology & Operational Technology Modernization Review
4. Best Practices and Methodologies – Implementing enhanced logging
5. Leveraging CISA Services (e.g., Cyber Hygiene Services, NCSR)

The five (5) required elements rated as the lowest maturity across the municipalities include:

1. Leveraging CISA Services (e.g., Cyber Hygiene Services, NCSR)
2. Workforce Development and adoption of the NICE Framework
3. Best Practices and Methodologies – Data encryption for data at rest and in transit
4. Information Technology & Operational Technology Modernization Review
5. Assessment and Mitigation

The table below (Table 5) depicts the required element-based questions included in the survey that went out to the GPR agencies and the municipalities. For any "yes" response to each question, the official responding on behalf of the entity then selected a maturity level rating and had the opportunity to provide any additional comments relevant to the response. All completed questionnaires were returned to the PRITS team, which compiled all results and mapped each entity's individual responses to a standard quantitative score. This scoring system resulted in an average and comparable score for each required element across all responding entities and for each of the GPR agency and municipality entity types.

Table 5 Required Element-based Capabilities Assessment Questions

Capability Assessment Questions	
Required Element	**Associated Question for GPR Agency or Municipality POCs**
1. Manage, Monitor, and Track	Does your organization manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, your organization, as well as the information technology deployed on those information systems, including any legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology?

Capability Assessment Questions	
Required Element	Associated Question for GPR Agency or Municipality POCs
2. Monitor, Audit, and Track	Does your organization monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, your organization?
3. Enhance Preparedness	Does your organization enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, your organization against cybersecurity risks and cybersecurity threats?
4. Assessment and Mitigation	Has your organization implemented a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, your organization?
5. Best Practices and Methodologies	
a. Implement multi-factor authentication	Does your organization implement multi-factor authentication?
b. Implement enhanced logging	Does your organization implement enhanced logging?
c. Data encryption for data at rest and in transit	Does your organization encrypt data at rest and/or in transit?
d. End use of unsupported/end of life software and hardware that are accessible from the Internet	Has your organization ended the use of unsupported/end of life software and hardware that are accessible from the Internet?
e. Prohibit use of known/fixed/default passwords and credentials	Does your organization prohibit the use of known/fixed/default passwords and credentials?
f. Ensure the ability to reconstitute systems (backups)	Does your organization ensure the ability to reconstitute systems from backups?
g. Migration to the .gov internet domain	Does your organization use the .gov Internet domain?
6. Safe Online Services	Does the Government of Puerto Rico promote the delivery of safe, recognizable, and trustworthy online services by agencies and local governments within Puerto Rico, including through the use of the .gov Internet domain?
7. Continuity of Operations	Does your organization ensure continuity of operations in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident?
8. Workforce Development	Does your organization use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in your organization's cybersecurity workforce, enhance recruitment and retention efforts for your workforce, and bolster the knowledge, skills, and abilities of your organization's personnel, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training?
9. Continuity of Communications and Data Networks	Does the Government of Puerto Rico ensure continuity of communication and data networks within the jurisdiction of Puerto Rico and between agencies and local governments within Puerto Rico in the event of an incident involving those communications or data networks?
10. Assess and Mitigate Cybersecurity Risks and Threats	Does the Government of Puerto Rico assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical

Capability Assessment Questions	
Required Element	**Associated Question for GPR Agency or Municipality POCs**
to Critical Infrastructure and Key Resources	infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of Puerto Rico?
11. Cyber Threat Indicator Information Sharing	Does the Government of Puerto Rico work to enhance capabilities to share cyber threat indicators and related information between GPR, the municipalities, and CISA?
12. Leverage CISA Services	Does your organization leverage cybersecurity services offered by CISA, including participating in CISA's Cyber Hygiene Services (web application and external network vulnerability scanning) and completing the annual Nationwide Cybersecurity Review (NCSR)?
13. Information Technology and Operational Technology Modernization Review	Has your organization implemented an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives?
14. Cybersecurity Risk and Threat Strategies	Does the State develop and coordinate strategies to address cybersecurity risks and cybersecurity threats with other organizations, including in consultation with local governments and associations of local governments within your State, neighboring entities, members of an ISAC, etc.?
15. Rural Communities	Is adequate access to, and participation in, SLCGP-funded services and programs provided to rural areas within Puerto Rico?
16. Distribution to Local Governments	N/A

Table 6 below represents an aggregation of the responses across Puerto Rico, as well as across each of the GPR agency and municipality entity types and is not representative of any individual entity type or individual entity. However, and where appropriate, additional information on capability assessment results and associated trends for a required element(s) that are especially relevant to a particular entity type (GPR agency or municipality) is described in the table.

Table 6 Capabilities Assessment Results

Completed by the Commonwealth of Puerto Rico			
Required Element	**Brief Description of Current Capabilities of Entities within Puerto Rico**	**Capability Level**	**Project #(s)**
1. Manage, Monitor, and Track			N/A
2. Monitor, Audit, and Track			PR-5

Completed by the Commonwealth of Puerto Rico			
Required Element	Brief Description of Current Capabilities of Entities within Puerto Rico	Capability Level	Project #(s)
3. Enhance Preparedness			PR-4, PR-16, PR-17
4. Assessment and Mitigation			PR-7, PR-8
5. Best Practices and Methodologies			
a. Implement multi-factor authentication			PR-12
b. Implement enhanced logging			PR-5
c. Data encryption for data at rest and in transit			PR-11
d. End use of unsupported/end of life software and hardware that are accessible from the Internet			PR-13

Completed by the Commonwealth of Puerto Rico			
Required Element	**Brief Description of Current Capabilities of Entities within Puerto Rico**	**Capability Level**	**Project #(s)**
e. Prohibit use of known/fixed/default passwords and credentials			N/A
f. Ensure the ability to reconstitute systems (backups)			PR-4, PR-17
g. Migration to the .gov internet domain			PR-10
6. Safe Online Services			PR-10
7. Continuity of Operations			PR-4, PR-17
8. Workforce			

Completed by the Commonwealth of Puerto Rico			
Required Element	Brief Description of Current Capabilities of Entities within Puerto Rico	Capability Level	Project #(s)
9. Continuity of Communications and Data Networks			PR-4, PR-17
10. Assess and Mitigate Cybersecurity Risks and Threats to Critical Infrastructure and Key Resources			PR-3, PR-6
11. Cyber Threat Indicator Information Sharing			PR-7
12. Leverage CISA Services			PR-7
13. Information Technology and Operational Technology Modernization Review			PR-15
14. Cybersecurity Risk and Threat Strategies			PR-3, PR-6
15. Rural Communities			N/A

Completed by the Commonwealth of Puerto Rico			
Required Element	Brief Description of Current Capabilities of Entities within Puerto Rico	Capability Level	Project #(s)
16. Distribution to Local Governments	N/A		

APPENDIX B: PROJECT SUMMARY WORKSHEET

As depicted in Table 7 below, this Project Summary Worksheet provides a list of cybersecurity projects that the Commonwealth of Puerto Rico plans to complete to develop or improve cybersecurity capabilities identified in “Appendix A: Cybersecurity Plan Capabilities Assessment.”

Table 7 Project Summary Worksheet

Project Summary Worksheet							
No.	**Project Name**	**Project Description**	**Related Required Element #**		**Status**	**Priority**	**Project Type**
PR-1	Puerto Rico Cybersecurity Plan Development	Develop an initial Puerto Rico Cybersecurity Plan that meets all State and Local Cybersecurity Grant Program requirements and obtains CISA approval.	N/A		Ongoing	High	Plan
PR-2	PR Cybersecurity Plan Education & Awareness Campaign	Plan, coordinate, and launch a mass education and awareness campaign, in conjunction with National Cybersecurity Awareness Month on the Puerto Rico Cybersecurity Plan for employees of the GPR, municipalities, and private sector entities that operate or manage IT systems on behalf of the GPR or municipalities.	8		Future (near-term using FY 2022 funding)	High	Train
PR-3	Cybersecurity Risk Assessment & Analysis for the Five Key GPR Agencies	Perform comprehensive cyber risk assessments utilizing the NCSR, MS-ISAC Foundational Assessment, etc. for the Departments of Education, Family Affairs, Health, Public Safety, and Finance (i.e., the five key GPR agencies) to understand those entities’ cybersecurity posture and identify cybersecurity risks and control gaps. Assessment results will be leveraged to update the Cybersecurity Plan and select future SLCGP investment projects.	10, 14		Future (near-term using FY 2022 funding)	High	Organize
PR-4	Table-Top & Full-Scale Cyber Exercises	Develop and facilitate cyber exercises that help improve the ability to monitor, evaluate, and assess cyber incident response capabilities of GPR agencies and the municipalities, as well as GPR/PRITS’ own information sharing and incident management processes and procedures in the event of a cyber-related emergency impacting one or more GPR agencies or municipalities.	3, 5f, 7, 9		Future (near-term using FY 2022 funding)	High	Exercise
PR-5	Enhanced Logging & Analysis	Perform enhanced logging and analysis for GPR agencies and/or municipalities through the	2, 5b		Future (near-term using FY 2022 funding)	High	Equipment

Project Summary Worksheet

No.	Project Name	Project Description	Related Required Element #		Status	Priority	Project Type
		implementation and integration of an enterprise SIEM tool to enable centralized log ingestion and monitoring.					
PR-6	Cybersecurity Risk Assessments & Analyses for GPR Agencies and Municipalities	Plan and perform comprehensive cyber risk assessments utilizing the NCSR, MS-ISAC Foundational Assessment, etc. for additional GPR agencies and/or municipalities to understand those entities' cybersecurity posture and identify cybersecurity risks and control gaps. Assessment results will be leveraged to update the Cybersecurity Plan and select future SLCGP investment projects.	10, 14		Future (near-term using FY 2022 funding)	High	Organize
PR-7	Implementation of CISA Services	Inform and educate GPR agencies and municipalities on registering for and implementing CISA's cybersecurity services, including CISA Cyber Hygiene Services.	4, 11, 12		Future (near-term)	High	Organize
PR-8	Cybersecurity Vulnerability Assessments	Perform recurring cybersecurity vulnerability scans of municipalities' internal and external networks, systems, and applications and provide recommended mitigations for highest criticality vulnerabilities.	4	TBD	Future	High	Organize
PR-9	NICE Framework Planning	Develop a strategic plan and roadmap for assisting GPR agencies and municipalities with adopting and leveraging the NICE Framework to assess and enhance their cybersecurity workforces. (This project may also include an initial proof of concept involving a small number of GPR agencies and/or municipalities.)	8	TBD	Future	High	Plan
PR-10	Migration to .gov Internet Domain	Advise and assist appropriate municipalities with migration to the .gov Internet domain.	5g, 6	TBD	Future	High	Organize
PR-11	Encryption of Sensitive Data	Advise and assist appropriate GPR agencies and municipalities with encrypting sensitive data at rest and in transit.	5c	TBD	Future	High	Organize
PR-12	Multi-Factor Authentication	Advise and assist appropriate GPR agencies and municipalities with implementing multi-factor authentication.	5a	TBD	Future	High	Organize
PR-13	Ending Use of Unsupported/End of Life Software and Hardware	Advise and assist appropriate GPR agencies and municipalities with planning and implementation associated with ending the use of unsupported/end of life software and hardware that are accessible from the Internet.	5d	TBD	Future	High	Organize

Project Summary Worksheet							
No.	**Project Name**	**Project Description**	**Related Required Element #**	**Cost**	**Status**	**Priority**	**Project Type**
PR-14	NICE Framework Adoption	Advise and assist GPR agencies and municipalities with adopting and leveraging the NICE Framework to establish formal cybersecurity workforce development programs for recruiting, retaining, and training cybersecurity personnel within their organizations.	8	TBD	Future	High	Plan
PR-15	IT & OT Modernization Review Process	Advise and assist appropriate GPR agencies and municipalities with implementing an IT and OT modernization review process with aligned cybersecurity objectives	13	TBD	Future	Moderate	Organize
PR-16	Cyber Incident Response Plan and template development	Develop a formal and comprehensive Cyber Incident Response Plan for Puerto Rico, as well as a Cyber Incident Response Plan template that can be utilized by each GPR agency and municipality to produce its own customized Cyber Incident Response Plan.	3	TBD	Future	Moderate	Plan
PR-17	Business Continuity & Disaster Recovery Plans and template development	Develop formal and comprehensive Business Continuity & Disaster Recovery Plans for Puerto Rico, as well as Business Continuity & Disaster Recovery Plan templates that can be utilized by each GPR agency and municipality to produce its own customized Business Continuity & Disaster Recovery Plans.	3, 5f, 7, 9	TBD	Future	Moderate	Plan

APPENDIX C: ENTITY METRICS

Table 8 Entity Metrics

Cybersecurity Plan Metrics			
Program Goals	Program Objectives	Associated Metrics	Metric Description (details, source, frequency)
1. Establish centralized cybersecurity governance, policies & standards, and recommended baselines for cybersecurity and resilience across Puerto Rico.	1.1 Continue, enhance, and expand the Cybersecurity Planning Committee to involve and meet the cybersecurity needs of an increasing number of stakeholders.	▪ The total number of municipality focused SLCGP investment projects that are successfully completed ▪ Percentage of municipalities involved in and/or benefiting from SLCGP investment projects ▪ The total number of GPR agency focused SLCGP investment projects that are successfully completed ▪ Percentage of GPR agencies involved in and/or benefiting from SLCGP investment projects	Details: ▪ The total number of municipality focused SLCGP investment projects that are successfully completed ▪ The number of municipalities involved in and/or benefiting from SLCGP investment projects divided by the total number of municipalities ▪ The total number of GPR agency focused SLCGP investment projects that are successfully completed ▪ The number of GPR agencies involved in and/or benefiting from SLCGP investment projects divided by the total number of agencies Source: SLCGP project review Frequency: Annual
	1.2 Develop and promulgate a cybersecurity framework based on industry leading practices, such as the NIST CSF.	▪ An overarching cybersecurity framework based on industry leading practices, such as the NIST CSF, has been developed, is reviewed periodically (e.g., annually), and is updated, as needed ▪ Percentage of municipalities that have implemented the cybersecurity framework (tailored to each municipality's specific cyber risk profile) ▪ Percentage of GPR agencies that have implemented the cybersecurity framework (tailored to each GPR agency's specific cyber risk profile)	Details: ▪ An overarching cybersecurity framework based on industry leading practices, such as the NIST CSF, has been developed, is reviewed periodically (e.g., annually), and is updated, as needed ▪ The number of municipalities that have implemented the cybersecurity framework (tailored to each municipality's specific cyber risk profile) divided by the total number of municipalities responding to a request for that information ▪ The number of GPR agencies that have implemented the cybersecurity framework (tailored to each GPR agency's specific cyber risk profile) divided by the total number of GPR agencies responding to a request for that information Source: ▪ Policy review ▪ Cyber risk assessment questionnaire

Cybersecurity Plan Metrics			
Program Goals	**Program Objectives**	**Associated Metrics**	**Metric Description (details, source, frequency)**
			Frequency: Annual
	1.3 Develop, test, and enhance cyber incident response and business continuity plans, processes, and procedures.	- Percentage of municipalities that have approved cyber incident response and business continuity plans, processes, and procedures in place - Percentage of municipalities that test and update cyber incident response and business continuity plans, processes, and procedures - Percentage of GPR agencies that have approved cyber incident response and business continuity plans, processes, and procedures in place - Percentage of GPR agencies that test and update cyber incident response and business continuity plans, processes, and procedures	Details: - The number of municipalities that: - Have approved cyber incident response and business continuity plans, processes, and procedures in place - Test and update cyber incident response and business continuity plans, processes, and procedures divided by the total number of municipalities responding to a request for that information - The number of GPR agencies that: - Have approved cyber incident response and business continuity plans, processes, and procedures in place - Test and update cyber incident response and business continuity plans, processes, and procedures divided by the total number of GPR agencies responding to a request for that information Source: - Policy review - Cyber risk assessment questionnaire Frequency: Annual
2. Understand cybersecurity posture and continually assess risk to entities across Puerto Rico.	2.1. Perform continual, comprehensive, and periodic (e.g., annual) cyber risk assessments.	- Percentage of municipalities that perform organization-wide, cyber risk assessments (at least annually) - Percentage of GPR agencies that perform organization-wide, cyber risk assessments (at least annually)	Details: - The number of municipalities that perform organization-wide, cyber risk assessments (at least annually) divided by the total number of municipalities responding to a request for that information - The number of GPR agencies that perform organization-wide, cyber risk assessments (at least annually) divided by the total number of GPR agencies responding to a request for that information Source: - Program review - Cyber risk assessment questionnaire Frequency: Annual

Cybersecurity Plan Metrics			
Program Goals	Program Objectives	Associated Metrics	Metric Description (details, source, frequency)
	2.2. Maintain complete inventories of IT and operational technology (OT) hardware and software owned or operated by or on behalf of government entities.	▪ Percentage of municipalities that maintain complete inventories of IT and OT hardware and software owned or operated by or on behalf of the municipality ▪ Percentage of GPR agencies that maintain complete inventories of IT and OT hardware and software owned or operated by or on behalf of the GPR agency	Details: ▪ The number of municipalities that maintain complete inventories of IT and OT hardware and software owned or operated by or on behalf of the municipality divided by the total number of municipalities responding to a request for that information ▪ The number of GPR agencies that maintain complete inventories of IT and OT hardware and software owned or operated by or on behalf of the GPR agency divided by the total number of GPR agencies responding to a request for that information Source: ▪ Program review ▪ Cyber risk assessment questionnaire Frequency: Annual
	2.3. Continually assess government entities' cybersecurity maturity and identify areas for enhancement.	▪ Percentage of municipalities that assess their cybersecurity maturity and identify areas for enhancement (at least annually) ▪ Percentage of GPR agencies that assess their cybersecurity maturity and identify areas for enhancement (at least annually)	Details: ▪ The number of municipalities that assess their cybersecurity maturity and identify areas for enhancement (at least annually) divided by the total number of municipalities responding to a request for that information ▪ The number of GPR agencies that assess their cybersecurity maturity and identify areas for enhancement (at least annually) divided by the total number of GPR agencies responding to a request for that information Source: Cyber risk assessment questionnaire Frequency: Annual
	2.4. Obtain CISA Cyber Hygiene assessments across external government networks and web applications.	▪ Percentage of municipalities that have registered for and obtain CISA Cyber Hygiene assessments across their external networks and web applications ▪ Percentage of GPR agencies that have registered for and obtain CISA Cyber Hygiene assessments across their external networks and web applications	Details: ▪ The number of municipalities that have registered for and obtain CISA Cyber Hygiene assessments across their external networks and web applications divided by the total number of municipalities responding to a request for that information ▪ The number of GPR agencies that have registered for and obtain CISA Cyber Hygiene assessments across their external networks and

Cybersecurity Plan Metrics			
Program Goals	Program Objectives	Associated Metrics	Metric Description (details, source, frequency)
			web applications divided by the total number of GPR agencies responding to a request for that information Source: - Program review - Cyber risk assessment questionnaire Frequency: Annual
	2.5. Perform recurring vulnerability scans of internal and external networks, systems, and applications.	- Percentage of municipalities that perform recurring vulnerability scans of internal and external networks, systems, and applications - Percentage of GPR agencies that perform recurring vulnerability scans of internal and external networks, systems, and applications	Details: - The number of municipalities that perform recurring vulnerability scans of internal and external networks, systems, and applications divided by the total number of municipalities responding to a request for that information - The number of GPR agencies that perform recurring vulnerability scans of internal and external networks, systems, and applications divided by the total number of GPR agencies responding to a request for that information Source: Cyber risk assessment questionnaire Frequency: Annual
3. Protect citizen data, secure digital public services, and enhance the resilience of critical infrastructure throughout Puerto Rico.	3.1. Migrate all remaining and appropriate government domains to the .gov Internet domain.	- Percentage of municipality domains that have migrated to the .gov Internet domain	Details: - The number of municipality domains that have migrated to the .gov Internet domain divided by the total number of municipality domains identified - The number of GPR agency domains that have migrated to the .gov Internet domain divided by the total number of GPR agency domains identified Source: - Program review - Cyber risk assessment questionnaire - Online research Frequency: Annual
	3.2. Upgrade or replace outdated, end-of-life, and unsupported software.	- Percentage of municipalities with outdated, end-of-life, and unsupported software - Percentage of GPR agencies with outdated, end-of-life, and unsupported software	Details: - The number of municipalities with outdated, end-of-life, and unsupported software divided by the total number of municipalities

Cybersecurity Plan Metrics			
Program Goals	Program Objectives	Associated Metrics	Metric Description (details, source, frequency)
			responding to a request for that information ▪ The number of GPR agencies with outdated, end-of-life, and unsupported software divided by the total number of GPR agencies responding to a request for that information Source: ▪ Program review ▪ Cyber risk assessment questionnaire Frequency: Annual
	3.3. Establish effective software patch management processes.	▪ Percentage of municipalities that have implemented software patch management processes ▪ Percentage of GPR agencies that have implemented software patch management processes	Details: ▪ The number of municipalities that have implemented software patch management processes divided by the total number of municipalities responding to a request for that information ▪ The number of GPR agencies that have implemented software patch management processes divided by the total number of GPR agencies responding to a request for that information Source: ▪ Program review ▪ Cyber risk assessment questionnaire Frequency: Annual
	3.4. Implement architectural measures and controls to protect data at rest and in transit from unauthorized access and use.	▪ Percentage of municipalities that have implemented architectural measures and controls (e.g., encryption) to protect data at rest and in transit from unauthorized access and use ▪ Percentage of GPR agencies that have implemented architectural measures and controls (e.g., encryption) to protect data at rest and in transit from unauthorized access and use	Details: ▪ The number of municipalities that have implemented architectural measures and controls (e.g., encryption) to protect data at rest and in transit from unauthorized access and use divided by the total number of municipalities responding to a request for that information ▪ The number of GPR agencies that have implemented architectural measures and controls (e.g., encryption) to protect data at rest and in transit from unauthorized access and use divided by the total number of GPR agencies responding to a request for that information Source: ▪ Program review

Cybersecurity Plan Metrics			
Program Goals	**Program Objectives**	**Associated Metrics**	**Metric Description (details, source, frequency)**
			▪ Cyber risk assessment questionnaire Frequency: Annual
	3.5. Enhance identity and access management, particularly for administrative and other privileged accounts. 3.5.1. Implement strong password policies and controls. 3.5.2. Require Multi-Factor Authentication (MFA) for public services and government accounts.	▪ Percentage of municipalities that have implemented a strong password policy and controls ▪ Percentage of municipalities that require MFA for public services and government accounts ▪ Percentage of GPR agencies that have implemented a strong password policy and controls ▪ Percentage of GPR agencies that require MFA for public services and government accounts	Details: ▪ The number of municipalities that: - Have implemented a strong password policy and controls - Require MFA for public services and government accounts divided by the total number of municipalities responding to a request for that information ▪ The number of GPR agencies that: - Have implemented a strong password policy and controls - Require MFA for public services and government accounts divided by the total number of GPR agencies responding to a request for that information Source: ▪ Program review ▪ Cyber risk assessment questionnaire Frequency: Annual
	3.6. Implement and enhance system and network logging and monitoring capabilities.	▪ Percentage of municipalities that have implemented network logging and monitoring capabilities ▪ Percentage of GPR agencies that have implemented network logging and monitoring capabilities	Details: ▪ The number of municipalities that have implemented network logging and monitoring capabilities divided by the total number of municipalities responding to a request for that information ▪ The number of GPR agencies that have implemented network logging and monitoring capabilities divided by the total number of GPR agencies responding to a request for that information Source: ▪ Program review ▪ Cyber risk assessment questionnaire Frequency: Annual
4. Cultivate Puerto Rico's government cybersecurity workforce through education, training, and partnerships.	4.1. Adopt and leverage the NICE Framework (i.e., Workforce Framework for Cybersecurity) to build and enhance cyber workforce development, training, and retention programs.	▪ Percentage of municipalities that have adopted and leverage the NICE Framework to build and enhance cyber workforce development, training, and retention programs ▪ Percentage of GPR agencies that have adopted and	Details: ▪ The number of municipalities that have adopted and leverage the NICE Framework to build and enhance cyber workforce development, training, and retention programs divided by the total number of municipalities

Cybersecurity Plan Metrics			
Program Goals	**Program Objectives**	**Associated Metrics**	**Metric Description (details, source, frequency)**
		leverage the NICE Framework to build and enhance cyber workforce development, training, and retention programs	responding to a request for that information ▪ The number of GPR agencies that have adopted and leverage the NICE Framework to build and enhance cyber workforce development, training, and retention programs divided by the total number of GPR agencies responding to a request for that information Source: ▪ Program review ▪ Cyber risk assessment questionnaire Frequency: Annual
	4.2. Continually deliver cybersecurity awareness training to all government personnel, including simulated phishing campaigns targeting specific users.	▪ Percentage of municipalities in which all personnel have received cybersecurity awareness training, including simulated phishing campaigns targeting specific users ▪ Percentage of GPR agencies in which all personnel have received cybersecurity awareness training, including simulated phishing campaigns targeting specific users	Details: ▪ The number of municipalities in which all personnel have received cybersecurity awareness training, including simulated phishing campaigns targeting specific users, divided by the total number of municipalities responding to a request for that information ▪ The number of GPR agencies in which all personnel have received cybersecurity awareness training, including simulated phishing campaigns targeting specific users, divided by the total number of GPR agencies responding to a request for that information Source: ▪ Program review ▪ Cyber risk assessment questionnaire Frequency: Annual
	4.3. Develop and provide specialized, role- and skills-based cybersecurity training for cyber, IT, and OT teams.	▪ Percentage of municipalities that develop and provide specialized, role- and skills-based cybersecurity training for cyber, IT, and OT teams ▪ Percentage of GPR agencies that develop and provide specialized, role- and skills-based cybersecurity training for cyber, IT, and OT teams	Details: ▪ The number of municipalities that develop and provide specialized, role- and skills-based cybersecurity training for cyber, IT, and OT teams divided by the total number of municipalities responding to a request for that information ▪ The number of GPR agencies that develop and provide specialized, role- and skills-based cybersecurity training for cyber, IT, and OT teams divided by the total number of GPR agencies responding to a request for that information

Cybersecurity Plan Metrics			
Program Goals	**Program Objectives**	**Associated Metrics**	**Metric Description (details, source, frequency)**
			Source: ▪ Program review ▪ Cyber risk assessment questionnaire Frequency: Annual
	4.4. Establish a cybersecurity mentorship program between students and cyber & IT professionals.	▪ The total number of students participating in the cybersecurity mentorship program ▪ The percentage increase in total number of students participating in the cybersecurity mentorship program	Details: ▪ The total number of students participating in the cybersecurity mentorship program ▪ The percentage increase in total number of students participating in the cybersecurity mentorship program Source: Mentorship program review Frequency: Annual
5. **Promote a secure cyberculture throughout Puerto Rico.**	5.1. Develop and launch cyber awareness and education initiatives for businesses, educational institutions, and citizens.	▪ The total number of cyber awareness and education campaigns launched ▪ The total number of individuals attending each cyber awareness campaign event	Details: ▪ The total number of cyber awareness and education campaigns launched ▪ The total number of individuals attending each cyber awareness campaign event Source: Cyber awareness and education initiatives review Frequency: Annual
	5.2. Establish and enhance public-private partnerships aimed at improving cybersecurity across Puerto Rico.	▪ The total number of public-private partnerships aimed at improving cybersecurity that are formally established	Details: The total number of public-private partnerships aimed at improving cybersecurity that are formally established Source: Public-private cybersecurity partnerships program review Frequency: Annual

APPENDIX D: ACRONYMS

Table 9 Acronyms

Acronym	Definition
BIA	Business Impact Analysis
CIKR	Critical Infrastructure and Key Resources
CISA	Cybersecurity and Infrastructure Security Agency
CPGs	Cybersecurity Performance Goals
CSF	Cybersecurity Framework
CTI	Cyber Threat Intelligence
EDR	Endpoint Detection and Response
EO	Executive Order
EOL	End-of-life
GPR	Government of Puerto Rico
IR	Incident Response
IT	Information Technology
MFA	Multi-Factor Authentication
MS-ISAC	Multi-State Information Sharing and Analysis Center
NCSAM	National Cybersecurity Awareness Month
NCSR	Nationwide Cybersecurity Review
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NOFO	Notice of Funding Opportunity
OT	Operational Technology
PHI	Protected Health Information
PII	Personally Identifying (or Identifiable) Information
POC	Point of Contact
PRC3	Puerto Rico Cyber Command Center
PRITS	Puerto Rico Innovation and Technology Service
RPOs	Recovery Point Objectives
RTOs	Recovery Time Objectives
SAA	State Administrative Agency
SIEM	Security Information and Event Management
SLAs	Service Level Agreements
SLCGP	State and Local Cybersecurity Grant Program
SLT	State, Local, Territorial
SOC	Security Operations Center
VAPT	Vulnerability Assessment and Penetration Testing
VPN	Virtual Private Network