2023 – 2025 "PACIFIC CYBERGUARD: KONTRA I PILIGRU"

September 28, 2023

Version 1.0

Approved by Guam Homeland Security and the Office of Technology (designated cyber/IT experts for the MRFC)

TABLE OF CONTENTS

LOURDES A. LEON GUERRERO
GOVERNOR

JOSHUA F. TENORIO
LT. GOVERNOR

UFISINAN I MAGA'HÅGAN GUÅHAN
OFFICE OF THE GOVERNOR OF GUAM

Hafa Adai!

I am pleased to introduce Guam's comprehensive cybersecurity state plan, officially referred to as the *Pacific Cyberguard: Kontra I Piligru Island-wide Cybersecurity Plan ("PCG")*. The PCG complies with the U.S. Department of Homeland Security guidelines for the State and Local Cybersecurity Grant Program ("SLCGP"), Grant No. EMW-2022-CY-00052-S01.

The Government of Guam Cybersecurity Working Group developed the PCG as an Incident Annex to the Guam Emergency Response Plan. Recognizing the urgent need to bolster the security and resiliency of our island's digital environment, and to improve the accessibility and efficiency of digital systems, the Cybersecurity Working Group engaged a diverse group of experts and stakeholders from various sectors of our island community to ensure a collaborative and inclusive process in the PCG's development. These "whole of government" efforts culminated in a comprehensive plan and "living document" that will assist all sectors of local government, including critical infrastructure and private sector partners, as well as higher education institutions, finance, health, election, transportation, commissions, boards, and councils in the development of strategic processes and implementation of mature cybersecurity systems. The PCG represents a significant measure in safeguarding our island's digital infrastructure to ensure the safety and security of our community, and in bridging gaps in technical assistance and support for cyber plan development and maturity.

The Guam Homeland Security/Office of Civil Defense ("GHS/OCD") and the Guam Office of Technology ("OTECH"), the designated cyber or information technology experts for the Marianas Regional Fusion Center ("MRFC"), will administer the PCG. As a division of the GHS/OCD, the MRFC collects, evaluates, and disseminates intelligence relating to criminal and terrorist activity in the Marianas and protects information networks and telecommunications networks from cyberattacks. In implementing the PCG, the GHS/OCD will leverage technology and industry resources to enhance the security and efficiency of our digital systems, and improve the resilience of our digital environment.

As our community grows and progresses, our people will continue to rely on the efficiency and security of digital engagement with our government agencies and with each other. With the implementation of the *Pacific Cyberguard: Kontra I Piligru Island-wide Cybersecurity Plan*, I am confident we are setting a course toward ensuring a safe and reliable digital environment that meets the needs of our people at this moment in our island's history, and in the days to come.

Lou Leon Guerrero

LOURDES A. LEON GUERRERO
Maga'hågan Guåhan
Governor of Guam

LETTER FROM GUAM HOMELAND SECURITY ADVISOR

Hafa Adai! I am pleased to introduce a vital component of our collective security efforts, The Pacific CyberGuard: Kontra I Piligru Island-wide Cybersecurity Plan ("PCG"). This plan highlights the ongoing collaboration with Guam's hardworking IT talent within our government agencies and local organizations, and our federal partners (CISA, Guam Army National Guard, FBI, Coast Guard, etc.) as we work together to synchronize a "whole of government" strategy to effectively counter cyber incidents that could affect our territory and region.

This plan operates as an Incident Annex to the broader Guam Emergency Response Plan ("GERP"), detailing the roles, responsibilities, and collaborative measures to be taken by local government agencies and departments. It's designed to be a dynamic document that continuously adapts and improves, drawing from ongoing planning, tabletop exercises, and lessons learned from real-world experiences.

Taking guidance from The Presidential Policy Directive ("PPD")-41, which sets the U.S. Federal Government's response parameters for cyber incidents, PCG emphasizes and embodies the importance of a unified and coordinated "whole of government" approach to handling significant cyber incidents affecting our region.

Oversight for this document is provided by the Guam Office of Homeland Security ("GHS"), and the Guam Office of Technology ("OTECH") whom are also the designated cyber/IT experts for the Marianas Regional Fusion Center ("MRFC"). These agencies collaborate with a variety of local government departments and agencies to ensure its currency and effectiveness.

By adopting the "The Pacific CyberGuard: Kontra I Piligru Island-wide Cybersecurity Plan" as an Incident Annex to the Guam Emergency Response Plan, I hereby affirm its importance and relevance.

Sincerely,

Esther J.C. Aguigui
HSA17
Homeland Security Advisor
Office of Guam Homeland Security and Civil Defense

LETTER FROM GOV GUAM CYBERSECURITY PLANNING COMMITTEE AND WORKING GROUP

Håfa Adai,

The Government of Guam Cybersecurity Working Group is pleased to present to you the 2023-2025 Pacific Cyber Guard: Kontra I Piligru Island wide Cybersecurity Plan. This living document represents the Government of Guam's continued commitment to improving cybersecurity throughout all government agencies and local organizations and supporting the efforts of a "Whole of Government" approach with all local critical stakeholders. In addition, this update meets the requirement of the current U.S. Department of Homeland Security guidelines for the State and Local Cybersecurity Grant Program (SLCGP).

Representatives from the Government of Guam Cybersecurity Working Group collaborated to develop and update the Cybersecurity Plan with actionable and measurable goals and objectives that have champions identified to ensure completion.

The goals and objectives in this plan are designed to support our island in planning for new technologies and navigating the ever-changing cybersecurity landscape. They also incorporate the 16 SLCGP required plan elements.

As we continue to enhance cybersecurity, we must remain dedicated to improving our resilience among disciplines and across jurisdictional boundaries. With help from cybersecurity practitioners and our federal partners, we will work to achieve the goals set forth in the Cybersecurity Plan and become a model for cyber resilience.

Senseramente,

OFFICE OF TECHNOLOGY
GOVERNMENT OF GUAM

Frank L.G. Lujan, Jr.
Chief Technology Officer
Government of Guam - Office of Technology
211 Aspinall Avenue
PO Box 884, Hagåtña, GUAM 96932
frank.lujan@otech.guam.gov
Office: 671.635.4500

GOALS AND OBJECTIVES:

1) Collaboration & Partnerships

2) Assessments

3) Cybersecurity Governance

4) Cyber workforce Development (NICE)

5) Implementation of Best Practices

6) Risk Management

7) Emergency Communications and Business Continuity

8) Community Outreach

CYBER PLANNING COMMITTEE (CPC) MEMBERSHIP

The CPC shall be composed of nine (9) individuals. The members shall consist of the following:

i. Guam Homeland Security – Homeland Security Advisor
ii. Guam Homeland Security – Grants Manager
iii. Mariana Regional Fusion Center – Director or Cybersecurity Liaison
iv. Office of Technology – Chief Technology Officer
v. Office of Technology – Cybersecurity Analyst
vi. Office of Technology – Data Processing Manager
vii. Guam National Guard-J6 Director
viii. Office of Attorney General
ix. Guam Power Authority-IT & Cybersecurity

CYBER WORKING GROUP (CWG) MEMBERSHIP

The CWG participants consist of, but not limited to, representatives from the following areas:

i. Office of the Guam Homeland Security – Emergency Management;
ii. Mariana Regional Fusion Center – Cybersecurity;
iii. Office of Technology –Systems Administrator;
iv. The Guam Waterworks Authority;
v. The Port Authority of Guam;
vi. The Guam International Airport Authority;
vii. Guam Election Commission;
viii. Guam Police Department;

ix. Guam Fire Department;
x. Guam Department of Education;
xi. Guam Memorial Hospital;
xii. Department of Public Health and Social Services;
xiii. Guam Behavioral Health and Wellness Center;
xiv. The Mayors Council of Guam;
xv. Judiciary of Guam
xvi. Guam Legislature
xvii. The University of Guam;
xviii. The Guam Community College;
xix. Guam Regional Medical Center;
xx. Telecommunication Companies;
xxi. Financial Institutions;
xxii. Fuel Providers

The Governor of Guam or the Homeland Security Advisor may, at their discretion, request/appoint additional representatives to the CPC. The term of each member shall be for two (2) years, except that a member may continue to serve until a successor is appointed.

INTRODUCTION

The content of the following plan adheres to the Cybersecurity Plan Template provided by the FY22 Notice of Funding Opportunity (NOFO) for the State and Local Cybersecurity Grant Program (SLCGP).

The Pacific Cyber Guard: Kontra I Piligru Islandwide Cybersecurity Plan is a four year strategic planning living document that contains the following components:

- **Vision and Mission**: Articulates the vision and mission for improving cybersecurity resilience interoperability over the next one-to-three-years.
- **Organization, and Roles and Responsibilities:** Describes the current roles and responsibilities, and any governance mechanisms for cybersecurity within the Government of Guam as well as successes, challenges, and priorities for improvement. This also includes a strategy for the cybersecurity program and the organizational structure that identifies how the cybersecurity program is supported. In addition, this section includes governance that identifies authorities and requirements of the Government of Guam cybersecurity program. The Cybersecurity Plan is a guiding document and does not create any authority or direction over any of the Government of Guam's local systems or agencies.
- **How feedback and input from local governments and associations was incorporated.** Describes how inputs from government agencies, critical infrastructure, and mission

partners are used to reduce overall cybersecurity risk across the eligible entity. This is especially important in order 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 Government of Guam along with methods and strategies for funding sustainment and enhancement to meet long-term goals.
- **Implementation Plan:** Describes the Government of Guam'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 Government of Guam will measure the outputs and outcomes of the program across the entity. The National Institute of Standards and Technology (NIST) Cybersecurity Framework[1], included in Figure 1, helps guide key decision points about risk management activities through various levels of an organization from senior executives to business and process level, as well as implementation and operations.

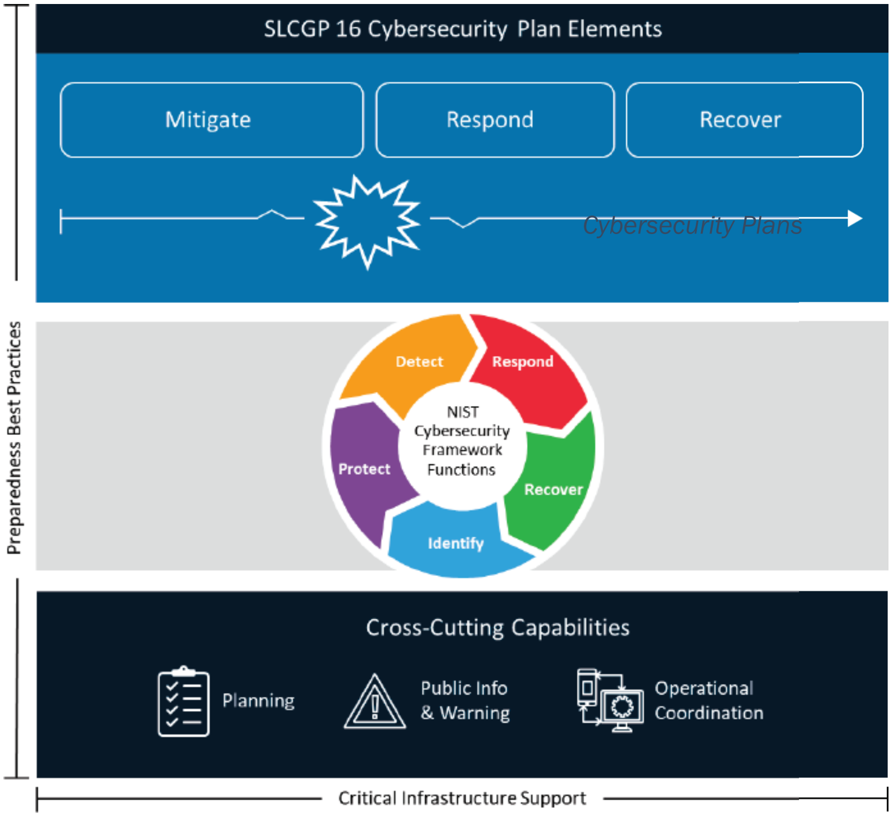
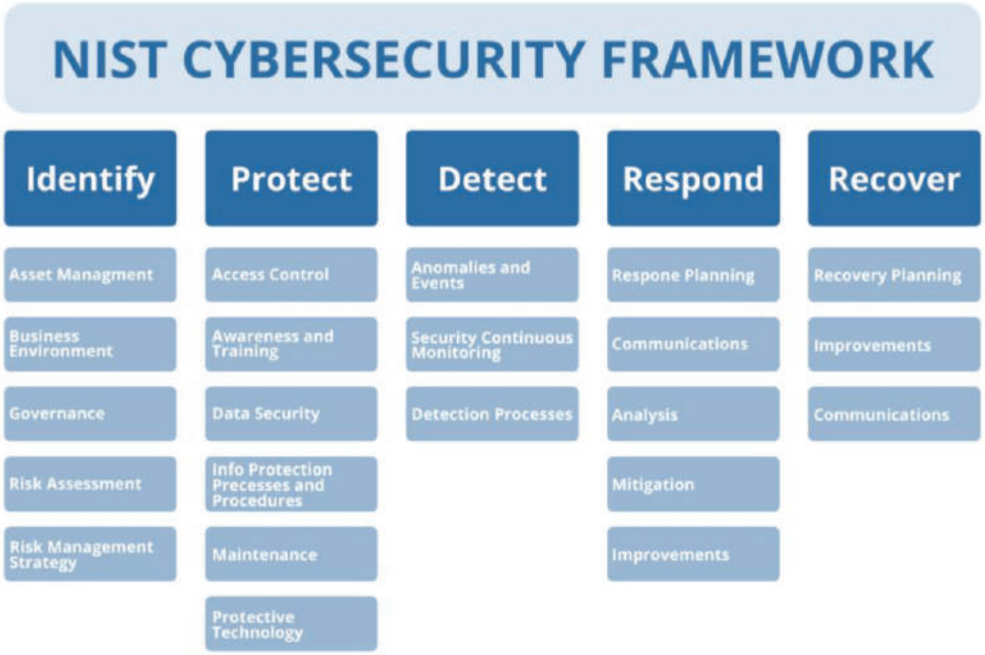

SLCGP 16 Cybersecurity Plan Elements
Mitigate
Respond
Recover
Preparedness Best Practices
Detect
Respond
NIST Cybersecurity Framework Functions
Protect
Recover
Identify
Cross-Cutting Capabilities
Planning
Public Info & Warning
Operational Coordination
Critical Infrastructure Support

Figure 1: Achieving Cyber Resilience Through Comprehensive Cybersecurity Plans

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



NIST CYBERSECURITY FRAMEWORK

Identify	Protect	Detect	Respond	Recover
Asset Managment	Access Control	Anomalies and Events	Respone Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Precesses and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

Figure 2: NIST Framework elements

National Institute of Standards and Technology (NIST)

Vision and Mission

Vision:

Collaboratively building a comprehensive island-wide cybersecurity program to empower all government entities to collaborate and effectively prevent and respond to cyber-attacks.

Mission:

To identify, assess, mitigate, and reduce cyber risks with Guam's critical stakeholders, government agencies, public and private institutions.

CYBERSECURITY PROGRAM GOALS AND OBJECTIVES

Government of Guam Cybersecurity goals and objectives include the following:

2023-2025 Cybersecurity Program	
Program Goal	Program Objectives
1. Collaboration & Partnerships	1.1 Develop a comprehensive directory of contacts across government agencies and critical infrastructure communities to facilitate engagement with the "Whole of Government" effort, share resources, and ensure that all participants are aware of support. 1.2 Create a platform where all stakeholders can securely share information among trusted stakeholder groups: critical infrastructure partners, third-party suppliers, K-12 school districts, and higher education institutions. 1.3 Identify and document all government agencies/organization's roles and responsibilities in supporting Government of Guam's Pacific Cyber Guard: Kontra I Piligru Islandwide Cybersecurity Plan - Whole of Government approach. 1.4 Collaborate and train together with mission stakeholders from Department of Defense, Guam Army National Guard, and Federal Agencies such as FBI, CISA, Coast Guard, etc.
2. Assessments	2.1 Assist Government IT departments to conduct an asset inventory of all organizationally owned, leased, licensed, or managed information assets to help understand their environment, and leverage self-evaluations and assessments through CISA and MS-ISAC to establish a baseline. 2.2 Implement data classification to assist agencies with determining what is critical and essential for emergency communications and business continuity.

Program Goal	Program Objectives
	2.3 Assist Agencies and Organizations to complete the Nationwide Cybersecurity Review ("NCSR")
3. Cybersecurity Governance	3.1 Establish management structures and roles along with their associated authorities and responsibilities for centrally managing, coordinating, developing, implementing, and maintaining the agency/organization's cybersecurity program. 3.2 Assist agencies with Implementing policies and standards based off of the NIST Framework to securely protect organizational data and information systems while maintaining compliance with applicable statutory and regulatory requirements pertaining to confidentiality, integrity, availability, privacy, and safety. 3.3 Work with government agencies and critical infrastructure partners to develop incident response plans and an overarching island-wide cyber disruption response plan. 3.4 Develop and implement trainings and workshops aimed at assisting agencies and organizations to develop and test their robust governance policies and procedures. 3.5 Work closely with legislators to advance bills aimed at strengthening information/cyber security. Additionally, seek revisions to Guam's procurement regulations to provide IT departments with increased flexibility in procuring subscriptions, IT support licenses, and replacing outdated software and equipment.
4. Developing Cyber Workforce: aligning with National Initiative for Cybersecurity Education ("NICE") Framework	4.1 Provide government IT personnel with resources and opportunities to continually improve and develop knowledge, skills, and abilities required to address evolving cybersecurity challenges and to enable career advancement. 4.1a Grant Funding can be designated to assist Gov of Guam IT personnel to earn cybersecurity certifications or attend off-island

Program Goal	Program Objectives
	hands-on workshops or conferences. Awardees are required to provide training to transfer knowledge to the Gov Guam Cybersecurity Working Group members. 4.2 Partner with Higher Education Institutions, federal government, and private businesses to create and execute a talent development pathway within our community. 4.3 Revise government job titles and job descriptions for IT roles and cybersecurity experts to reflect current needs. Collaborate with agencies to build consensus for salary enhancements for IT professionals, ensuring our ability to attract and retain local technical talent. 4.4 Appoint a Chief Information Security Officer (CISO) as a cabinet level C-Suite executive to reinforce the united "Whole of Government" cybersecurity strategy, facilitating collaboration with agencies, organizations, and critical stakeholders to bridge gaps in technical assistance and support for cyber plan development and maturity. CISO will directly report to the Governor and work closely with OTECH, GHS, and the MRFC to be able to continuously advise the administration on the current cybersecurity landscape and the risks that threaten our community.
5. Implementation of Best Practices	5.1 Assist agencies/organizations that intend to receive cybersecurity grant monies to prioritize and implement best practices projects that include the following: • Implementation of multi-factor authentication and strong password policy that discourages the use of known/fixed/default passwords and credentials. • Implement robust logging mechanisms. • Apply data encryption for data at rest and in transit. • Develop securities around all non-replaceable, unsupported/end of life software and hardware that are accessible

Program Goal	Program Objectives
	from the Internet, and move towards procuring replacements. • Ensure the ability to reconstitute systems (backups). • Migration to the .gov internet domain. • Implement free scanning services from MS-ISAC and CISA (such as cyber hygiene vulnerability, web application, etc.) 5.2 Implement administrative, technical, and physical controls necessary to safeguard information assets in all their forms from threats to their confidentiality, integrity, or availability, whether internal or external, deliberate, or accidental. 5.3 Research development, and implementation of Security Controls, Software Defined Network/Perimeter applications and technology that advance toward a "Zero Trust" Architecture.
6. Risk Management	6.1 Establish processes to categorize assets and information according to their sensitivity and criticality and require that protection mechanisms be implemented to commensurate with the impact should there be a loss of confidentiality, integrity, or availability of the asset or information. 6.2 Collaborate with key stakeholders to define risk tolerance levels and risk acceptance criteria that align with the organization's strategic objectives. 6.3 Foster a Risk-Aware Culture and accountability throughout the organization. Ensure that all employees understand their role in identifying and reporting potential risks. 6.4 Provide regular role-based training and awareness programs to educate all government employees on cybersecurity best practices and the importance of risk management. Establish clear incident reporting procedures and encourage a no-blame approach to reporting security incidents or vulnerabilities, fostering a collaborative response to threats.

Program Goal	Program Objectives
7. Emergency Communications and Business Continuity	7.1 Educate all government agency IT Departments on the Incident Command Structure (ICS) and ITSL accreditation to help agencies understand where they plug in during a large-scale cyber incident. 7.2 Ensure all Government of Guam IT Departments implement and test their emergency communications and business continuity plan. This will be an annex to the entities cybersecurity plan and overarching cyber disruption plan.
8. Community Outreach	8.1 Collaborate with Federal partners and mission critical stakeholders to provide cybersecurity awareness training and assist in creating a quick reference guide on best practices for protecting their sensitive data from criminal threat actors.

CYBERSECURITY PLAN ELEMENTS

The FY22 SLCGP NOFO 09-13-2022 listed 16 elements, four objectives and projects as part of the funding requirements. Below are the elements and objectives that will be incorporated in projects that will be initiated. Each item will be tracked and the metrics will be documented formally. These elements, objectives and projects align with the goals of Guam's Pacific Cyber Guard: Kontra I Piligru Islandwide Cybersecurity Plan (Whole of Government) approach to ensure all government agencies mature in their cybersecurity posture.

Manage, Monitor, and Track

Agencies/Organizations will implement procedures to control and limit access to agency information assets, allowing access only to authorized users as per business and legal requirements. They will employ mechanisms to manage, track, and protect information assets from unauthorized use or damage. Access will be granted based on a "need-to-use" or "need-to-know" basis.

Monitor, Audit, and Track

For the Government of Guam, it's crucial that asset owners, custodians, and information security and privacy officers take the following actions:

(a) Ensure that information assets they oversee are assessed for security and privacy risks. Configure them to enable event logging, enhancing awareness of potential threats to agency information and systems' confidentiality, integrity, availability, and privacy. Identify and manage these risks effectively.

(b) Review and securely retain event logs in full compliance with all relevant local and federal laws, regulations, executive orders, directives, internal agency policies, and contractual obligations.

Enhance Preparedness

The Government of Guam will establish ongoing risk management procedures that encompass the identification, assessment, mitigation, and monitoring of risks that could negatively impact their operations, information systems, and data. These procedures will guide the implementation of Incident Response Plans, Continuity of Operations Plans, and the Cyber Disruption Plan. Insights gained from these exercises will be used to improve future planning, influence organizational decisions, and identify additional equipment and training requirements. Additionally, there should be collaboration with critical infrastructure and mission stakeholders, such as the Guam Army National Guard, CISA, FBI, Coast Guard, etc., to exchange training resources and share lessons learned.

Assessment and Mitigation

It is crucial to conduct security assessments for all significant systems, applications, and general support systems, whether they are operated directly or on behalf of government entities. These assessments are essential to ensure that adequate security and privacy controls are in place and that risks are effectively managed throughout the entire lifecycle of these systems.

The risk management process encompasses identifying, assessing, and addressing security and privacy risks from the inception of a system project until its decommissioning. This proactive approach helps government entities on Guam maintain the security and privacy of systems over time.

Best Practices and Methodologies

The following best practices are included in the plan, and projects to implement will be considered over the life of the SLCGP:

- Implementation of multi-factor authentication and strong password policy that discourages the use of known/fixed/default passwords and credentials.
- Implement enhanced logging.
- Data encryption for data at rest and in transit.
- Develop securities around all non-replaceable, unsupported/end of life software and hardware that are accessible from the Internet, and move towards procuring replacements.
- Ensure the ability to reconstitute systems (backups).
- Migration to the .gov internet domain.

Safe Online Services

As a best practice methodology, government entities will implement a .gov domain unless their security program already has a secure, tested, audited web domain. Government entities should prioritize overall security measures and not rely solely on domain names as indicators of security.

Continuity of Operations

Government of Guam entities will develop and test contingency plans to guarantee the uninterrupted operation of information systems that provide or facilitate essential or critical functions for the Government of Guam and its emergency services. Contingency planning plays a crucial role in managing risks, as it guarantees the accessibility of critical systems and components. This enables agencies to fulfill their obligations as mandated by laws, executive orders, policies, contracts, and ensures the uninterrupted provision of essential government services.

Workforce

Recruitment and retaining a skilled technical workforce is a recognized challenge nationwide, affecting both the public and private sectors. Government agencies/organizations often face constraints due to outdated personnel job titles and descriptions. To address the shortage, Gov Guam agencies and organizations will adopt the NICE framework to create a pipeline for IT/cybersecurity professionals to grow and advance in their careers. Partnerships with the local community college and university will also be developed to help creatively address this issue.

Everyone has a role in securing our environment, thus Government of Guam entities will encourage the education of all employees about the security and privacy risks associated with their roles. Employees should also have a clear understanding of their responsibilities and the relevant laws, regulations, executive orders, directives, policies, standards, and procedures pertaining to the security and privacy of government information and systems.

Cyber Threat Indicator Information Sharing

In coordination with the Regional CISA representative, the FBI, and respective MS-ISAC indicator sharing efforts, the Marianas Regional Fusion Center will monitor information from a variety of open and classified sources, analyze that information, and distribute relevant information across all Government of Guam IT Departments.

Leverage CISA Services

CISA is a critical mission partner with a number of free resources that can be implemented to help government entities advance in their cybersecurity posture. GovGuam Cybersecurity Workforce will encourage the collaboration with CISA to utilize all free resources and implement tools, such as Vulnerability Scanning and Web Application Scanning. These Cyber Hygiene services, as well as the NCSR, will be required for recipients and sub-recipients of SLCGP funds

Information Technology and Operational Technology Modernization Review

Government of Guam entities will be encouraged to implement a plan to replace unsupported software and end of life/outdated equipment such as Windows XP and/or Windows 7 Machines. Should the entity be unable to replace unsupported software or equipment, additional securities around legacy software/equipment should be implemented and risks should be communicated to leadership.

Cybersecurity Risk and Threat Strategies

The GovGuam Cybersecurity Working Group will use this plan and operate under the approved charter to develop and coordinate strategies and projects to address cybersecurity risks and cybersecurity threats with other organizations, including consultation with federal government agencies and the Guam Army National Guard.

FUNDING & SERVICES

In compliance with the SLCGP grant requirements, projects that are approved for funding will be written into the government entities budget to maintain continuity. Collaboration with leadership and lawmakers will ensure continued support for funded projects.

ASSESS CAPABILITIES

Government of Guam entities will use Appendix A: Cybersecurity Plan Capabilities Assessment to assess and document capabilities for the cybersecurity plan elements included in this plan.

IMPLEMENTATION PLAN

Organization, Roles and Responsibilities

Accomplishing goals and objectives will require support and cooperation from numerous individuals, groups, or agencies, and may be added as formal agenda items for review during the Government of Guam Cybersecurity Working Group. Final approval will be from the members of the Cybersecurity Planning Committee.

Appendix B: Project Summary Worksheet will be provided to all participants of the cybersecurity working group to help list proposed cybersecurity projects that tie to each goal and objective of the Pacific Cyber Guard: Kontra I Piligru Islandwide Cybersecurity Plan.

Resource Overview and Timeline Summary

Projects submitted and approved by the Cybersecurity Planning Committee will provide a resource overview and timeline summary of completion.

METRICS

Goal and Objective metrics will be formally documented to clearly show progress of implementation and cybersecurity maturity. Appropriate metrics of successful implementation will be determined by the Cybersecurity Planning Committee and will include metrics such as number of participants, completed surveys by participating government entities, number of risks/vulnerabilities mitigated, security awareness aptitude tests, stakeholder feedback, frequency of exercises, response times etc. Appendix C will be the form used as a guideline for metric reporting.

APPENDIX D: ACRONYMS

Acronym	Definition
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CTO	Chief Technology Officer
FBI	Federal Bureau of Investigations
GERP	Guam Emergency Response Plan
GHS	Guam Homeland Security
HSA	Homeland Security Advisor
ICS	Incident Command Structure
ITSL	Information Technology Service Unit Leader
MRFC	Marianas Regional Fusion Center
MS-ISAC	Multi-State Information Sharing and Analysis Center
NCSR	Nationwide Cybersecurity Review
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
OCD	Office of Civil Defense
OTECH	Office of Technology
PPD	Presidential Policy Directive