



Hawai'i Statewide Cybersecurity Strategy and Implementation Plan

Hawai'i Office of Homeland Security



September 26, 2023

This page intentionally blank



Table of Contents

Authority and Adoption Letter	v
Executive Summary.....	vii
Introduction.....	1
Cybersecurity Plan Essential Elements.....	11
SLCGP Grant Requirements.....	19
Cybersecurity Strategic Plan Projects.....	25
Funding and Services	43
Implementation Plan.....	45
Appendix A: Cybersecurity Plan Capabilities Assessment.....	49
Appendix B: Project Summary Worksheet.....	57
Appendix C: Metrics.....	67
Appendix D: Data Collection Methodology	71
Appendix E: Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR).....	73
Appendix F: Acronyms	75
Appendix G: Stakeholders and Contributors	77



This page intentionally blank

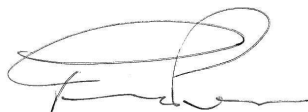


Authority and Adoption Letter

The Hawai'i Statewide Cybersecurity Strategy and Implementation Plan reflects our state's steadfast commitment to enhancing cybersecurity readiness, response, and recovery. Furthermore, this plan aligns with the current guidelines established by the United States (U.S.) Department of Homeland Security (DHS) for the State and Local Cybersecurity Grant Program (SLCGP) and includes all required elements from the Notice of Funding Opportunity (NOFO).

Collaboratively crafted by representatives from diverse stakeholder groups across Hawai'i, this strategy features concrete, measurable goals and objectives, each backed by dedicated champions to ensure successful implementation. These objectives encompass various facets, such as organizational improvement, coordination, collaboration, strategic planning, education, training, exercises, and bolstering our systems and infrastructure. Their overarching purpose is to empower Hawai'i to effectively plan for emerging cybersecurity threats and navigate the dynamic landscape of cybersecurity while adhering to the essential components mandated by the SLCGP.

In our ongoing mission for a more secure and resilient State, it remains paramount that we maintain a persistent commitment to enhancing our resilience across disciplines and beyond jurisdictional boundaries. By harnessing the expertise of our state's cybersecurity professionals, we aim to realize the aspirations outlined in the Statewide Cybersecurity Strategy and Implementation Plan and set an example of cyber resilience for others to follow.



Frank J. Pace
Administrator
Hawai'i Office of Homeland Security
September 26, 2023



Vincent Hoang
Chief Information Security Officer
Hawai'i Office of Enterprise Technology Services
September 26, 2023



This page intentionally blank



Executive Summary

The complex ecosystem of cybersecurity is constantly evolving with the growing interconnectedness and digitization of the world. Consequently, the assurance of security and resilience for critical infrastructure and digital assets becomes increasingly imperative. Hawai'i acknowledges the vital role of cybersecurity in protecting federal, state, and county systems, data, and information, including the vital role of the private sector.

The primary objective of the Hawai'i Statewide Cybersecurity Strategy and Implementation Plan is to establish a comprehensive framework that empowers Hawai'i to proactively address cybersecurity challenges and cultivate a culture centered on tangible steps towards increased security and resilience. Through the implementation of this Hawai'i State Cybersecurity Strategy and Implementation Plan, Hawai'i can take concrete measures to enhance its readiness for cybersecurity incidents, foster relationships with crucial cybersecurity partners, and collectively develop the necessary capabilities for improved preparedness, mitigation, response, and recovery from cybersecurity threats.

The creation of this Hawai'i Statewide Cybersecurity Strategy and Implementation Plan was the result of collaborative planning involving key federal, state, county, and private sector partners, as well as input from cybersecurity subject-matter experts (SMEs). It takes into account Hawai'i's unique characteristics, including its critical infrastructure sectors, and addresses specific cybersecurity threats and hazards that pose risks to Hawai'i from a comprehensive statewide perspective. Furthermore, the Hawai'i Statewide Cybersecurity Strategy and Implementation Plan aims to align with the requirements of the Department of Homeland Security's (DHS) State and Local Cybersecurity Preparedness (SLCGP) program and other established cybersecurity frameworks and best practices to offer a unified and comprehensive approach to cybersecurity.



This page intentionally blank



Introduction

As digital interconnectedness and dependency increases, the State of Hawai'i faces ever-evolving cyber threats. Compounded by geographic isolation, Hawai'i is uniquely vulnerable to growing threats against its critical infrastructure, economy, and the personal data of its government systems and residents. This evolving threat landscape demands a proactive and vigilant approach to cybersecurity, one that recognizes the unique challenges posed by the state's geographic isolation, reliance on digital networks, and interdependency between critical infrastructure sectors. The Hawai'i Statewide Cybersecurity Strategy and Implementation Plan aims to establish a comprehensive approach and vision for building a more secure and resilient state.

Vision and Mission

Vision

Through active collaboration with key private sector, federal, state, regional, and local stakeholders, Hawai'i fosters the growth, improvement, and augmentation of cybersecurity systems, capacities, assets, alliances, and educational initiatives, bolstering the state's ability to provide more robust support to its partners in their efforts to prepare for, respond to, mitigate, and recover from cybersecurity incidents.

Mission

Hawai'i is committed to implementing a comprehensive statewide strategy to strengthen its cybersecurity readiness, ensuring the enhanced protection of digital infrastructure, critical systems, and sensitive information from current and emerging cyber threats.

The state will achieve its vision and mission through a series of initiatives, including:

- (1) Strengthening cybersecurity planning,
- (2) Enhancing the organizational structures for cybersecurity,
- (3) Facilitating improved coordination and collaboration among partners,
- (4) Providing training and education to partners on cybersecurity plans, protocols, procedures, and available resources,



- (5) Conducting exercises to test and refine these plans, protocols, and procedures, and
- (6) Enhancing the resilience of systems and infrastructure against cybersecurity incidents.

Governance

To support the development of the Hawai'i Statewide Cybersecurity Strategy and Implementation Plan, Hawai'i organized a Cybersecurity Planning Committee (CSPC) including 54 individuals representing 36 different federal, state, county, and private sector organizations. Members of the CSPC reflect expertise across emergency management, cybersecurity, and information technology (IT) domains, as well as representatives from education, public health, rural, suburban, and high-population jurisdictions. Over half of the representatives of the CSPC have professional experience relating to cybersecurity or information technology. The CSPC member organizations include the following (listed alphabetically):

- AT&T
- City and County of Honolulu
- County of Hawai'i
- County of Kaua'i
- County of Maui
- DRFortress
- Hawai'i Department of Accounting and General Services
- Hawai'i Department of Attorney General
- Hawai'i Department of Education
- Hawai'i Department of Health
- Hawai'i Department of Human Services
- Hawai'i Department of Transportation
- Hawai'i Gas
- Hawai'i Health Systems Corporation
- Hawai'i Judiciary
- Hawai'i Legislature, House
- Hawai'i Legislature, Senate
- Hawai'i National Guard
- Hawai'i Office of Enterprise Technology Services
- Hawai'i Office of Hawaiian Affairs
- Hawai'i Office of Homeland Security
- Hawai'i Office of the Governor
- Hawai'i State Energy Office
- Hawai'i State Fusion Center
- Hawaiian Electric Company
- Hawaiian Telecom
- Kauai Island Utility Cooperative
- Matson
- Par Pacific
- Servco Pacific Inc.
- The Queen's Health System
- T-Mobile
- U.S. Department of Homeland Security, Coast Guard
- U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency
- U.S. Department of Homeland Security, Secret Service
- U.S. Department of Health and Human Services
- U.S. Department of Justice, Federal Bureau of Investigation
- University of Hawai'i



Prior to its application for the initial year of the SLCGP, Hawai'i established a SLCGP Subcommittee (under its Homeland Security Executive Advisory Council) consisting of at least one representative from relevant stakeholders to include:

- County representatives;
- Officials involved in production of the state's THIRA/SPR;
- State, county, and/or Urban Area Chief Information Officers (CIOs) or Chief Information Security Officers (CISOs);
- State Fusion Center;
- Statewide Interoperability Coordinator (SWIC);
- Public safety (i.e., fire service, law enforcement, emergency medical services, and emergency managers);
- Public health officials and other appropriate medical practitioners and/or hospitals;
- Individuals representing educational institutions such as K-12 schools and higher education, public and/or private;
- Critical infrastructure sector/owner/operator representatives (public and private); and
- Nonprofit, faith-based, and other voluntary organizations such as the American Red Cross.

The purpose and responsibilities of the CSPC include the following:

- Supporting the development, implementation, revision, and approval of the Hawai'i Statewide Cybersecurity Strategy and Implementation Plan;
- Integrating county government members into cybersecurity planning activities;
- Organizing a cohesive planning network aimed at constructing and executing cybersecurity preparedness initiatives using Cybersecurity and Infrastructure Security Agency (CISA) and Federal Emergency Management Agency (FEMA) resources, as well as other federal, state, local, private sector, and community resources;



- Facilitating the identification of funding priorities while also collaborating with other committees and similar entities to enhance coordination and minimize redundant efforts;
- Ensuring investments support closing capability gaps or sustaining capabilities through the Threat and Hazard Identification and Risk Assessment/Stakeholder Preparedness Review (THIRA/SPR) and the Nationwide Cybersecurity Review (NCSR) scorecard; and,

The SLCGP Subcommittee will ultimately oversee the implementation of the Hawai'i Statewide Cybersecurity Strategy and Implementation Plan. This includes:

- Providing guidance and expertise to the planning of the strategy;
- Maintaining version control of the plan, making updates as needed;
- Tracking implementation of this plan through identified metrics;
- Overseeing funding allocation and distribution; and,
- Supporting any other reporting needs, as required.



Cybersecurity Program Goals and Objectives

Hawai'i's cybersecurity goals and objectives include the following listed in Table 1 below. The SLCGP Subcommittee will be responsible for oversight of all goals and objectives and OHS will be responsible for the implementation of each goal and objective. Specific organizations responsible for the implementation of each goal and objective are included in the table.

Table 1: Cybersecurity Program Goals and Objectives

Cybersecurity Program Goals and Objectives				
Program Goal	Program Objectives		Oversight Responsibility	Implementer Responsibility
1. Conduct a capability / cyber maturity assessment (gap assessment / maturity model) to understand Hawai'i's current cybersecurity readiness posture and identify opportunities to enhance safety and security.	1.1	Identify opportunities to develop asset (e.g., devices, data, software) protections and recovery actions to prioritize them based on the asset's criticality and business value.	SLCGP Subcommittee	Subrecipients/ implementing agencies; OHS (supporting via grant funding)
	1.2	Ensure State and County agencies understand their current cybersecurity posture and areas for improvement based on continuous testing, education, evaluation, and structured assessments.		
	1.3	Conduct ongoing inventory of physical devices, systems, software platforms, and applications across Hawai'i.		



Cybersecurity Program Goals and Objectives

Program Goal	Program Objectives		Oversight Responsibility	Implementer Responsibility
	1.4	Ensure cybersecurity risks to different organizations' operations and assets across Hawai'i are well understood.		
	1.5	Perform vulnerability scans and develop and implement a risk-based vulnerability management plan.		
	1.6	Implement security protections commensurate with risk.		
	1.7	Reduce gaps identified through assessment and planning processes and apply increasingly sophisticated security protections commensurate with risk.		
2. Establish a formal governance structure at the state to oversee the planning and implementation of Hawai'i's Cybersecurity Program.	2.1	Develop and establish appropriate governance structures for Hawai'i's Cybersecurity Program.	SLCGP Subcommittee	OHS; subrecipients/ implementing agencies, as supporting
	2.2	Implement a program to evaluate the maturity and effectiveness of Hawai'i's Cybersecurity Program aligned to Cybersecurity Performance Goals		



Cybersecurity Program Goals and Objectives

Program Goal	Program Objectives	Oversight Responsibility	Implementer Responsibility
	established by CISA, the National Institute of Standards and Technology (NIST), and the Center of Internet Security (CIS).		
3. Establish a Statewide Cybersecurity Workforce Development Strategy and Implementation Plan.	3.1 Develop and provide the resources needed for County agencies to adopt fundamental cybersecurity best practices, in accordance with the Statewide Cybersecurity Workforce Development Strategy and Implementation Plan.	SLCGP Subcommittee	OHS; subrecipients/ implementing agencies, as supporting
	3.2 Assist organizations with having access to an appropriate number of staff members with the fundamental knowledge and skills necessary to recognize cybersecurity risks and understand their roles and responsibilities within established cybersecurity policies, procedures, and practices.		
	3.3 Ensure that organizations across Hawai'i can adopt the National Initiative for		



Cybersecurity Program Goals and Objectives

Program Goal	Program Objectives	Oversight Responsibility	Implementer Responsibility
	Cybersecurity Education (NICE) Cybersecurity Workforce Framework.		
	3.4 Explore collaborative and cooperative purchasing opportunities for cybersecurity products and services for cost-savings.		
4. Further clarify the roles and responsibilities of cybersecurity partners across Hawai'i and enhance coordination and communication mechanisms between these partners.	4.1 Ensure the appropriate capabilities are in place to monitor assets, identify cybersecurity incidents, and ensure those are communicated across Hawai'i.	SLCGP Subcommittee	OHS; subrecipients/ implementing agencies, as supporting
	4.2 Ensure processes are in place to action insights on cybersecurity incidents derived from deployed capabilities.		
	4.3 Facilitate entity efforts to develop, implement, or revise cybersecurity plans, including cyber disruption response plans, with clearly defined roles and responsibilities.		
	4.4 Facilitate entity efforts to ensure appropriate processes are in place for		



Cybersecurity Program Goals and Objectives

Program Goal	Program Objectives		Oversight Responsibility	Implementer Responsibility
		state and county partners to respond to events, document root causes, and share information and lessons learned with other stakeholders.		
5. Develop and implement a robust cybersecurity training program to enhance awareness of cybersecurity threats and hazards as well as Hawai'i's organizational structure for responding to cybersecurity incidents.	5.1	Ensure implementors and the SLCGP Subcommittee understand the state's and relevant entities' current cybersecurity posture and areas for improvement based on continuous testing, education, evaluation, and structured assessments.	SLCGP Subcommittee	OHS; subrecipients/ implementing agencies, as supporting via grant funding
	5.2	Ensure cybersecurity risks to operations and assets are well understood across the state.		
	5.3	Ensure organizations and personnel are appropriately trained in cybersecurity, commensurate with responsibility.		
	5.4	Facilitate training availability for personnel to have the fundamental knowledge and skills		



Cybersecurity Program Goals and Objectives

Program Goal	Program Objectives		Oversight Responsibility	Implementer Responsibility
		necessary to recognize cybersecurity risks and understand their roles and responsibilities within established cybersecurity policies, procedures, and practices.		
6. Develop and implement a robust cybersecurity exercise program to test and evaluate cybersecurity plans, policies, and procedures more effectively.	6.1	Collaborate with relevant entities to develop and field cybersecurity-focused exercise opportunities to test cybersecurity plans.	SLCGP Subcommittee	OHS; subrecipients/ implementing agencies, as supporting via grant funding
	6.2	Assist relevant entities in understanding their current cybersecurity posture and areas for improvement based on continuous testing, education, evaluation, and structured assessments.		



Cybersecurity Plan Essential Elements

As part of the SLCGP, the Federal government developed a Cybersecurity Plan Template as a tool for entities to develop their cybersecurity plan. This template includes the following elements:

1. Manage, Monitor, and Track
2. Monitor, Audit, and Track
3. Enhance Preparedness
4. Assessment and Mitigation
5. Incident Response Best Practices and Methodologies
6. Continuity of Operations
7. Safe Online Services / Collaborative Cyber Information Sharing
8. Workforce
9. Continuity of Communications and Data Networks
10. Assess and Mitigate Cybersecurity Risks and Threats to Critical Infrastructure and Key Resources (CIKR)
11. Cyber Threat Indicator Information Sharing
12. Leverage CISA Resources
13. IT / Operational Technology (OT) Cybersecurity Technology Modernization Review
14. Cybersecurity Risk and Threat Strategies
15. Rural Communities
16. Distribute funds, items, services, capabilities, or activities to local governments

The sections below briefly describe these elements and how they are applied across Hawai'i.

1. Manage, Monitor, and Track

IT partners in the Hawai'i State Government are responsible for creating an enterprise data strategy, supporting the sharing and accessibility of state data, and ensuring data is leveraged and used as assets, such as understanding patterns to determine strategic



projections. There are specific teams that focus on providing high-quality delivery of enterprise support services to the Hawai'i State Government and educational institutions.

The Office of Enterprise Technology Services (ETS) was established by Hawai'i Revised Statutes §27-43. ETS is headed by a full-time chief information officer (CIO) to organize, manage, and oversee statewide information technology. The chief information officer is appointed by the governor and reports directly to the governor. ETS services are provided to Hawai'i Executive Branch agencies. ETS oversees a Services-Oriented Infrastructure (SOI), also known as shared services, involving the management of enterprise-shared services centrally to leverage economies of scale (e.g., network, data management, unified communications, data center, and various cloud services).

2. Monitor, Audit, and Track

IT partners in the Hawai'i State Government are also responsible for providing secure and reliable technology infrastructure for Hawai'i. This includes, but is not limited to, the following:

- **Business Application Services** provide specialized business application design and support for platforms or applications compatible with any cloud infrastructure, such as cloud-native and cloud-agnostic design solutions. This includes providing mainframe system administration, database management, script maintenance and execution, data storage, disaster recovery, account management, security services, and application interfaces.
- The **Systems** teams design, implement, and support operating systems, software, and data storage environments for all state-centralized servers and infrastructure. They provide system administration and application support for Active Directory, email, digital data backup, virtual application, the server environment, web and database application hosting, and cloud hosting services. This team also actively monitors enterprise systems, ensuring unexpected problems are reported, and services are restored promptly.

3. Enhance Preparedness

The Hawai'i Office of Homeland Security (OHS) leads the statewide effort to coordinate federal, state, and county agencies to prepare, prevent, respond to, recover from, and mitigate the effects of cyber incidents. OHS promotes collaboration between the respective cyber functions and emergency management expertise of various entities. The State of Hawai'i Cyber Disruption Response Plan (CDRP) establishes the framework State



Government will use to organize and coordinate its response activities for a coordinated approach to responding to cyber disruptions that impact our state. This CDRP, an Incident Annex to the State Emergency Operations Plan, outlines organizations, actions, and responsibilities of state and county departments and agencies and identifies how they will work together to ensure the state is prepared to execute a well-coordinated, timely and consistent cyber disruption response. It is intended to be a living document that evolves and improves as the outcomes of ongoing planning efforts, exercises, and real-world events are incorporated. It is intended to be a living document that evolves and improves as the outcomes of ongoing planning efforts, exercises, and real-world events are incorporated. This plan was written in accordance with Hawai'i Revised Statutes (HRS) Chapters 128A (Homeland Security) and 128B (Cybersecurity) and applies to all state departments including agencies, offices, institutions of higher education, commissions, boards, and councils. This plan was developed to adhere to federal standards, including the National Incident Management System (NIMS) and the Incident Command System (ICS) structure. Adherence to such standards will help Hawai'i take a coordinated and unified approach to enhance cybersecurity preparedness capabilities.

4. Assessment and Mitigation

Proactive preparedness measures serve as highly effective solution in reducing the consequences of a cybersecurity incident The Hawai'i Statewide Cybersecurity Strategy and Implementation Plan plays a crucial role in this regard by facilitating ongoing evaluations and examinations of cybersecurity strategies. Beyond these annual assessments, organizations across Hawai'i are also urged to revisit and revise their plans as required in the aftermath of significant cybersecurity incidents.

5. Incident Response Best Practices and Methodologies

Through the creation of the Hawai'i Statewide Cybersecurity Strategy and Implementation Plan, the planning team developed the following recommendations and best practices related to cybersecurity. This list is not exhaustive but includes some high-level recommendations any partner can take to promote cybersecurity. The SLCGP Subcommittee will continue to develop and refine this list as part of the expansion of Hawai'i's Cybersecurity Program:

- 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 use of known/fixed/default passwords and credentials;
- Ensure the ability to reconstitute systems (backups);
- Migration to the .gov internet domain;
- NIST Cybersecurity Framework;
- NIST's cyber chain supply risk management best practices;
- Knowledge bases of adversary tools and tactics;
- Adopt a cybersecurity framework;
- Ensure the integrity of process control systems;
- Secure Protected Critical Infrastructure Information (PCII);
- Leverage CIS Services (e.g., CIS Benchmarks (workstation, server, cloud, and network hardening guidelines), Multi-State Information Analysis Center (MS-ISAC) enrollments);
- Maintain citizen confidence; and,
- Exercise Emergency Response Plans.

Additionally, ETS established a set of seven strategic priorities for the state's IT strategy which guide and inform the Hawai'i Cybersecurity Strategy and Implementation Plan and the projects highlighted within:

1. **Partner for Successful Outcomes:** Shape the partnership between government functions and IT by creating a standard framework to ensure successful outcomes.
2. **Expand Statewide Cyber Security Strategy:** Extend the statewide cyber security strategy to protect the State's IT infrastructure and constituent data through adoption of cyber security industry best practices across the State's IT systems.
3. **Enhance the Value of State Data:** Maximize the value of State data by designing, implementing and governing State systems for data stewardship, sharing, and public use.
4. **Optimize Enterprise Systems:** Optimize ETS enterprise systems to leverage the state's investment of centralized IT services.



5. **Extend IT Portfolio Governance:** Extend the State IT Governance Model to better align the state’s functions with resources and ensure the State follows industry best practices and garners the full benefits of its investments.
6. **Implement Dynamic and Sustainable IT Operations:** Implement dynamic and sustainable IT operations to ensure business systems are up-to-date and ready to support the current and future needs of business users and citizens at all times.
7. **Digital Workforce Development:** Establish a continuous learning culture and growth mindset to modernize how we work and enable the state to develop and sustain the digital workforce needed in a constantly evolving IT world.¹

NIST Principles

This Hawai'i Statewide Cybersecurity Strategy and subsequent referenced plans throughout this document use NIST as a framework to develop recommendations, projects, and initiatives. Adopting this framework and using its industry best practices encourages a unified message in this plan and documents that will be developed in the future based on this Hawai'i Statewide Cybersecurity Strategy.

Supply Chain Risk Management

Through implementing the Hawai'i Statewide Cybersecurity Strategy, the SLCGP Subcommittee will continue to work to mitigate supply chain risk management issues. This will include developing and socializing purchasing standards in accordance with FEMA/DHS and other grant guidance, requirements, and regulations as well as other established standards and best practices.

Tools and Tactics

This Hawai'i Statewide Cybersecurity Strategy encourages developing and using cybersecurity tools and tactics, such as information-sharing platforms, situational awareness portals, communication processes, etc.. Through these tools, entities across Hawai'i will gain a greater knowledge of cybersecurity preparedness, prevention, response, recovery, and mitigation efforts.

¹ <https://ets.hawaii.gov/wp-content/uploads/2019/06/1.-State-IT-Strategic-Plan-Overview-Presentation-6182019-dgm.pdf>



6. Continuity of Operations

The initiative of securing efficient practices of continuity of cybersecurity operations across Hawai'i will take place through training, education, and exercises. The categories of this Hawai'i Statewide Cybersecurity Strategy that support this essential element are coordination and collaboration, planning, training and education, and exercises.

7. Safe Online Services / Collaborative Cyber Information Sharing

The Hawai'i Statewide Cybersecurity Strategy aims to secure safe online services for cybersecurity efforts, such as information sharing and situational awareness, by developing frameworks, processes, and associated platforms that promote threat intelligence sharing across Hawai'i. This will be done by first securing funds, then by developing the information-sharing portal, and lastly, by socializing and advertising this new initiative to entities across Hawai'i.

8. Workforce

The SLCGP Subcommittee aims to train and educate appropriate personnel on cybersecurity best practices and increase cybersecurity talent across Hawai'i. The Hawai'i Statewide Cybersecurity Strategy consists of projects that support this element through encouraging training and exercises, as well as establishing college funding assistance and programs that may assist in securing additional cybersecurity talent for Hawai'i.

9. Continuity of Communications and Data Networks

The projects within this Hawai'i Statewide Cybersecurity Strategy aim to enhance and secure the continuity of systems and infrastructures, such as routes of communication and data networks. The projects supporting this essential element fall under the categories of training and education as well as exercises. Through these projects, Hawai'i will create programs to educate and test entities on their communication platforms and data networks.

10. Assess and Mitigate Cybersecurity Risks and Threats to CIKR

Because cybersecurity threat advances have been increasing in severity and frequency, efforts to prepare for, respond to, and recover from these events must also advance. By



doing so, these efforts will improve Hawai'i's cybersecurity mitigation posture. Hawai'i aims to achieve these efforts by maximizing its CIKR capabilities as outlined in the projects in this Cybersecurity Strategic Plan.

11. Cyber Threat Indicator Information Sharing

The Hawai'i State Government closely collaborates with federal partners for threat intelligence and information sharing. The Hawai'i State Fusion Center (HSFC) is a Hawai'i State government program under OHS that facilitates intelligence sharing between county, state, and federal agencies, and the public and private sectors. It is uniquely structured to empower front-line law enforcement, public safety, fire service, emergency response, public health, critical infrastructure partners, and private sector security personnel to understand local implications of national intelligence, thus enabling county officials to better protect their communities. The HSFC collects tips, leads, and other threat information through suspicious activity reporting (SAR). It conducts analysis, disseminates intelligence, and provides training and technology resources. The top priorities for the HSFC are counter terrorism and cyber security.

12. Leverage CISA Services

Hawai'i currently leverages free federal cybersecurity resources and plans to continue to promote and share these resources and services with other state, regional, public, and private partners. Some counties and state organizations also participate in the NCSR. One objective of Hawai'i's Cybersecurity Program includes encouraging more partners across Hawai'i to elect to participate in the NCSR.

- Cybersecurity Performance Goals (CPGs): baseline set of cybersecurity practices broadly applicable across critical infrastructure with known risk-reduction value.
- CISA Cyber Hygiene: Enrollment in CISA's Cyber Hygiene services. Enrollment will be required for recipients and sub-recipients of SLCGP funding.
- National Cybersecurity Review (NCSR): Completion of the NCSR, a self-assessment survey designed to help SLTT organizations evaluate their cybersecurity processes. Completion of the NCSR will be required for recipients and sub-recipients of SLCGP funding.



13. IT / OT Cybersecurity Technology Modernization Review

The Hawai'i Statewide Cybersecurity Strategy projects support the modernization review process that ensures alignment between IT / OT cybersecurity objectives by establishing formal partnerships with sector partners conducting joint IT / OT security planning with Hawai'i.

- **IT:** Systems that use, store, retrieve, send, and process information.
- **OT:** Industrial control systems, including hardware and software, which manage, monitor, and cause physical changes to systems such as water, power, fuels, wastewater, mechanical, industrial, safety, and other systems and processes.

14. Cybersecurity Risk and Threat Strategies

The Hawai'i Statewide Cybersecurity Strategy consists of projects that aim to address its cybersecurity risks and threats by developing and coordinating strategies that include consultation with local governments and statewide entities. All the relevant projects and initiatives that support these essential elements fall under either training and education or coordination and collaboration.

15. Rural Communities

One project in this plan focuses specifically on funding cybersecurity projects at the local level, including rural communities (in accordance with the most recent Hawai'i State Data Center report on Urban and Rural Areas in the State of Hawai'i by County). This is a critical priority for Hawai'i, given that these local and rural communities support several critical infrastructure sectors. As such, it is essential to ensure that they are engaged in cybersecurity projects to ensure adequate access to resources, information, technology, and funding to build their local readiness and preparedness against cyber threats.

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

In compliance with SLCGP requirements, Hawai'i will pass through at least 80% of the federal funds provided under the grant. With the consent of the recipients, this pass-through may be in the form of in-kind services, capabilities, or activities, or a combination of funding and other services. This 80% goal is reflected in proposed projects and funding estimations.



SLCGP Grant Requirements

This section of the Plan describes each of the 16 SLCGP grant requirements that must be addressed through the plan and proposed projects.

The SLCGP requirements include the following:

1. Manage, Monitor, and Track Systems, Applications, and User Accounts
2. Monitor, Audit, and Track Network Activity
3. Enhance the Preparation, Response, and Resilience of Information Systems, Applications, and User Accounts
4. Implement a Process of Continuous Cybersecurity Vulnerability Assessments and Threat Mitigation Practices
5. Ensure that State and Local Governments Adopt and Use Best Practices and Methodologies to Enhance Cybersecurity
6. Promote the Delivery of Safe, Recognizable, and Trustworthy Online Services Through the Use of the '.gov' Internet Domain
7. Ensure Continuity of Operations in the Event of a Cyber Incident, Including Conducting Exercises
8. Use the NICE Workforce Framework to Identify Gaps in Workforces, Enhance Recruitment and Retention, and Bolster Knowledge / Abilities of Personnel to Address Risks and Threats
9. Ensure Continuity of Communication and Data Networks Within the State in the Event of an Incident Involving Those Networks
10. Assess and Mitigate Cybersecurity Risks and Threats Relating to CIKR
11. Enhance Capabilities to Share Cyber Threat Indicators and Related Information
12. Leverage Cybersecurity Services Offered by CISA
13. Implement an IT / OT Modernization Review Process that Ensures Alignment Between IT and OT Cybersecurity Objectives
14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats
15. Ensure rural communities have adequate access to, and participation in plan activities
16. Distribute Funds, Items, Services, Capabilities, or Activities to Local Governments



1. Manage, Monitor, and Track Systems, Applications, and User Accounts

This element includes the knowledge and experience of IT and cybersecurity professionals in the internal assessment process, which identifies security gaps at the operations level of the network using standards-based (i.e., NIST, Cyber Excepted Service (CES), etc.) evaluation criteria. This requirement focuses on a combination of architectural (i.e., systems and applications) and operational (i.e., people) needs.

2. Monitor, Audit, and Track Network Activity

This element helps identify ways in which normal and anomalous activities occur within the operational environment while providing further information on the behavioral analysis efforts by the organization.

3. Enhance the Preparation, Response, and Resilience of Information Systems, Applications, and User Accounts

This element addresses the methods and ways in which the evolution of the environment and operations will occur over time. These enhancements close security gaps and improve resilience and continuity at both the architectural and operational levels. It speaks to the future of operations, training, and exercises.

4. Implement a Process of Continuous Cybersecurity Vulnerability Assessments and Threat Mitigation Practices

The focus of this element is continuous validation; this includes ways in which Hawai'i will implement a program to constantly self-assess its security and vulnerabilities as a threat evolves. Continuous validation assesses procedures and checklists over time to ensure they evolve to meet a threat. Moreover, training and exercises are used to validate the effectiveness of changes and improve the security performance of personnel, configuration changes, evolutionary improvements, new tools, and more. All of these are focused inside the lens of an emerging threat as it also evolves.



5. Ensure that State and Local Governments Adopt and Use Best Practices and Methodologies to Enhance Cybersecurity

This element seeks to establish a commonality of standards and lexicon related to the implementation of state and local governments' cybersecurity methodologies. This effort is standards-based and aims to make processes, responses, and reports consistent across localities within states, between states, and from states up through the federal government.

6. Promote the Delivery of Safe, Recognizable, and Trustworthy Online Services Through the Use of the '.gov' Internet Domain

The Federal government has several resources available to state and local governments to assist during a cyber response event. This element allows a state to know the available resources, integrate them into the response process, and provide links to resources to continuously improve security over time – even during steady-state operations.

7. Ensure Continuity of Operations in the Event of a Cyber Incident, Including Conducting Exercises

This element is fundamental to effective cybersecurity operations before, during, and throughout a cybersecurity event. It begins with prevention-based efforts, including user training, configuration, and vulnerability management. It also includes effective response plans, procedures, and reports for information-sharing purposes. It culminates with redundancies and practiced failover and failure, both informed and validated through exercises.

8. Use the NICE Workforce Framework to Identify Gaps in Workforces, Enhance Recruitment and Retention, and Bolster Knowledge / Abilities of Personnel to Address Risks and Threats

The weakest link in the cybersecurity chain continues to be the end user. The element of implementing NICE is an effort to standardize (or at least provide a basic standard for) the training and education of the workforce and to reduce or eliminate the threat from end



users. This requirement specifically serves to identify and close security gaps in the workforce.

9. Ensure Continuity of Communication and Data Networks Within the State in the Event of an Incident Involving Those Networks

This element will utilize the expertise of network operators and defenders at the state level to ensure communications and operational redundancies, effective failover, and continuity during cybersecurity events. By ensuring communications and data access, Hawai'i will be able to meet public safety and service needs. This is a key concern for every state and local government.

10. Assess and Mitigate Cybersecurity Risks and Threats Relating to CIKR

As the cyber threat landscape evolves, cybersecurity defense efforts must also evolve to meet the threat. This requires the continuous validation of the efforts identified above. This element applies to the technologies, critical infrastructures, and key resources that validate operations and provide critical public safety and services.

11. Enhance Capabilities to Share Cyber Threat Indicators and Related Information

Information sharing is essential to effectively close security gaps, defend the environment, and ensure operational continuity. This element focuses on implementing the technologies, communications, and services necessary to maximize information sharing throughout the cybersecurity lifecycle.

12. Leverage Cybersecurity Services Offered by CISA

Similar to promoting hosted services and resources described above, this element focuses on utilizing and sharing federal resources, specifically those at DHS CISA, and with state and local government entities. When properly implemented, these resources provide steady-state threat information, access to funds and resources (i.e., SLCGP) to improve security, and defensive staff and teams to meet cybersecurity staffing shortfalls or expertise



specialties during a cybersecurity event. This includes high-profile events, like participation in DHS' biennial cybersecurity exercise, CYBER STORM, and similar exercise events.

13. Implement an IT / OT Cybersecurity Modernization Review Process that Ensures Alignment Between IT and OT Cybersecurity Objectives

A key component of defensive evolution in any operational environment is modernization. This element addresses the implementation of IT / OT modernization to state and local entities over time. Furthermore, this element combines efforts to improve continuity and reduce potential security gaps.

14. Ensure Adequate Access to and Participation in the Services and Programs Described in the Statewide Cybersecurity Strategy by Rural Areas in the State

In more rural states, such as Hawai'i, it is essential that information, resources, and programs applied at the state level are made available to all county governments and entities regardless of the rural location of the local government. They must also be included in the Hawai'i Statewide Cybersecurity Strategy. This element ensures that local governments and entities are included in the Hawai'i Statewide Cybersecurity Strategy and have the resources to prevent or succeed during a cyber event.

15. Distribute Funds, Items, Services, Capabilities, or Activities to Local Governments

Because state and local governments are connected, a vulnerability or compromise of one entity would potentially affect both parties. Therefore, it is essential that funds, resources, and capabilities are distributed to County governments to maximize the coordinated protection and defense of Hawai'i. This element certifies that the state government provides resources and funds to all to defend the entire operational environment at all levels.



16. Distribute Funds, Items, Services, Capabilities, or Activities To Local Governments

The SLCGP recipient must pass through at least 80% of the federal funds provided under the grant. With the consent of the recipients, this pass-through may be in the form of in-kind services, capabilities, or activities, or a combination of funding and other services.



Cybersecurity Strategic Plan Projects

Overview of Projects

Below is a list of projects Hawai'i plans to execute to improve its cybersecurity preparedness posture. The planning team structured the Hawai'i Statewide Cybersecurity Strategy and Implementation Plan around several key categories, which form the basis of its organizational framework. Each of these categories encompasses one or more projects, and within each project, you will find a breakdown of the work steps necessary for its successful completion. See below for an overview of the structure.

Table 2: Cybersecurity Projects and Categories

Cybersecurity Projects	
Organization	
1.	Expansion and Formalization of the Roles and Responsibilities
2.	Enhance Cybersecurity Workforce Recruitment and Staffing
3.	Develop Purchasing Standards for Cybersecurity Third-Party Vendors
4.	Development and Deployment of a Cyber Response Team (CRT)
5.	Support Funding of Cybersecurity Projects at the County Level
Coordination and Collaboration	
6.	Develop a Framework, Process, and Associated Platforms to Promote Threat Intelligence and Information Sharing Across Hawai'i
7.	Expand Existing and Develop New Relationships With Critical Infrastructure Partners and Private Infrastructure Owners Across Hawai'i and integrate them into Cybersecurity Planning Efforts
8.	Integrate State Executive Leaders and Decision Makers Into Cybersecurity Planning Efforts
9.	Integrate County, Legislative, Judicial Partners, and Decision Makers Into Cybersecurity Planning Efforts



Cybersecurity Projects
10. Expand Existing and Develop New Relationships With Academic Partners Across Hawai'i
Planning
11. Develop Educational Materials on Cybersecurity Insurance
12. Develop and Provide Tailored Cybersecurity Planning Resources to State and County Partners
13. Implement an Annual Assessment Process for Cybersecurity Plans
Training and Education
14. Develop and Implement a Robust Cybersecurity Training Program
Exercises
15. Develop and Implement of a Mature Cybersecurity Exercise Program
Systems and Infrastructure
16. Secure and Enhance Cybersecurity Infrastructure

Additionally, each project contains details for the following:

- Project Description
- Project Type
- Project Work Steps
- SLCGP Requirements Addressed
- Federal Template Elements Addressed
- Project Interdependencies
- Project Initiation Timeline (Project Initiation Timelines are assumed to start after plan approval and acceptance)
- Priority
- Funding Source(s)



Organization

Project #1: Expansion and Formalization of the Roles and Responsibilities of the SLCGP Subcommittee

- **Project Description:** The SLCGP Subcommittee presently manages cybersecurity strategic planning in Hawai'i. To foster continuous and improvement in cybersecurity capabilities, it would be advantageous for the SLCGP Subcommittee to broaden and define its roles and duties while also establishing a structured governance framework to supervise the execution of the 2023 Hawai'i Statewide Cybersecurity Strategy and any forthcoming cybersecurity endeavors.
- **Project Type:** Organization
- **Project Work Steps:**
 - **Work Step #1:** Assign executive leadership for the SLCGP Subcommittee within the Hawai'i State Government and establish a governance structure, including assigning someone to oversee the implementation of the Hawai'i Statewide Cybersecurity Strategy and Implementation Plan.
 - **Work Step #2:** Assign a SLCGP Subcommittee member responsible for organizing all future meetings / engagements.
 - **Work Step #3:** Consider expanding the scope of SLCGP Subcommittee membership to include additional critical infrastructure partners.
 - **Work Step #4:** Further define the roles and responsibilities of SLCGP Subcommittee committee members, voting requirements, and meeting cadence in the SLCGP Subcommittee Charter.
 - **Work Step #5:** Identify and establish SLCGP Subcommittee sub-committees, which will each oversee specific technical or oversight areas related to implementing this plan.
- **SLCGP Requirements Addressed:**
 - Enhance the Preparation, Response, and Resilience of Information Systems, Applications, and User Accounts
 - Ensure that State and Local Governments Adopt and Use Best Practices and Methodologies to Enhance Cybersecurity
- **Federal Template Elements Addressed:**
 - Enhance Preparedness
- **Project Interdependencies:** Project #7



- **Project Initiation Timeline:** 6 Months
- **Priority:** Medium
- **Funding Source(s):** SLCGP

Project #2: Enhance Cybersecurity Workforce Recruitment and Staffing

- **Project Description:** The SLCGP Subcommittee should establish a sub-committee to develop potential courses of action for bridging the skills gap and recruiting IT and cybersecurity professionals with required knowledge and expertise to include conducting a gap analysis of skills needed and enhancing the cyber workforce in Hawai'i. This specific project refers to recruiting cybersecurity staff at the state and county levels for daily / steady-state activities. This could be accomplished through different partnerships with other state, county, and academic partners.
- **Project Type:** Organization
- **Project Work Steps:**
 - **Work Step #1:** Conduct a baseline staffing gap analysis and annual survey, based on industry best practices and standards, to understand current and potentially desired staffing levels and skills.
 - **Work Step #2:** Pilot programs to encourage increased cybersecurity recruiting through initiatives (e.g., college tuition assistance program).
 - **Work Step #3:** Leverage academic programs in Hawai'i to support workforce development within cybersecurity.
- **SLCGP Requirements Addressed:**
 - Use the NICE Workforce Framework to Identify Gaps in Workforces, Enhance Recruitment and Retention, and Bolster Knowledge / Abilities of Personnel to Address Risks and Threats
- **Federal Template Elements Addressed:**
 - Workforce
- **Project Interdependencies:** N / A
- **Project Initiation Timeline:** 12 Months
- **Priority:** High
- **Funding Source(s):** SLCGP & Other Funding



Project #3: Develop Purchasing Standards for Cybersecurity Third-Party Vendors

- **Project Description:** State and county entities throughout Hawai'i procure the services of cybersecurity third-party vendors through inconsistent processes and procedures. Hawai'i has the potential to aid its diverse partners by establishing procurement standards for these third-party vendors based on ETS guidelines and reinforcing information security in vendor communications. This guidance would be applicable to all hardware, products, and services.
- **Project Type:** Organization
- **Project Work Steps:**
 - **Work Step #1:** Develop and socialize purchasing standards for cybersecurity services utilizing ETS guidelines.
 - **Work Step #2:** Identify safe modes of communication (i.e., Traffic Light Protocols (TLP)²) for coordinating and sharing information with third-party vendors.
- **SLCGP Requirements Addressed:**
 - Distribute Funds, Items, Services, Capabilities, or Activities to Local Governments
- **Federal Template Elements Addressed:**
 - Enhance Preparedness
- **Project Interdependencies:** N / A
- **Project Initiation Timeline:** 2-3 Years
- **Priority:** Low
- **Funding Source(s):** SLCGP

Project #4: Development and Deployment of a Cyber Response Team (CRT)

- **Project Description:** A CRT would spearhead cybersecurity response efforts in Hawai'i. To sustain the advancement and bolstering of cybersecurity response capabilities in the state, it would be advantageous to engage in additional planning to define the roles, responsibilities, and available resources of the CRT Team. Furthermore, it is crucial to disseminate this information among state and county partners.
- **Project Type:** Organization

² <https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage>



- **Project Work Steps:**
 - **Work Step #1:** Refine response activities, roles, responsibilities, and resources that can be brought to bear by the CRT with regional representatives.
 - **Work Step #2:** Identify opportunities to socialize this information with state and county partners.
 - **Work Step #3:** Develop CRTs to provide cybersecurity support to state and county partners, including steady-state preparedness and response support.
- **SLCGP Requirements Addressed:**
 - Ensure that State and County Governments Adopt and Use Best Practices and Methodologies to Enhance Cybersecurity
 - Develop and Coordinate Strategies to Address Cybersecurity Risks and Cybersecurity Threats
- **Federal Template Elements Addressed:**
 - Best Practices and Methodologies
- **Project Interdependencies:** Project #16
- **Project Initiation Timeline:** 12 Months
- **Priority:** High
- **Funding Source(s):** SLCGP & Other Funding

Project #5: Support Funding of Cybersecurity Projects at the County Level

- **Project Description:** Hawai'i presently supports substantial cybersecurity planning efforts at the state level. Nevertheless, there are opportunities to delve deeper into the cybersecurity requirements of county partners, which is particularly crucial since county governments function within resource-limited settings and cannot replicate the structures used at the state level.
- **Project Type:** Organization
- **Project Work Steps:**
 - **Work Step #1:** Ensure County and underrepresented rural community partners are effectively integrated into cybersecurity planning initiatives.
 - **Work Step #2:** Host IT / cybersecurity / tech summits on a regular basis to promote collaboration and networking. Aspects of these engagements could specifically focus on identifying and addressing the needs of county partners and rural communities.



- **Work Step #3:** Coordinate closely with county, and rural partners to identify opportunities for potential funding to support cybersecurity-related initiatives in compliance with SLCGP funding requirements.
- **Work Step #4:** Support Counties with remedying capability gaps identified in assessments.
- **SLCGP Requirements Addressed:**
 - Assess and Mitigate Cybersecurity Risks and Threats Relating to CIKR
 - Enhance Capabilities to Share Cyber Threat Indicators and Related Information
 - Ensure Adequate Access to and Participation in the Services and Programs Described in the State of Hawai'i Cybersecurity Strategic Plan by Rural Areas in the State
 - Leverage Cybersecurity Services Offered by CISA
- **Federal Template Elements Addressed:**
 - Assess and Mitigate Cybersecurity Risks and Threats to CIKR
 - Cybersecurity Risk and Threat Strategies
 - Rural Communities
 - Leverage CISA Resources
- **Project Interdependencies:** N / A
- **Project Initiation:** 12 Months
- **Priority:** High
- **Funding Source:** SLCGP

Coordination and Collaboration

Project #6: Develop a Framework, Process, and Associated Platforms to Promote Threat Intelligence and Information Sharing Across Hawai'i

- **Project Description:** Hawai'i should aim to enhance the sharing of threat intelligence and information with essential federal, state, regional, county, and private sector collaborators. Establishing a structured framework, along with relevant procedures and the identification of information-sharing platforms, will foster a collective understanding of threats and promote cooperation on significant cybersecurity challenges and issues.
- **Project Type:** Coordination and Collaboration
- **Project Work Steps:**



- **Work Step #1:** Fund monitoring software for the Hawai'i State Fusion Center (HSFC) that is accessible to stakeholders and partners across Hawai'i as appropriate.
- **Work Step #2:** Expand capabilities to include a cybersecurity-specific resource portal for authorized personnel to find information on risk management and other aspects of cybersecurity.
- **Work Step #3:** Reinforce and expand Hawai'i's cyber threat intelligence sharing initiatives through the HSFC.
- **Work Step #4:** Support entities with remedying information-sharing gaps identified in assessments.
- **SLCGP Requirements Addressed:**
 - Promote the Delivery of Safe, Recognizable, and Trustworthy Online Services Through the Use of the '.gov' Internet Domain
 - Implement a Process of Continuous Cybersecurity Vulnerability Assessments and Threat Mitigation Practices
 - Enhance Capabilities to Share Cyber Threat Indicators and Related Information
 - Develop and Coordinate Strategies to Address Cybersecurity Risks and Cybersecurity Threats
- **Federal Template Elements Addressed:**
 - Safe Online Services
 - Enhance Preparedness
 - Cyber Threat Indicator Information Sharing
- **Project Interdependencies:** N / A
- **Project Initiation Timeline:** 12 Months
- **Priority:** High
- **Funding Source(s):** SLCGP

Project #7: Expand Existing and Develop New Relationships With Critical Infrastructure Partners and Private Infrastructure Owners Across Hawai'i

- **Project Description:** Hawai'i should seek to broaden and strengthen its current partnerships while also building new relationships with essential critical infrastructure partners and private infrastructure owners. These efforts will facilitate further collaboration on cybersecurity preparedness initiatives.
- **Project Type:** Coordination and Collaboration
- **Project Work Steps:**



- **Work Step #1:** Enhance integration of critical infrastructure partners with Hawai'i cybersecurity initiatives by including infrastructure partners in planning and resource-sharing efforts and encouraging their use of CISA cybersecurity resources such as free vulnerability assessments³.
- **Work Step #2:** Determine the feasibility of establishing additional seats for critical infrastructure partners in the SLCGP Subcommittee.
- **Work Step #3:** Establish formal partnerships and / or a working group with water sector partners to conduct joint IT / OT security planning with Hawai'i.
- **Work Step #4:** Establish formal partnerships and / or a working group with energy sector partners (Essential Support Function (ESF) #12 – electricity) to include critical lifelines such as water/wastewater, transportation, and communications) to conduct joint IT / OT security planning with Hawai'i.
- **Work Step #5:** Establish formal partnerships and / or a working group with election security partners (physical and cybersecurity) to conduct joint IT / OT security planning with Hawai'i.
- **Work Step #6:** Conduct critical infrastructure interdependency study and share with relevant stakeholders.
- **SLCGP Requirements Addressed:**
 - Implement an IT / OT Cybersecurity Modernization Review Process that Ensures Alignment Between IT and OT Cybersecurity Objectives
 - Enhance the Preparation, Response, and Resilience of Information Systems, Applications, and User Accounts
 - Ensure that State and Local Governments Adopt and Use Best Practices and Methodologies to Enhance Cybersecurity
 - Enhance Capabilities to Share Cyber Threat Indicators and Related Information
- **Federal Template Elements Addressed:**
 - IT and OT Modernization Review
 - Enhance Preparedness
 - Best Practices and Methodologies
 - Cyber Threat Indicator Information Sharing
- **Project Interdependencies:** N / A

³ <https://www.cisa.gov/resources-tools/resources/cisas-free-cyber-vulnerability-scanning-water-utilities>



- **Project Initiation Timeline:** 6 Months
- **Priority:** Medium
- **Funding Source(s):** SLCGP & Other Funding

Project #8: Integrate State Executive Leaders and Decision Makers into Cybersecurity Planning Efforts

- **Project Description:** To guarantee that cybersecurity remains a top priority in Hawai'i, it is essential to enhance the integration of executive leaders and decision-makers into cybersecurity planning endeavors. Furthermore, executive roles and responsibilities related to cybersecurity incidents should be clearly delineated and integrated into training and exercise programs.
- **Project Type:** Coordination and Collaboration
- **Project Work Steps:**
 - **Work Step #1:** Conduct bi-annual exercises for executive leaders and decision-makers to test and enhance their cybersecurity skills / knowledge.
 - **Work Step #2:** Work with legislators to define criteria for decision-making processes concerning cybersecurity.
 - **Work Step #3:** Identify roles and responsibilities of the Governor's Office in cybersecurity incidents, especially within critical infrastructure.
- **SLCGP Requirements Addressed:**
 - Ensure Continuity of Operations in the Event of a Cyber Incident, Including Conducting Exercises
 - Ensure that State and Local Governments Adopt and Use Best Practices and Methodologies to Enhance Cybersecurity
 - Enhance Capabilities to Share Cyber Threat Indicators and Related Information
- **Federal Template Elements Addressed:**
 - Enhance Preparedness
 - Best Practices and Methodologies
 - Cyber Threat Indicator Information Sharing
- **Project Interdependencies:** Project #9 and Project #15
- **Project Initiation Timeline:** 12 Months
- **Priority:** Medium
- **Funding Source(s):** SLCGP & Other Funding



Project #9: Integrate County, Legislative, Judicial Partners, and Decision Makers into Cybersecurity Planning Efforts

- **Project Description:** To ensure the acquisition of funding for cybersecurity initiatives and to enhance security, it is crucial to better incorporate county governments, legislative partners, judicial collaborators, and other executive decision-makers into cybersecurity planning. This integration can aid in the identification and procurement of funding opportunities, while also ensuring the inclusion of relevant partners in cybersecurity efforts.
- **Project Type:** Coordination and Collaboration
- **Project Work Steps:**
 - **Work Step #1:** Work with elected officials and judicial partners to explore funding options for cybersecurity projects.
 - **Work Step #2:** Identify a list of other cybersecurity funding opportunities.
 - **Work Step #3:** Work with elected officials and Hawai'i Department of Defense (DOD) to validate procedures for how the Hawai'i Army National Guard (HING) will be engaged during cybersecurity incidents.
 - **Work Step #4:** Develop educational products to increase cybersecurity knowledge among elected officials.
- **SLCGP Requirements Addressed:**
 - Leverage Cybersecurity Services Offered by CISA
 - Distribute Funds, Items, Services, Capabilities, or Activities to Local Governments
- **Federal Template Elements Addressed:**
 - Leverage CISA Resources
- **Project Interdependencies:** Project #5
- **Project Initiation Timeline:** 2 Years
- **Priority:** Low
- **Funding Source(s):** SLCGP

Project #10: Expand Existing and Develop New Relationships with Academic Partners Across Hawai'i

- **Project Description:** Hawai'i should strive to grow and strengthen its current partnerships, while also creating and nurturing new partnerships, with public education institutions. These efforts will facilitate collaborative engagement in cybersecurity preparedness and workforce development initiatives.



- **Project Type:** Coordination and Collaboration
- **Project Work Steps:**
 - **Work Step #1:** Enhance integration of academic partners with Hawai'i cybersecurity initiatives by including academic stakeholders in planning and resource-sharing efforts.
 - **Work Step #2:** Conduct outreach to privately-owned educational institutions, as well as private sector vendors to include them in the academic network focused on workforce development.
- **SLCGP Requirements Addressed:**
 - Use the NICE Workforce Framework to Identify Gaps in Workforces, Enhance Recruitment and Retention, and Bolster Knowledge / Abilities of Personnel to Address Risks and Threats
- **Federal Template Elements Addressed:**
 - Workforce
- **Project Interdependencies:** Project #2
- **Project Initiation Timeline:** 12 Months
- **Priority:** Medium
- **Funding Source(s):** SLCGP

Planning

Project #11: Develop Educational Materials on Cybersecurity Insurance

- **Project Description:** Currently, a statewide cyber insurance policy is available to many state organizations. However, there is a general lack of understanding of that policy. Additionally, some state organizations are not covered by this policy (e.g., legislative and judicial branches). Hawai'i could assist state and county partners by providing educational materials around cybersecurity insurance.
- **Project Type:** Planning
- **Project Work Steps:**
 - **Work Step #1:** Develop educational materials and guidance for cyber insurance.
 - **Work Step #2:** Establish a SLCGP Subcommittee that meets on a regular basis to discuss key trends and share information.
- **SLCGP Requirements Addressed:**
 - Enhance the Preparation, Response, and Resilience of Information Systems, Applications, and User Accounts



- **Federal Template Elements Addressed:**
 - Enhance Preparedness
- **Project Interdependencies:** N / A
- **Project Initiation Timeline:** 6 Months
- **Priority:** Low
- **Funding Source(s):** SLCGP

Project #12: Develop and Provide Tailored Cybersecurity Planning Resources to State and County Partners

- **Project Description:** To aid state and county partners in their cybersecurity planning, response, and recovery endeavors, Hawai'i should aim to create and distribute tailored cybersecurity resources, templates, and checklists.
- **Project Type:** Planning
- **Project Work Steps:**
 - **Work Step #1:** Develop a recommended list of key response activities for county jurisdictions to integrate into their own cybersecurity policies, plans, and procedures.
 - **Work Step #2:** Provide templates, tools, and job aids to support the development of cyber response capabilities locally.
 - **Work Step #3:** Create a job aid that includes initial incident notification email templates addressed to Hawai'i State Government partners and the Federal Bureau of Investigation (FBI).
 - **Work Step #4:** Socialize and promote available planning, response, and recovery cybersecurity resources.
- **SLCGP Requirements Addressed:**
 - Enhance the Preparation, Response, and Resilience of Information Systems, Applications, and User Accounts
 - Implement a Process of Continuous Cybersecurity Vulnerability Assessments and Threat Mitigation Practices
 - Ensure that State and Local Governments Adopt and Use Best Practices and Methodologies to Enhance Cybersecurity
 - Ensure Adequate Access to and Participation in the Services and Programs Described in the Hawai'i Statewide Cybersecurity Strategy by Rural Areas in the State
 - Distribute Funds, Items, Services, Capabilities, or Activities to Local Governments



- Develop and Coordinate Strategies to Address Cybersecurity Risks and Cybersecurity Threats
- **Federal Template Elements Addressed:**
 - Enhance Preparedness
 - Best Practices and Methodologies
 - Continuity of Operations
- **Project Interdependencies:** N / A
- **Project Initiation Timeline:** 2 Years
- **Priority:** High
- **Funding Source(s):** SLCGP

Project #13: Implement an Annual Assessment Process for Cybersecurity Plans

- **Project Description:** To promote a culture of continuous improvement, Hawai'i should strive to establish an annual assessment procedure for all cybersecurity-related plans, along with recommended guidelines for the review process. This assessment process may involve the following steps: (1) Incorporating all state cybersecurity response and incident notification best practices, and lessons learned from recent incidents, (2) Updating the roles and responsibilities of each organization during a cybersecurity incident, and (3) Revising their data retention policies.
- **Project Type:** Planning
- **Project Work Steps:**
 - **Work Step #1:** Offer an optional self-cybersecurity risk assessment that aims to identify cybersecurity gaps and capabilities within an organization.
 - **Work Step #2:** Identify efficient and cost-effective ways to update cybersecurity software and hardware and encourage organizations to continuously update and upgrade their software and hardware to meet the current threat environment.
 - **Work Step #3:** Enhance partnerships with ETS for an evaluation of Hawai'i's systems.
 - **Work Step #4:** Conduct more regular audits to identify vulnerable points.
- **SLCGP Requirements Addressed:**
 - Enhance the Preparation, Response, and Resilience of Information Systems, Applications, and User Accounts
 - Implement a Process of Continuous Cybersecurity Vulnerability Assessments and Threat Mitigation Practices



- Ensure Continuity of Communication and Data Networks Within the State in the Event of an Incident Involving Those Networks
- Manage, Monitor, and Track Systems, Applications, and User Accounts
- Monitor, Audit, and Track Network Activity
- **Federal Template Elements Addressed:**
 - Continuity of Operations
 - Assessment and Mitigation
 - Continuity of Communications and Data Networks
 - Manage, Monitor, and Track
 - Monitor, Audit, and Track
- **Project Interdependencies:** N / A
- **Project Initiation Timeline:** 3 Years
- **Priority:** Medium
- **Funding Source(s):** SLCGP

Training and Education

Project #14: Develop and Implement a Robust Cybersecurity Training Program

- **Project Description:** Hawai'i aims to create a robust and all-encompassing cybersecurity training and education program to enhance cybersecurity preparedness. This program will educate various sectors on essential emerging threats and hazards and encompass state and county cybersecurity response plans.
- **Project Type:** Training and Education
- **Project Work Steps:**
 - **Work Step #1:** Conduct ongoing training for stakeholders to evaluate and enhance their cybersecurity skills and knowledge, and raise visibility of training opportunities through the state's Integrated Preparedness Plan.
 - **Work Step #2:** Develop and disseminate a consolidated list of available free federal training.
 - **Work Step #3:** Create an appendix of common cybersecurity events, motives, and threats to add to cybersecurity plans and integrate into training initiatives.
- **SLCGP Requirements Addressed:**



- Use the NICE Workforce Framework to identify gaps in workforces, enhance recruitment and retention, and bolster the knowledge and abilities of personnel to address risks and threats.
- Develop and Coordinate Strategies to Address Cybersecurity Risks and Cybersecurity Threats
- **Federal Template Elements Addressed:**
 - Workforce
- **Project Interdependencies:** Project #15 and Project #2
- **Project Initiation Timeline:** 2 Years
- **Priority:** High
- **Funding Source(s):** SLCGP

Exercises

Project #15: Develop and Implement a Comprehensive Exercise Program

- **Project Description:** Hawai'i should establish a comprehensive cybersecurity exercise program. This program should emphasize the execution of exercises in various cybersecurity topic areas including continuity of operations (COOP), at both the state and county levels. It should also involve leveraging resources that can be shared with stakeholders for them to conduct their own exercises such as through CISA's Tabletop Exercise Packages (CTEPs) program⁴.
- **Project Type:** Exercises
- **Project Work Steps:**
 - **Work Step #1:** Conduct state-level COOP testing in addition to regular exercises.
 - **Work Step #2:** Develop and / or socialize exercise materials that can be leveraged by county partners to assist with conducting their own exercise to evaluate their cybersecurity plans, policies, and procedures.
 - **Work Step #3:** Create a separate set of exercises tailored for state leadership, decision-makers, and legislators.
 - **Work Step #4:** Develop a state-level exercise program that documents requirements for conducting cybersecurity exercises across Hawai'i.

⁴ <https://www.cisa.gov/resources-tools/resources/cybersecurity-scenarios>



- **SLCGP Requirements Addressed:**
 - Ensure Continuity of Operations in the Event of a Cyber Incident, Including Conducting Exercises
 - Implement a Process of Continuous Cybersecurity Vulnerability Assessments and Threat Mitigation Practices
 - Leverage Cybersecurity Services Offered by CISA
- **Federal Template Elements Addressed:**
 - Continuity of Communications and Data Networks
 - Assessment and Mitigation
 - Leverage CISA Resources
- **Project Interdependencies:** Project #14
- **Project Initiation Timeline:** 2 Years
- **Priority:** Medium
- **Funding Source(s):** SLCGP

Systems and Infrastructure

Project #16: Secure and Enhance Connections in Cybersecurity Infrastructure

- **Project Description:** Hawai'i presently provides cybersecurity infrastructure for multiple organizations, benefiting various regional, county, and other partners. Hawai'i should actively explore opportunities to improve these infrastructure systems, aiming for more seamless integration, coordination, streamlining, and regular updates. This effort will secure and enhance connections throughout the state of Hawai'i.
- **Project Type:** Systems and Infrastructure
- **Project Work Steps:**
 - **Work Step #1:** Support broadband and fiber enhancements using the Broadband Equity, Access, and Deployment (BEAD) program.
 - **Work Step #2:** Explore cloud-based system-secure data storage policies.
 - **Work Step #3:** Assess, maintain, and improve existing infrastructure and systems.
 - **Work Step #4:** Create and update a government systems and hardware inventory.
 - **Work Step #5:** Support entities with remedying systems and infrastructure gaps identified in annual assessments.
- **SLCGP Requirements Addressed:**
 - Manage, Monitor, and Track Systems, Applications, and User Accounts



- Monitor, Audit, and Track Network Activity
- Ensure Continuity of Communication and Data Networks Within the State in the Event of an Incident Involving Those Networks
- Enhance the Preparation, Response, and Resilience of Information Systems, Applications, and User Accounts
- **Federal Template Elements Addressed:**
 - Manage, Monitor, and Track
 - Monitor, Audit, and Track
 - Continuity of Operations
 - Enhance Preparedness
- **Project Interdependencies:** Project #5
- **Project Initiation Timeline:** 3 Years
- **Priority:** High
- **Funding Source(s):** SLCGP & Other Funding



Funding and Services

Distribution to Local Governments

In relation to the implementation of this plan, the SLCGP Subcommittee intends to use at least 80% of the funding received through the SLCGP to deliver services, capabilities, and resources to county government entities as described in **Appendix B: Project Summary Worksheet**. As part of the funding process, the SLCGP Subcommittee does intend to provide sub-grants or direct pass-through of funds as part of Hawai'i's Cybersecurity Program as required to meet specific project needs. This would allow passing funds to be distributed to specific county governments supporting cybersecurity-related projects.

This approach, including ensuring that 25% of the grant funding is received as services, capabilities, and resources to rural areas, meets the State and Local Cybersecurity Improvement Act requirement: e.2.B.xvi. This approach also provides Hawai'i the flexibility to maximize cybersecurity benefits to all partners. Appendix B: Project Summary Table provides a high-level overview of funding estimates based on the projects outlined in this plan.



This page intentionally blank



Implementation Plan

Overview

The Implementation Plan serves as a roadmap to steer Hawai'i towards the realization of the strategic timelines, goals, and projects outlined in this plan. To facilitate the execution of the Hawai'i Statewide Cybersecurity Strategy, OHS will be responsible for overseeing and initiating specific projects, and program management will be included in staffing resource plans for grant applications. OHS will be responsible for overseeing the implementation of projects and tracking project progress via established metrics.

The SLCGP Subcommittee through OHS' Statewide Cybersecurity Program management staff will be responsible for setting specific metrics for each project, such as the number of meetings held, amount of feedback received on proposed products, and improved cybersecurity outcomes. OHS will also be responsible for finalizing projects specifics upon initiation, to include detailed funding allocations.

The SLCGP Subcommittee will be responsible for directly coordinating with local and private sector partners to ensure they are appropriately integrated into planning and implementation efforts. The SLCGP Subcommittee will also be responsible for reflecting and advocating for the key interests and priorities on behalf of local and private sector partners.

The SLCGP Subcommittee will focus on coordinating with key emergency management, law enforcement, and IT partners across the Hawai'i State Government to develop guidance and recommendations related to 1) steady-state activities to promote preparedness for cybersecurity incidents and 2) incident response processes following cybersecurity incidents.

Finally, the SLCGP Subcommittee will specifically focus on developing comprehensive, robust, and mature training, education, and exercise plans. They will also be responsible for tracking the implementation of and adherence to each training, education, and exercise plan.



Timeline and Implementation Risks

Given the scale and scope of the projects identified in the Hawai'i Statewide Cybersecurity Strategy, there are inherent risks to both the project timelines and implementation processes. These risks include, but are not limited to:

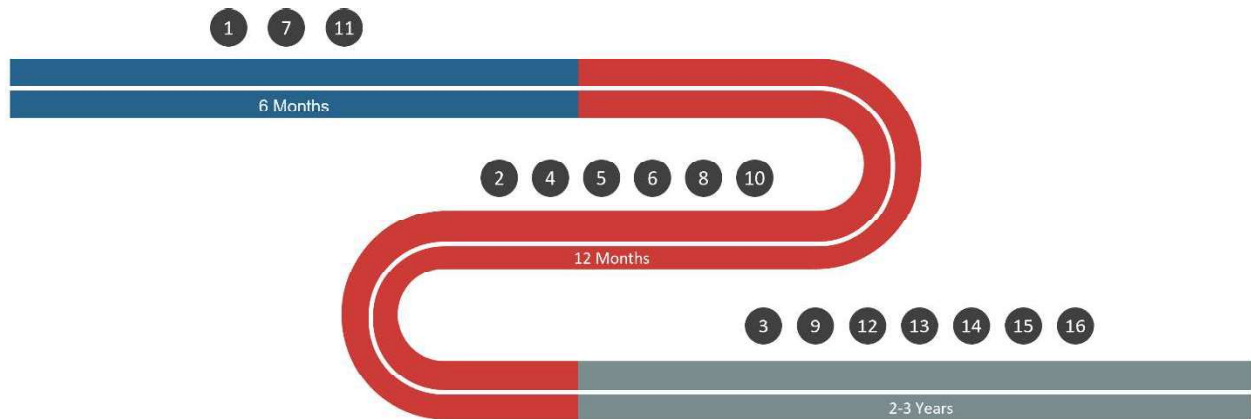
- Lack of state agency or department engagement may stall or impede projects;
- Lack of county engagement and feedback may limit the applicability of projects and narrow the scope of recipients;
- Lack of a detailed timeline that is regularly checked and adhered to may cause projects to be delayed;
- Inaction or lack of coordination between sub-committees may cause duplication of projects or gaps in project success;
- Undue administrative burdens may cause delays in project implementation; and,
- Failure to regularly check and align project budgets may cause significant overages or unused funds.

The SLCGP Subcommittee through OHS's Statewide Cybersecurity Program management staff will be responsible for tracking these risks and developing and implementing mitigation strategies accordingly.



Implementation Roadmap

The Implementation Roadmap on the page that follows provides a graphic representation of projects organized by anticipated completion timeline, giving an overview and outline that can guide the order of SLCGP Subcommittee through OHS's Statewide Cybersecurity Program management staff actions. The Implementation Roadmap can be referenced throughout project implementation and can be modified to meet changing needs or priorities. The Project Worksheets also includes information about critical interdependencies between projects to help align efforts and avoid duplication. This Implementation Roadmap may also be used to help describe the process and intended flow of project implementation.



#	Project Name	Timeframe	#	Project Name	Timeframe
1	Expansion and Formalization of the Roles and Responsibilities of the SLCGP Subcommittee	6 Months	9	Integrate County, Legislative, Judicial Partners, and Decision Makers Into Cybersecurity Planning Efforts	2 Years
2	Enhance Cybersecurity Workforce Recruitment and Staffing	12 Months	10	Expand Existing and Develop New Relationships With Academic Partners Across Hawai'i	12 Months
3	Develop Purchasing Standards for Cybersecurity Third-Party Vendors	2-3 Years	11	Develop Educational Materials on Cybersecurity Insurance	6 Months
4	Continue the Development and Deployment of the CRT Team	12 Months	12	Develop and Provide Tailored Cybersecurity Planning Resources to State and County Partners	2 Years
5	Support Funding of Cybersecurity Projects at the County Level	12 Months	13	Implement an Annual Assessment Process for Cybersecurity Plans	3 Years
6	Develop a Framework, Process, and Associated Platforms to Promote Threat Intelligence and Information Sharing Across Hawai'i	12 Months	14	Develop and Implement a Robust Cybersecurity Training Program	2 Years
7	Expand Existing and Develop New Relationships With Critical Infrastructure Partners and Private Infrastructure Owners Across Hawai'i	6 Months	15	Develop and Implement a Mature Exercise Program	2 Years
8	Integrate State Executive Leaders and Decision Makers Into Cybersecurity Planning Efforts	12 Months	16	Secure and Enhance Connections in Cybersecurity Infrastructure	3 Years

Figure 1: Implementation Roadmap



This page intentionally blank



Appendix A: Cybersecurity Plan Capabilities Assessment

This table assesses Hawai'i's cybersecurity capabilities against the 16 SLCGP-required essential elements. The assessment outlines each essential element and briefly describes how the plan will be used to satisfy each element by leveraging projects. Additionally, the assessment highlights the level of capability for each project that is used to satisfy each essential element. Level of capabilities are as listed: Foundational, Fundamental, Intermediary, or Advanced.

Table 3: Hawai'i Cybersecurity Plan Capabilities Assessment

Hawai'i Cybersecurity Capabilities Assessment			Assessment
Cybersecurity Plan Required Elements	Brief Description of Current Capabilities of State and Local governments within the Eligible Entity	Select capability level from: Foundational Fundamental Intermediary Advanced	Project # (s) <i>(If applicable – as provided in Appendix B)</i>
			Met
1. Manage, monitor, and track information systems, applications, and user accounts	<ul style="list-style-type: none"> Hawai'i is currently seeking input from IT stakeholders and SMEs on how the monitoring, auditing, and tracking of information systems can be improved 	Foundational	13, 16
2. Monitor, audit, and track network traffic and activity	<ul style="list-style-type: none"> Hawai'i is currently seeking input from IT stakeholders and SMEs on how both automated and manual monitoring, 	Foundational	13, 16
			Partial
			Partial



Hawaii Cybersecurity Capabilities Assessment			Assessment
	auditing, and tracking efforts can be improved		
3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts	<ul style="list-style-type: none"> Hawaii is working to assess existing resources and identify future needed resources. Hawaii is working to assess current training and develop a more comprehensive training program. Hawaii is working to develop cybersecurity resources (e.g., checklists, policies, procedures, & reporting) for state and local partners 	Foundational	1, 7, 11, 12, 13, 16 Partial
4. Implement a process of continuous cybersecurity risk factors and threat mitigation. Practices prioritized by degree of risk	<ul style="list-style-type: none"> Hawaii is working to implement NIST-based protection, alerting, and reporting practices to standardize security operations across state entities using the Federally approved framework. Through the Hawaii Statewide Cybersecurity Strategy, the OHS Statewide Cybersecurity Program management staff is currently creating efforts that support the development of regular trainings and exercises (including both certifications for 	Foundational	6, 12, 13, 15 Partial



Hawaii Cybersecurity Capabilities Assessment		Assessment
	IT professionals and security awareness for authorized users)	
<p>5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST)</p> <ul style="list-style-type: none"> 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 use of known / fixed / default passwords and credentials Ensure the ability to reconstitute systems (backups) Migration to the .gov internet domain 	<p>Hawaii is working to align cybersecurity practices to common frameworks and best practices (e.g., NIST, Cybersecurity Frameworks (CSF)).</p> <p>Hawaii is also seeking to develop cybersecurity resources (e.g., checklists) that are structured off these best practices and frameworks.</p> <p>Hawaii will work to develop training programs to meet NIST framework guidance while meeting Federal regulation requirements for security awareness and IT professionals certifications</p> <p>Hawaii is working to develop exercises to support the identification of security gaps, to test policy & procedural implementation, and to improve reporting</p>	<p>1, 4, 7, 8, 12</p> <p>Foundational</p>
<p>6. Ensure continuity of operations including by conducting exercises</p>	<p>The OHS Statewide Cybersecurity and Critical Infrastructure Resiliency and Security Program management staff is seeking to promote collaboration and</p>	<p>8, 15</p> <p>Intermediary</p>
		Partial



Hawai'i Cybersecurity Capabilities Assessment

Assessment

	<p>planning with critical infrastructure entities (e.g., joint planning, trainings, and exercises).</p> <ul style="list-style-type: none"> Partners across the Hawai'i State Government currently have some continuity plans that exist at all levels of government and within private organizations. Hawai'i State Government is working to identify alternate facilities, connections, and operations for critical public services state-wide 	
<p>7. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain</p>	<ul style="list-style-type: none"> Hawai'i is seeking input from IT / cybersecurity stakeholders and SMEs related to promoting end-user education on safe online services and cyber-security enhancements. Hawai'i is working to develop, socialize, and provide via online resources, a list of strategies and best practices related to cybersecurity based upon the NIST framework 	<p>6</p> <p>Intermediary</p> <p>Partial</p>
<p>8. Use the NICE workforce framework to identify gaps in workforces, enhance</p>	<ul style="list-style-type: none"> Governing groups across the Hawai'i State Government are in close communication about the cybersecurity talent shortage 	<p>2, 10, 14</p> <p>Foundational</p> <p>Partial</p>



Hawai'i Cybersecurity Capabilities Assessment

Assessment

<p>recruitment and retention, and bolster knowledge / abilities of personnel to address risks and threats.</p>	<p>and are creating initiatives to secure a more technologically advanced workforce</p> <ul style="list-style-type: none"> Hawai'i is currently gathering input from state stakeholders and partners to identify gaps in IT professional certifications and standardize a centralized capability to provide access to those certifications to state IT staff 	
<p>9. Ensure continuity of communications and data networks in the event of an incident involving communications or data networks</p>	<ul style="list-style-type: none"> Hawai'i follows relevant response plans (e.g., Hawai'i Cyber Disruption Response Plan) to aid in their communication during different stages and types of cybersecurity incidents. Hawai'i is currently soliciting input from state stakeholders and partners in identifying gaps in security reporting and improving communications for improved security operations. 	<p>Foundational</p> <p>13, 16</p> <p>Partial</p>
<p>10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to CIKR, the degradation of which may impact the performance of information</p>	<ul style="list-style-type: none"> Hawai'i is currently receiving consultation from cybersecurity SMEs on mitigation best practices. Hawai'i is seeking to standardize cybersecurity operations, practices, and reporting using the NIST framework, 	<p>Intermediary</p> <p>5</p> <p>Partial</p>



Hawaii Cybersecurity Capabilities Assessment			Assessment
systems within the jurisdiction of the eligible entity	including for degraded and continuity operational conditions		
11. Enhance capabilities to share cyber threat indicators and related information	<ul style="list-style-type: none"> Hawaii is currently planning to create platforms to support cybersecurity information and threat intelligence sharing. 	Foundational	5, 6, 7, 8 Partial
12. Leverage cybersecurity services offered by CISA	<ul style="list-style-type: none"> OHS facilitates and coordinates with CISA to access resources, both pre-incident and during incident response. Impacted organizations often report to CISA to access resources. CISA is in weekly to daily coordination with OHS. OHS is continuously seeking to identify other services offered by CISA (e.g., assessments, training courses) to promote the statewide readiness posture. Hawaii participates in CISA-led cybersecurity events and exercises. 	Intermediary	5, 9, 15 Partial
13. Implement an IT / Cybersecurity and OT modernization cybersecurity review process that ensures	<ul style="list-style-type: none"> Hawaii is currently seeking input from IT / cybersecurity and OT stakeholders on how to modernize cybersecurity planning and security. 	Foundational	7 Partial



Hawaii Cybersecurity Capabilities Assessment			Assessment
alignment between IT and OT cybersecurity objectives	<ul style="list-style-type: none"> OHS is working to develop a plan / framework for regularly reviewing cybersecurity plans and best practices. 		
14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats	<ul style="list-style-type: none"> Hawaii is working to assess current training and develop a more comprehensive training program that addresses cybersecurity risks and threats. Hawaii is working to develop cybersecurity resources (e.g., checklists) to share with state and local partners. 	Foundational	4, 6, 12, 14 Partial
15. Ensure adequate access to, and participation in, the services and programs described in the Statewide Cybersecurity Strategy by rural areas in the state	<ul style="list-style-type: none"> The four Hawaii counties served on the CSPC and are active members of the SLCGP Subcommittee. They represent rural, suburban, and highly populated areas. The SLCGP Subcommittee, through the implementation of this plan, intends to follow relevant SLCGP funding requirements to ensure ample funds are distributed to rural areas across Hawaii to build cybersecurity preparedness. 	Foundational	5, 12 Partial
16. Distribute funds, items, services, capabilities, or	<ul style="list-style-type: none"> The SLCGP Subcommittee, through the implementation of this plan, intends to follow relevant SLCGP funding 	Intermediary	3, 9, 12 Partial



Hawai'i Cybersecurity Capabilities Assessment			Assessment
activities to local governments	requirements to ensure ample funds are distributed to county governments for various cybersecurity efforts.		



Appendix B: Project Summary Worksheet

The Project Summary Worksheets on the following pages list the cybersecurity projects Hawai'i plans to implement to improve its cybersecurity posture. Below are descriptions of each column within each worksheet.

- **Column 1:** Project number assigned by the entity.
- **Column 2:** Project name.
- **Column 3:** Brief (e.g., one-line) description of the purpose of the project.
- **Column 4:** Targeted initiation timeframe.
- **Column 5:** Funding source (SLCGP, Other Funding, Both).
- **Column 6:** Status of project (future, ongoing, complete).
- **Column 7:** Project priority listing (high, medium, low).

FY22 SLCGP funds are currently being used to plan and implement cybersecurity projects with the State of Hawai'i, with oversight from OHS and the SLCGP Subcommittee. Current funding is detailed below and, where applicable, projects listed below include FY22 SLCGP funds which are currently being used to initiate these efforts.



Table 4: FY22 SLCGP Funding Received and FY2023-25 Estimated Allocations - Hawai'i

	FY 2022	%	FY 2023*	%	FY 2024*	%	FY 2025*	%	FY 2022-2025
Federal Allocation (* anticipated beyond FY22)	\$2,243,539.00	100	\$4,483,000.00	80	\$3,362,000.00	70	\$1,121,000.00	60	\$11,209,539.00
** State Match	Waived	-	\$1,120,750.00	20	\$1,440,857.14	30	\$747,333.33	40	\$3,308,940.47
Total Available	\$2,243,539.00	100	\$5,603,750.00	100	\$4,802,857.14	100	\$1,868,333.33	100	\$14,518,479.47
Grant Administration	\$112,176.95	5	\$280,187.50	5	\$240,142.86	5	\$93,416.67	5	\$725,923.97
Objective 1: Governance and Planning									
<i>Statewide Cybersecurity Plan</i>	\$450,000.00						\$250,000.00		\$700,000.00
<i>Cyber Incident Response Plans</i>	\$100,000.00		\$50,000.00		\$50,000.00		\$50,000.00		\$250,000.00
<i>Cyber Incident Response Exercises</i>	\$91,249.05		\$50,000.00		\$50,000.00		\$50,000.00		\$241,249.05
Objective 2: Assessment and Evaluation									
<i>County/Entity Assessment/Evaluation</i>	\$213,750.00		\$25,000.00		\$25,000.00		\$25,000.00		\$288,750.00
Objective 3: Mitigation									
<i>Notional task until Obj 1, Investment 1 & Obj 2 met</i>	\$848,863.00		\$5,198,562.50		\$4,437,714.28		\$1,149,916.66		\$11,635,056.45
Objective 4: Workforce Development									
<i>Workforce Development Strategy/Implementation Plans</i>	\$427,500.00						\$250,000.00		\$677,500.00



Project Summary Worksheet

1.	2. Project Name	3. Project Description	4. Initiation Timeframe	5. Funding Source	6. Status	7. Priority
Organization						
1	Expansion and Formalization of the Roles and Responsibilities of the SLCGP Subcommittee	The SLCGP, via the temporary planning construct of the CSPC, presently manages cybersecurity strategic planning in Hawai'i. To foster continuous improvement in cybersecurity capabilities, the State will broaden and define the SLCGP Subcommittee's roles and duties while also establishing a structured governance framework to supervise the execution of the 2023 Hawai'i Statewide Cybersecurity Strategy and any forthcoming cybersecurity endeavors.	6 Months	SLCGP	Ongoing	Medium
2	Enhance Cybersecurity Workforce Recruitment and Staffing	The SLCGP Subcommittee should establish a sub-committee to develop potential courses of action for bridging the skills gap and recruiting IT and cybersecurity professionals with required knowledge and expertise to include conducting a gap analysis of skills needed and enhancing the cyber workforce in Hawai'i. This specific project refers to recruiting cybersecurity staff at the state and county levels for daily / steady-state activities. This could be accomplished through different partnerships with other state, county, and academic partners.	12 Months	SLCGP & Other Funding	Future	High
3	Develop Purchasing Standards for Cybersecurity Third-Party Vendors	State and county entities throughout Hawai'i procure the services of cybersecurity third-party vendors through inconsistent processes and procedures. Hawai'i has the potential to aid its diverse partners by establishing procurement standards for these third-party vendors based on ETS guidelines and reinforcing information security in vendor communications. This guidance would be applicable to all hardware, products, and services.	2 – 3 Years	SLCGP	Future	Low



4	Continue the Development and Deployment of the CRT Team	A CRT would spearhead cybersecurity response efforts in Hawai'i. To sustain the advancement and bolstering of cybersecurity response capabilities in the state, it would be advantageous to engage in additional planning to elucidate the roles, responsibilities, and available resources of the CRT Team. Furthermore, it is crucial to disseminate this information among state, county, and local partners.	2 Years	SLCGP & Other Funding	Ongoing	High
5	Support Funding of Cybersecurity Projects at the County Level	Hawai'i presently supports substantial cybersecurity planning efforts at the state level. Nevertheless, there are opportunities to delve deeper into the cybersecurity requirements of county and local partners, which is particularly crucial since numerous county and local governments may function within resource-limited settings.	12 Months	SLCGP	Future	High
Total Estimated Funding: \$873,000 in SLCGP Funding, \$100,000 in FY2022 OHS Funding						



Project Summary Worksheet

1.	2. Project Name	3. Project Description	4. Initiation Timeframe	5. Funding Source	6. Status	7. Priority
Coordination and Collaboration						
6	Develop a Framework, Process, and Associated Platforms to Promote Threat Intelligence and Information Sharing Across Hawai'i	Hawai'i should aim to enhance the sharing of threat intelligence and information with essential federal, state, regional, county, and local collaborators. Establishing a structured framework, along with relevant procedures and the identification of information-sharing platforms, will foster a collective understanding of threats and promote cooperation on significant cybersecurity challenges and issues.	12 Months	SLCGP	Future	High
7	Expand Existing and Develop New Relationships With Critical Infrastructure Partners and Private Infrastructure Owners Across Hawai'i	Hawai'i should seek to broaden and strengthen its current partnerships while also building new relationships with essential critical infrastructure partners and private infrastructure owners. These efforts will facilitate further collaboration on cybersecurity preparedness initiatives.	6 Months	SLCGP & Other Funding	Future	Medium
8	Integrate State Executive Leaders and Decision Makers Into Cybersecurity Planning Efforts	To guarantee that cybersecurity remains a top priority in Hawai'i, it is essential to enhance the integration of executive leaders and decision-makers into cybersecurity planning endeavors. Furthermore, executive roles and responsibilities related to cybersecurity incidents should be clearly delineated and integrated into training and exercise programs.	12 Months	SLCGP & Other Funding	Future	Medium



9	Integrate County, Legislative, Judicial Partners, and Decision Makers Into Cybersecurity Planning Efforts	To ensure the acquisition of funding for cybersecurity initiatives and to enhance security, it is crucial to better incorporate county and local governments, legislative partners, judicial collaborators, and other executive decision-makers into cybersecurity planning. This integration can aid in the identification and procurement of funding opportunities, while also ensuring the inclusion of relevant partners in cybersecurity efforts.	2 Years	SLCGP	Future	Low
10	Expand Existing and Develop New Relationships With Academic Partners Across Hawai'i	Hawai'i should strive to grow and strengthen its current partnerships, while also creating and nurturing new partnerships, with public education institutions. These efforts will facilitate collaborative engagement in cybersecurity preparedness and workforce development initiatives.	12 Months	SLCGP	Future	Medium
Total Estimated Funding: \$960,750 in SLCGP Funding, \$250,000 in FY2022 OHS Funding						



Project Summary Worksheet

1.	2. Project Name	3. Project Description	4. Initiation Timeframe	5. Funding Source	6. Status	7. Priority
Planning						
11	Develop Educational Materials on Cybersecurity Insurance	Currently, a statewide cyber insurance policy is available to many state organizations. However, there is a general lack of understanding of that policy. Additionally, some state organizations are not covered by this policy (e.g., legislative and judicial branches). Hawai'i could assist state, county, and local partners by providing educational materials around cybersecurity insurance.	6 Months	SLCGP	Future	Medium
12	Develop and Provide Tailored Cybersecurity Planning Resources to State and County Partners	To aid state and county partners in their cybersecurity planning, response, and recovery endeavors, Hawai'i should aim to create and distribute tailored cybersecurity resources, templates, and checklists.	2 Years	SLCGP	Future	High
13	Implement an Annual Assessment Process for Cybersecurity Plans	To promote a culture of continuous improvement, Hawai'i should strive to establish an annual assessment procedure for all cybersecurity-related plans, along with recommended guidelines for the review process. This assessment process may involve the following steps: (1) Incorporating all state cybersecurity response and incident notification best practices, (2) Updating the roles and responsibilities of each organization during a cybersecurity incident, and (3) Revising their data retention policies.	3 Years	SLCGP	Future	Medium

Total Estimated Funding: \$581,500 in SLCGP Funding



Project Summary Worksheet

1.	2. Project Name	3. Project Description	4. Initiation Timeframe	5. Funding Source	6. Status	7. Priority
Training and Education						
14	Develop and Implement a Robust Cybersecurity Training Program	Hawai'i aims to create a robust and all-encompassing cybersecurity training and education program to enhance cybersecurity preparedness. This program will educate various sectors on essential emerging threats and hazards and encompass state and county cybersecurity response plans.	2 Years	SLCGP	Future	High

Total Estimated Funding: \$482,000 in SLCGP Funding



Project Summary Worksheet

1.	2. Project Name	3. Project Description	4. Initiation Timeframe	5. Funding Source	6. Status	7. Priority
Exercises						
15	Develop and Implement a Mature Exercise Program	Hawaii'i should establish a comprehensive cybersecurity exercise program. This program should emphasize the execution of exercises in various cybersecurity topic areas including continuity of operations (COOP), at both the state and county levels. It should also involve leveraging resources that can be shared with stakeholders for them to conduct their own exercises such as through CISA's Tabletop Exercise Packages (CTEPs) program.	2 Years	SLCGP	Future	Medium

Total Estimated Funding: \$489,500 SLCGP Funding



Project Summary Worksheet

1.	2. Project Name	3. Project Description	4. Initiation Timeframe	5. Funding Source	6. Status	7. Priority
Systems and Infrastructure						
16	Secure and Enhance Connections in Cybersecurity Infrastructure	Hawaii presently provides cybersecurity infrastructure for multiple organizations, benefiting various regional, county, and local partners. Hawaii should actively explore opportunities to improve these infrastructure systems, aiming for more seamless integration, coordination, streamlining, and regular updates. This effort will secure and enhance connections throughout the state of Hawaii.	3 Years	SLCGP & Other Funding	Future	High
Total Estimated Funding: \$1,180,000 in SLCGP Funding, \$150,000 in FY2022 OHS Funding						



Appendix C: Metrics

The Appendix C Table documents performance measures and metrics for the goals included in this *Statewide Cybersecurity Strategy and Implementation Plan*. As part of the implementation plan, please note that more detailed/impactful metrics will be developed as each project is formally initiated.

Table 5: *Cybersecurity Program Metrics*

Cybersecurity Program Goals, Objectives, and Metrics		
Program Goal	Program Objectives	Metrics
<p>1. Conduct a capability / cyber maturity assessment (gap assessment / maturity model) to understand Hawai'i's current cybersecurity readiness posture and identify opportunities to enhance safety and security.</p>	<p>1.1: Identify opportunities to develop asset (e.g., devices, data, software) protections and recovery actions to prioritize them based on the asset's criticality and business value.</p>	<p>1.1.1. SLCGP Subcommittee creates or adopts an assessment framework and distributes it to local governments for review / edits.</p>
	<p>1.2: Verify State and County agencies understand their current cybersecurity posture and areas for improvement based on continuous testing, education, evaluation, and structured assessments.</p>	<p>1.1.2 SLCGP Subcommittee finalizes the assessment framework and distributes it for annual conduct.</p>
	<p>1.3: Conduct an inventory of government physical devices and systems, as well as software platforms and applications across Hawai'i.</p>	<p>1.1.3 Implementing entities conduct and share with the SLCGP Subcommittee annual assessments utilizing specified framework.</p>
	<p>1.4: Ensure cybersecurity risks to different organizations' operations and assets across Hawai'i are well understood.</p>	
	<p>1.5: Perform vulnerability scans and develop and implement a risk-based vulnerability management plan.</p>	
	<p>1.6: Implement security protections commensurate with risk.</p>	



Cybersecurity Program Goals, Objectives, and Metrics

Program Goal	Program Objectives	Metrics
<p>2. Establish a formal governance structure at the state to oversee the planning and implementation of Hawaii's Cybersecurity Program.</p>	<p>1.7: Reduce gaps identified through assessment and planning processes and apply increasingly sophisticated security protections commensurate with risk.</p> <p>2.1: Develop and establish appropriate governance structures for Hawaii's Cybersecurity Program.</p> <p>2.2: Implement a program to evaluate the maturity and effectiveness of Hawaii's Cybersecurity Program aligned to Cybersecurity Performance Goals established by CISA, NIST, and CIS.</p>	<p>2.1.1 OHS convenes SLCGP Subcommittee to determine a structure for formal governance.</p> <p>2.1.2 OHS and the SLCGP Subcommittee will be given the Implementation Roadmap to use as a checklist for Hawaii's Cybersecurity Program.</p> <p>2.1.3 OHS and the SLCGP Subcommittee will develop regular summary reports (e.g., annually) to summarize implementation progress.</p>
<p>3. Establish a Statewide Cybersecurity Workforce Development Strategy and Implementation Plan.</p>	<p>3.1: Develop and provide the resources needed for County agencies to adopt fundamental cybersecurity best practices, in accordance with the Statewide Cybersecurity Workforce Development Strategy and Implementation Plan.</p> <p>3.2: Assist organizations with having access to an appropriate number of staff members with the fundamental knowledge and skills necessary to recognize cybersecurity risks and understand their roles and responsibilities within established cybersecurity policies, procedures, and practices.</p> <p>3.3: Ensure that organizations across Hawaii can adopt the NICE Cybersecurity Workforce Framework.</p>	<p>3.1.1 OHS convenes SLCGP Subcommittee, and supporting working groups as deemed necessary, to establish a cybersecurity workforce development strategy and implementation planning effort, consisting of elements, such as: staffing gap analysis based on industry best practices and standards; gap analysis to identify and understand outstanding staffing needs; advisory content to support entities in securing more cybersecurity talent; and collaborative summits or engagement opportunities to foster collaboration among professionals.</p>



Cybersecurity Program Goals, Objectives, and Metrics

Program Goal	Program Objectives	Metrics
<p>4. Further clarify the roles and responsibilities of cybersecurity partners across Hawai'i and enhance coordination and communication mechanisms between these partners.</p>	<p>3.4: Explore collaborative and cooperative purchasing opportunities for cybersecurity products and services for cost-savings.</p> <p>4.1: Ensure the appropriate capabilities are in place to monitor assets, identify cybersecurity incidents, and ensure those are communicated across Hawai'i.</p> <p>4.2: Ensure processes are in place to action insights derived from deployed capabilities.</p> <p>4.3: Facilitate entity efforts to develop, implement, or revise cybersecurity plans, including cyber disruption response plans, with clearly defined roles and responsibilities.</p> <p>4.4: Facilitate entity efforts to ensure appropriate processes are in place for County and local partners to respond to events, document root causes, and share information and lessons learned with other partners.</p>	<p>4.1.1 Implementing entities conduct and share with the SLCGP Subcommittee annual assessments utilizing specified framework.</p> <p>4.1.2 Implementing entities develop, implement, or revise cybersecurity plans, including cyber disruption response plans, with clearly defined roles and responsibilities.</p> <p>4.1.3 Implementing entities establish and utilize processes for response, root cause analysis, information sharing, and lessons learned via the SLCGP Subcommittee.</p> <p>4.1.4 OHS, in collaboration with implementing agencies, conduct annual THIRA/SPR-relevant assessments identifying capability and capacity status, gaps, and proposed development activities.</p>
<p>5. Develop and implement a robust cybersecurity training program to enhance awareness of cybersecurity threats and hazards as well as Hawai'i's organizational structure for</p>	<p>5.1: Ensure implementors and the SLCGP Subcommittee understand the state's and relevant entities' current cybersecurity posture and areas for improvement based on continuous testing, education, evaluation, and structured assessments.</p>	<p>5.1.1 OHS, in collaboration with implementing agencies, conduct annual THIRA/SPR-relevant assessments identifying capability and capacity status, gaps, and proposed development activities.</p>



Cybersecurity Program Goals, Objectives, and Metrics

Program Goal	Program Objectives	Metrics
<p>responding to cybersecurity incidents.</p>	<p>5.2: Ensure cybersecurity risks to operations and assets are well understood across the state.</p> <p>5.3: Ensure organizations and personnel are appropriately trained in cybersecurity, commensurate with responsibility.</p> <p>5.4: Facilitate training availability for personnel to have the fundamental knowledge and skills necessary to recognize cybersecurity risks and understand their roles and responsibilities within established cybersecurity policies, procedures, and practices.</p>	<p>5.1.2 Implementing entities communicate risks to operations and assets annually, according to assessment framework, and ad hoc, based on current circumstances/incident impacts.</p> <p>5.1.3 SLCGP Subcommittee (via development of the state's workforce development strategy and implementation plan) develops a recruiting, retention, and training approach based on federal, state, and industry best practices and shares with implementing entities.</p> <p>5.1.4 Implementing entities support and provide input to annual tracking / auditing of trainings needed/completed.</p>
<p>6. Develop and implement a robust cybersecurity exercise program to test and evaluate cybersecurity plans, policies, and procedures more effectively.</p>	<p>6.1: Collaborate with relevant entities to develop and field cybersecurity-focused exercise opportunities to test cybersecurity plans.</p> <p>6.2: Assist relevant entities in understanding their current cybersecurity posture and areas for improvement based on continuous testing, education, evaluation, and structured assessments.</p>	<p>6.1.1 OHS collaborates with implementing entities to develop and field cybersecurity-focused exercises, to include after action/lessons learned feedback."</p> <p>6.1.2 OHS provides and implementing entities support annual tracking / auditing of exercises conducted."</p>



Appendix D: Data Collection Methodology

The section below provides insight into the information-gathering (data collection) process used to identify Hawai'i's cybersecurity capabilities and areas for improvement. The findings from this data collection process informed the projects and recommendations further built out in this Hawai'i Statewide Cybersecurity Strategy.

Document Matrix Review

The Document Matrix Review process consisted of reviewing current cybersecurity preparedness plans, policies, procedures, and protocols for strengths and areas of improvement. The project team provided documents to CSPC members, including the *Hawai'i OHS Cyber Disruption Plan* and the *Hawai'i Information Technology Strategic Plan*.

During the Document Matrix Review process, the project team compared findings to best practices found in the Comprehensive Preparedness Guide (CPG) 101, NIST, and CISA recommended practices. The project team then aligned the findings with SLCGP requirements and built out questions for a statewide Cybersecurity Preparedness Survey and Stakeholder Interviews.

Cybersecurity Preparedness Survey

The project team structured Cybersecurity Preparedness Survey questions around the OHS's areas of interest as well as common patterns identified throughout the Document Review Matrix process. Survey participants responded to 13 cybersecurity preparedness questions. The project team received responses from 16 survey takers.

Stakeholder Interviews

The project team used findings from the Document Review Matrix and Cybersecurity Preparedness Survey to further develop in-depth follow-up questions for Stakeholder Interviews. Nine Stakeholder Interviews were held in-person and virtually and lasted approximately 60 minutes. The project team conducted interviews individually or in small groups so that interviewees would feel comfortable sharing information in a no-fault environment.

The project team interviewed the following organizations:

- Hawai'i Gas



- Hawai'i Health Systems Corporation
- Hawai'i House of Representatives
- Hawai'i Legislative Reference Bureau
- Hawai'i Office of Homeland Security
- Hawai'i State Judiciary
- Hawai'i State Senate
- Office of Hawaiian Affairs



Appendix E: Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR)

Communities across Hawai'i use the THIRA / SPR to assess their risks and set capability targets that reflect their preparedness goals. Communities can use the THIRA / SPR process to better understand how to address their most challenging risks and achieve specific preparedness goals. They can use the results to support a variety of preparedness activities, including planning, training, and exercises. The THIRA / SPR also makes it easier for communities to direct resources where they will be most effective.

THIRA Cybersecurity Results

Hawai'i identifies Cybersecurity Attacks as one of its threats / hazards in its THIRA document. Within the THIRA document, Hawai'i also outlines specific capability targets for different core capabilities and functional areas impacted by a cybersecurity incident. The capability targets provide specific recommendations / steps that must be achieved after a cybersecurity incident. These capability targets reference a specific amount of time or number of days certain steps need to be achieved after a cybersecurity incident occurs.

SPR Overview

Although the SPR does not specifically identify cybersecurity threats in its document, impacted Hawai'i communities of cyber incidents may still use the SPR Tear Sheets to determine the priority and confidence rating of the incident. Priority Ratings reflect how important it is for the community to achieve the capability target or sustain its current capabilities. The priority rating is a selection between high, medium, and low. Confidence Ratings reflect how confident the community is in the accuracy of their reported current capability. The rating ranges from one to five, where a one indicates lower confidence in the estimate and a five indicates a higher confidence. The SPR also instructs impacted communities to identify gaps in five areas: Planning, Organization, Equipment, Training, and Exercises (POETE). This further organizes the next steps and recommendations.



This page intentionally blank



Appendix F: Acronyms

Acronym	Definition
BEAD	Broadband Equity, Access, and Deployment
CDRP	Hawai'i Cyber Disruption Response Plan
CES	Cyber Excepted Services
CIKR	Critical Infrastructure and Key Resources
CIO	Chief Information Officer
CIS	Center of Internet Security
CISA	Cybersecurity and Infrastructure Agency
CISO	Chief Information Security Officer
COOP	Continuity of Operations
CPG	Comprehensive Preparedness Guide
CPGs	Cybersecurity Performance Goals
CSF	Cybersecurity Frameworks
CSPC	Cybersecurity Planning Committee
CRT	Cyber Response Team
CTEPs	CISA Tabletop Exercise Packages
DBEDT	Department of Business, Economic Development, and Tourism
DHS	Department of Homeland Security
DHS	Hawai'i Department of Human Services
DOE	Hawai'i Department of Education
DOH	Hawai'i Department of Health
ESF	Essential Support Function
DOT	Hawai'i Department of Transportation
ETS	Enterprise Technology Services, Office of
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
HSEO	Hawai'i State Energy Office
HING	Hawai'i National Guard
HSFC	Hawai'i State Fusion Center
HRS	Hawai'i Revised Statutes
ICS	Incident Command System
IT	Information Technology
MS-ISAC	Multi-State Information Security Analysis Center



Acronym	Definition
NCSR	Nationwide Cybersecurity Review
NICE	National Initiative for Cybersecurity Education
NIMS	National Incident Management System
NIST	National Institute of Standards and Technology
OHA	Office of Hawaiian Affairs
OHS	Hawai'i Office of Homeland Security
OT	Operational Technology
PCII	Protected Critical Infrastructure Information
POETE	Planning, Organization, Equipment, Training, and Exercises
SANS	SysAdmin, Audit, Network, and Security
SAR	Suspicious Activity Reporting
SLCGP	State and Local Cybersecurity Grant Program
SLTT	State, Local, Tribal, and Territorial
SME	Subject Matter Experts
SPR	Stakeholder Preparedness Review
SWIC	Statewide Interoperability Coordinator
THIRA	Threat & Hazard Identification and Risk Assessment
TLP	Traffic Light Protocol
UH	University of Hawai'i
U.S.	United States
USSS	United States Secret Service
VoIP	Voice Over Internet Protocol



Appendix G: Stakeholders and Contributors

This section lists stakeholders and contributors who either have already contributed to the development of the Hawai'i Statewide Cybersecurity Strategy or who will have a role in overseeing its implementation. This list is broken down into the following groups and is not all inclusive of stakeholders who will be involved in implementation efforts:

- Federal Partners
- Industry Partners
- State Partners
- County / Local Partners
- Higher Education Institutions

Federal Partners

Coast Guard (USCG)

The USCG Cyber Command supports cybersecurity operations in the state by defending Coast Guard cyberspace, enabling Coast Guard operations, and protecting the Maritime Transportation System (MTS).⁵

Cybersecurity and Infrastructure Security Agency (CISA)

CISA operates under DHS and is responsible for strengthening cybersecurity and infrastructure protection across all levels of government, coordinating cybersecurity programs within the U.S., and improving the government's cybersecurity protections against private and nation-state hackers⁶.

Federal Bureau of Investigation (FBI):

The FBI is the lead federal agency for investigating cyber-attacks and intrusions. They collect and share intelligence and engage with victims while working to unmask those

⁵ <https://www.dco.uscg.mil/Our-Organization/CGCYBER/>

⁶ [Cybersecurity and Infrastructure Security Agency - Wikipedia](#)



committing malicious cyber activities. The FBI will work closely with state partners in the event of a cyber-attack to support investigations.⁷

Federal Emergency Management Agency (FEMA):

FEMA supports citizens and emergency personnel to prepare for, protect against, respond to, recover from, and mitigate all hazards, including cyber risks.⁸ FEMA's mission is to reduce the loss of life and property and protect institutions from all hazards, including cyber risks.

Secret Service (USSS)

The USSS's goal is to protect the nation's financial infrastructure and maintain a safe environment for the American people to conduct financial transactions. Its mission is to investigate complex cyber-enabled financial crimes.⁹

Industry Partners

DRFortress

Based in Honolulu, DRFortress is the largest and the only carrier-neutral data center and cloud marketplace operating in Hawai'i. They support needs of Hawai'i's enterprises, content companies, system integrators, carriers, wireless service providers, cable companies and ISPs.¹⁰

Hawaiian Electric Company

Hawaiian Electric serves 95 percent of Hawai'i's 1.4 million residents on the islands of Oahu, Maui, Hawai'i, Lanai and Molokai.¹¹

Hawai'i Gas

Since 1904, Hawai'i Gas has been the only franchised gas utility in the State of Hawai'i. They installed gas pipeline infrastructure, built bulk storage facilities with access to the

⁷ [Cyber Crime — FBI](#)

⁸ [FEMA Strategic Plan: 2022-2026 - Homeland Security Digital Library \(hsdl.org\)](#)

⁹ <https://www.secretservice.gov/investigation/cyber>

¹⁰ <https://www.drfortress.com/about/>

¹¹ <https://www.hawaiianelectric.com/about-us>



harbor, and developed a highly skilled workforce on every major island. Gas energy is a critical part of the fuel mix in Hawai'i.¹²

Hawaiian Telecom

Hawaiian Telcom provides integrated communications, including High-Speed Internet, data, video entertainment, and local and long-distance voice services in Hawai'i.¹³

Kauai Island Utility Cooperative

Kauai Island Utility Cooperative was formed in November of 2002 and operates as a not-for-profit organization that is owned by its members and governed by an elected board of directors.¹⁴

Par Pacific

The Par owns the East refinery, located on the Hawaiian Island of Oahu. The refinery, together with the logistics and retail arms of their Hawai'i operations, provides fuels to a network throughout Hawai'i, and distributes fuels via pipelines on Oahu and on barges to all major harbors in the state.¹⁵

The Queen's Health System

The Queen's Health System is a nonprofit health care organization in Hawai'i. With four hospitals and more than 70 preventive, specialty health care locations and labs it is the state's largest employer.

State Partners

Hawai'i Department of the Attorney General

The Attorney General is the chief legal officer and chief law enforcement officer of the State of Hawai'i. The Attorney General is appointed by the Governor. 180 attorneys and over 500 professional and support personnel assist the Attorney General in fulfilling the responsibilities of the office.

¹² <https://www.hawaiigas.com/about-us>

¹³ <https://www.hawaiiantel.com/aboutus>

¹⁴ <https://www.kiuc.coop/about-us>

¹⁵ <https://www.parpacific.com/operations/refining-logistics/hawaii>



Hawai'i State Department of Education (DOE)

The Hawai'i State Department of Education (DOE) is the state-level agency responsible for overseeing the public education system in the state of Hawai'i. It is the largest single state educational system in the United States. The HIDOE is responsible for managing and operating public schools in Hawai'i, from kindergarten through grade 12, and it serves both students and educators across the state.¹⁶

Hawai'i State Department of Health (DOH)

The Hawai'i State Department of Health (DOH) is responsible for overseeing public health and environmental quality in the state of Hawai'i. The Hawai'i State Department of Health plays a vital role in safeguarding the health and well-being of the people of Hawai'i by addressing a wide range of public health and environmental concerns. It works in collaboration with local communities, healthcare providers, and other stakeholders to fulfill its mission.¹⁷

Hawai'i State Department of Human Services (DHS)

The Hawai'i State Department of Human Services (DHS) is a state government agency responsible for providing a wide range of social services and assistance programs to the residents of Hawai'i. Its primary mission is to promote the well-being and self-sufficiency of individuals and families in need by offering various support services and benefits.¹⁸

Hawai'i State Department of Transportation (DOT)

The Hawai'i Department of Transportation (DOT) is responsible for planning, designing, constructing, operating, and maintaining State facilities and infrastructures in all modes of transportation (land, air, and water). To achieve these objectives, the Department coordinates with other State, County, Federal, and private agencies and programs.¹⁹

Hawai'i Office of Homeland Security (OHS)

The Office of Homeland Security's (OHS) primary responsibility is to enhance Hawai'i's security preparedness and resilience in an integrated, synergistic, relevant, proactive,

¹⁶ <https://www.hawaiipublicschools.org/Pages/Home.aspx>

¹⁷ <https://health.hawaii.gov/about/office-of-the-director/>

¹⁸ <https://humanservices.hawaii.gov/overview/>

¹⁹ <https://hidot.hawaii.gov/about-us/>



flexible, cost effective, full-spectrum effort across all domains in order to prevent, protect, mitigate, respond to and recover from attacks, natural disasters and emerging threats. OHS also manages the Hawai'i State Fusion Center (HSFC), a Hawai'i State government program that facilitates intelligence sharing between local, state, and federal agencies, and the public and private sectors. OHS, in coordination with appropriate entities and individuals, develops, regularly updates, maintains, and exercises adaptable response plans to address cybersecurity risks, including significant cyber incidents as described in the Hawai'i Cyber Disruption Response Plan.²⁰

Hawai'i Army National Guard (HING)

HING serves as the Senior Army National Guard command and control element in support of the JFHQ-State for Army units assigned to the State. HING provides trained, equipped, and ready forces capable of mobilizing in support of both Federal and State Missions.²¹

Hawai'i Judiciary

The Judiciary is one of three branches of state government in Hawai'i. The other two are the executive and legislative branches. As an independent government branch, the Judiciary is responsible for administering justice in an impartial, efficient, and accessible manner according to the law.²²

Hawai'i State Energy Office (HSEO)

The Hawai'i State Energy Office (HSEO) is a government agency within the state of Hawai'i that is dedicated to advancing the state's energy policy and sustainability goals. It operates under the Department of Business, Economic Development, and Tourism (DBEDT) and plays a central role in Hawai'i's efforts to transition to a clean and sustainable energy future.

Hawai'i State Legislature, House of Representatives and Senate

The Hawai'i State Legislature is the legislative branch of the government of the state of Hawai'i, responsible for making and passing laws for the state. It is a bicameral legislature,

²⁰ <https://dod.hawaii.gov/ohs/>

²¹ <https://dod.hawaii.gov/hiarng/about/>

²² https://www.courts.state.hi.us/general_information/general_information



meaning it consists of two separate chambers: the Hawai'i State House of Representatives and the Hawai'i State Senate.²³

Office of Enterprise Services (ETS)

ETS provides governance for executive branch IT projects and seeks to identify, prioritize and advance innovative initiatives with the greatest potential to increase efficiency, reduce waste, and improve transparency and accountability in state government. ETS also supports the management and operation of all state agencies by providing effective, efficient, coordinated and cost-beneficial computer and telecommunication services such that state program objectives may be achieved.²⁴

Office of the Governor

The Hawai'i Office of the Governor is the executive branch of the state government responsible for overseeing the administration of Hawai'i and implementing state laws and policies. The Governor of Hawai'i is the head of the executive branch and serves as the chief executive officer of the state. The Office of the Governor consists of the Governor, the Lieutenant Governor, and their respective staff.²⁵

Office of Hawaiian Affairs

OHA is a semi-autonomous state agency responsible for improving the wellbeing of all Native Hawaiians through advocacy, research, community engagement, land management and the funding of community programs. The agency is governed by a Board of Trustees, made up of nine members who are elected statewide to serve four-year terms and set organizational policy. OHA is administered by a Chief Executive Officer, who is appointed by the Board of Trustees to oversee a staff of about 170 people.²⁶

The HSEO focuses on various aspects of energy policy, conservation, renewable energy, and energy efficiency.²⁷

²³ <https://www.capitol.hawaii.gov/home.aspx>

²⁴ <https://ets.hawaii.gov/about/>

²⁵ <https://governor.hawaii.gov/>

²⁶ <https://www.oha.org/about/>

²⁷ <https://energy.hawaii.gov/who-we-are/>



Higher Education Partners

University of Hawai'i (UH)

As the state's public system of higher education, the University of Hawai'i System includes 3 universities, 7 community colleges and community-based learning centers across Hawai'i. UH is the only provider of public higher education and also owns an employment training center, three university centers, four education centers, and various other research facilities distributed across six islands throughout the state of Hawaii.²⁸

Local Partners

City and County of Honolulu

The City and County of Honolulu, a political and corporate body, consists of the island of Oahu, all other islands not included in any other county, adjacent waters, and is vested with all powers authorized by the State Constitution, the laws of the State of Hawaii, and the Revised Charter of the City and County of Honolulu. The City and County of Honolulu is the most densely populated of five counties within the state of Hawaii, with a population of approximately 905,601. It is organized as a mayor-council type of government in which there is a separation between legislative and executive functions. CSPC representatives from the City and County of Honolulu include the Honolulu Police Department and the Department of Information Technology.^{29,30}

County of Hawai'i

The County of Hawai'i is coextensive of the Island of Hawai'i and has an approximate population of 200,629. Hawai'i County is the largest county in the state in terms of geography. CSPC representatives from the County of Hawai'i include the Department of Information Technology.³¹

²⁸ <https://www.hawaii.edu/about-uh/>

²⁹ <https://www.honolulu.gov/>

³⁰ https://lrb.hawaii.gov/wp-content/uploads/CCHonolulu_guide.pdf

³¹ <https://www.hawaiicounty.gov/our-county>



County of Kaua'i

The County of Kaua'i consists of the islands of Kaua'i, Ni'ihau, Lehua, and Ka'ula. The approximate population is 73,298. CSPC representatives from the County of Kaua'i include the Information Technology Division and the Department of Water Supply.³²

County of Maui

The County of Maui consists of the islands of Maui, Lana'i, Moloka'i (except for a portion of Moloka'i that comprises Kalawao County), Kaho'olawe, and Molokini. The approximate population is 164,754, CSPC representatives from the County of Maui include the Information Technology Services Division.³³

³² <https://www.kauai.gov/Home>

³³ <https://www.mauicounty.gov/>




ESIGNATURE - HawaiiStatewideCyberStrategy _Final_100223 - Revised Final

Final Audit Report

2023-10-03

Created:	2023-10-03 (Hawaii-Aleutian Standard Time)
By:	Glen Badua (glen.m.badua@hawaii.gov)
Status:	Signed
Transaction ID:	CBJCHBCAABAAY2HMhMgMTVnqJfiFNPbSUNnxgPrIsR1Y
Number of Documents:	1
Document page count:	92
Number of supporting files:	0
Supporting files page count:	0

"ESIGNATURE - HawaiiStatewideCyberStrategy_Final_100223 - Revised Final" History

-  Document created by Glen Badua (glen.m.badua@hawaii.gov)
2023-10-03 - 8:49:21 AM HST
-  Document emailed to Vincent Hoang (vincent.hoang@hawaii.gov) for signature
2023-10-03 - 8:50:20 AM HST
-  Agreement viewed by Vincent Hoang (vincent.hoang@hawaii.gov)
2023-10-03 - 8:53:39 AM HST
-  Document e-signed by Vincent Hoang (vincent.hoang@hawaii.gov)
Signature Date: 2023-10-03 - 9:41:08 AM HST - Time Source: server
-  Document emailed to Frank Pace (frank.j.pace@hawaii.gov) for signature
2023-10-03 - 9:41:09 AM HST
-  Email viewed by Frank Pace (frank.j.pace@hawaii.gov)
2023-10-03 - 9:41:31 AM HST
-  Agreement viewed by Frank Pace (frank.j.pace@hawaii.gov)
2023-10-03 - 9:41:52 AM HST
-  Document e-signed by Frank Pace (frank.j.pace@hawaii.gov)
Signature Date: 2023-10-03 - 9:42:43 AM HST - Time Source: server

✔ Agreement completed.

2023-10-03 - 9:42:43 AM HST