Statewide Cybersecurity Program and the State and Local Cybersecurity Grant Program

Office of Homeland Security

Ft. Ruger
Rm 113, Bldg 306
3949 Diamond Head Rd, Honolulu HI 96816

15 October 2024

Agenda

Statewide Cybersecurity Program

Projects Underway (Planning)
- **Cyber Incident Response Plans and Exercises**
- **Workforce Development**

State and Local Cybersecurity Grant Program
- **Eligible Subrecipients**
- **Central Provisioning**
- **Funds Allocations**
- **Project Proposals (Admin and Central)**
- **Subrecipient Investment Project Proposals**
  - **Application Website**

Statewide Cybersecurity Program

Risk	Vulnerability
People	
High: **Increasing possibility of attacks that paralyze critical infrastructure sectors/facilities**, creating far-reaching effects statewide, impact most, if not all, of the population.	High**: Vulnerable populations could be specific agencies/ organizations or groups**, can encompass multiple sectors, critical functions, and create vulnerable populations with impacts.
Property	
High: **Damages are most likely going to be localized.** Property impacts from cyber incidents are increasingly fluid across a broad attack surface implicating multiple sectors/victims.	High: **Industrial control systems**. All critical infrastructure sectors are vulnerable to ransomware attacks, which render systems inoperable temporarily, or permanently.
Environment	
High: **Significant risk to cause damage to human health and the environment** as a result of physical impacts from events such as hazardous material releases, explosions and life-sustaining energy requirements.	High: **All ecosystems that interface with cyber-reliant or cyber-enabled human infrastructure systems** carry potential to sustain environmental impacts from and are vulnerable to cyber attacks.
Continuity / Operations	
Medium: **Cyber attack against government or critical infrastructure** could completely cripple State and local government and/or emergency management operations.	Medium: **Impact to Operational effectiveness of State & Local Govts.** Continuity Plans are not universal across sectors, response effectiveness will be impacted if critical infrastructure also experiences direct or cascading impacts.

Planning and Operations

- Translates the Homeland Security Strategy & Policy guidance into mission execution through the development of operational and response plans to include:
  - **Cyber Incident Response Plan -** incidents affecting computer information systems owned and operated by the State of Hawaiʻi.
  - **Cyber Disruption Response Plan -** incident/s that is/are likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.
  - **Hawaii Statewide Cybersecurity Strategy and Implementation Plan** - Articulated multi-year vision for building and strengthening cybersecurity capabilities across the state through 16 specific cybersecurity projects for priority SLCGP funding consideration

Fusion Center

- Facilitates state-wide information and intelligence sharing on Homeland Security matters between local, state, and federal agencies, and the public and private sectors.
  - Manages interactions with a variety of **Information Sharing and Analysis Centers (ISACs)** help critical infrastructure owners and operators protect their facilities, personnel and customers from cyber and physical security threats and other hazards.
  - ISACs collect, analyze and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency. ISACs reach deep into their sectors, communicating critical information far and wide and maintaining sector-wide situational awareness.

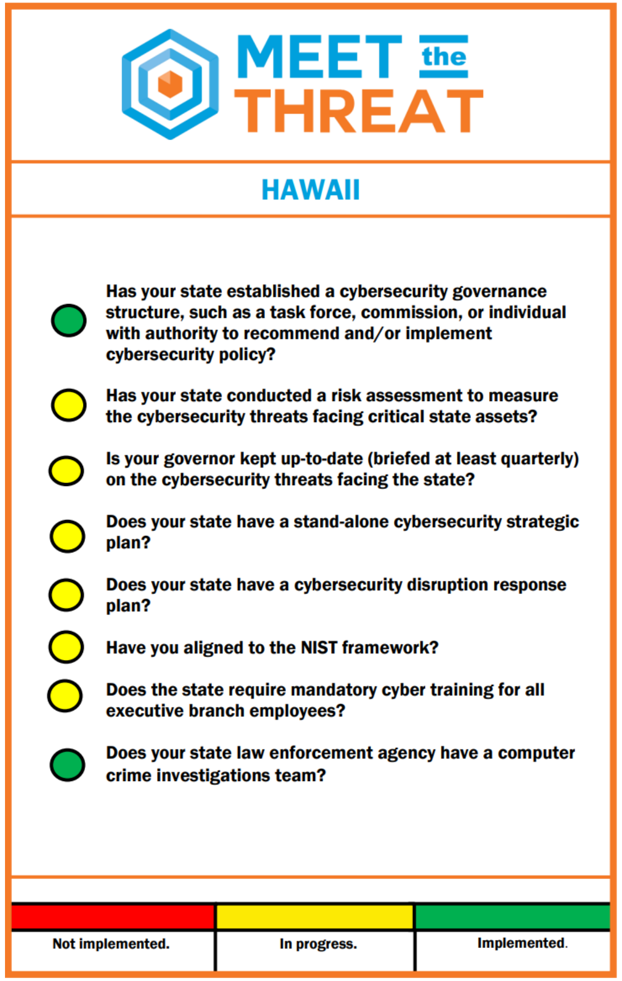
Grants Management

- Supports prevention, protection, response, recovery and mitigation in the areas of planning, equipment, training and exercises throughout the state and county jurisdictions. Allocations of Homeland Security Grant Program funding under the (previous) cybersecurity national priority to date:

Recipient	2017	2018	2019	2020	2021	Total
State	$55,662	$76,000	$30,000	$150,000	$0	$311,662
City & County of Honolulu	$0	$574,390	$580,000	$600,000	$985,000	$2,739,390
Maui County	$700,000	$350,000	$100,000	$100,000	$345,187	$1,595,187
Kauai County	$0	$450,000	$0	$0	$0	$450,000
Hawaii County	$343,206	$125,000	$0	$0	$0	$468,206
Total	$1,098,868	$1,575,390	$710,000	$850,000	$1,330,187	$5,564,445

OBJECTIVES

- **Dedicated State Cybersecurity Agency**
- **State Response Plans**
  - Incidents
  - Disruptions
  - Business Continuity
- **State Critical Infrastructure Program**
- **Defined cybercrime legislation**
- **Vibrant cybersecurity ecosystem** – mobilizing stakeholders to:
  - Tap into cybersecurity market opportunities
  - Develop capabilities of cybersecurity professionals and cybersecurity training providers
  - Create cybersecurity citizen-awareness
  - Reward excellence in cybersecurity
  - Inspire entrepreneurs to innovate
  - Support cutting-edge research
  - Motivate students to pursue cybersecurity careers



MEET the THREAT

HAWAII

- 🟢 **Has your state established a cybersecurity governance structure, such as a task force, commission, or individual with authority to recommend and/or implement cybersecurity policy?**
- 🟡 **Has your state conducted a risk assessment to measure the cybersecurity threats facing critical state assets?**
- 🟡 **Is your governor kept up-to-date (briefed at least quarterly) on the cybersecurity threats facing the state?**
- 🟡 **Does your state have a stand-alone cybersecurity strategic plan?**
- 🟡 **Does your state have a cybersecurity disruption response plan?**
- 🟡 **Have you aligned to the NIST framework?**
- 🟡 **Does the state require mandatory cyber training for all executive branch employees?**
- 🟢 **Does your state law enforcement agency have a computer crime investigations team?**

🟥	🟨	🟩
Not implemented.	**In progress.**	**Implemented.**

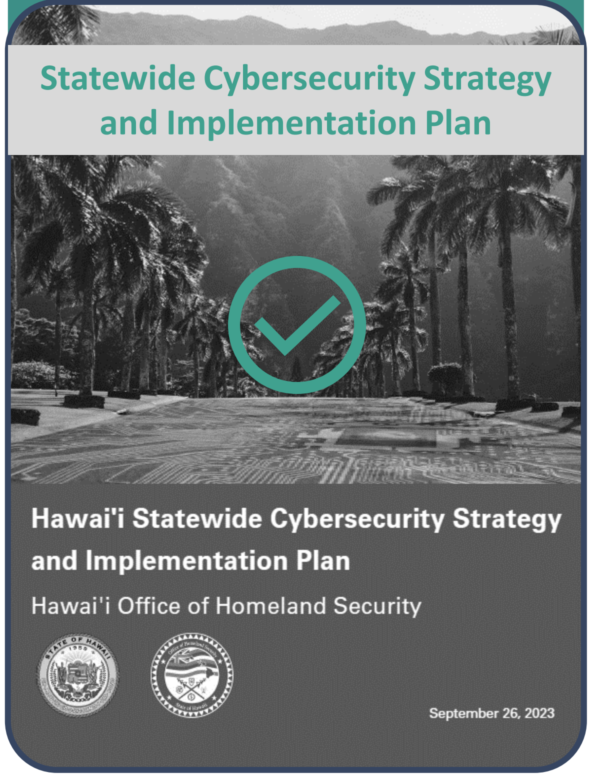
Projects Underway: Cyber Incident Response Plans and Exercises; Workforce Development

Purpose

Provide an update on OHS planning efforts related to the Cybersecurity Workstream

Cyber Workstream

Objective 3



Statewide Cybersecurity Strategy and Implementation Plan

Hawai'i Statewide Cybersecurity Strategy and Implementation Plan

Hawai'i Office of Homeland Security

September 26, 2023

Objective 4

Subrecipient Cyber Incident Response Plans

Develop subrecipient Cyber Incident Response Plans:

- Synchronize to the State Cyber Disruption Response Plan and model after the Office of Enterprise Technology Services Cyber Incident Response Plan
- Develop and implement field county/entity Cyber Incident Response Plan Exercises

Objective 5

Statewide Cyber Workforce Development Strategy

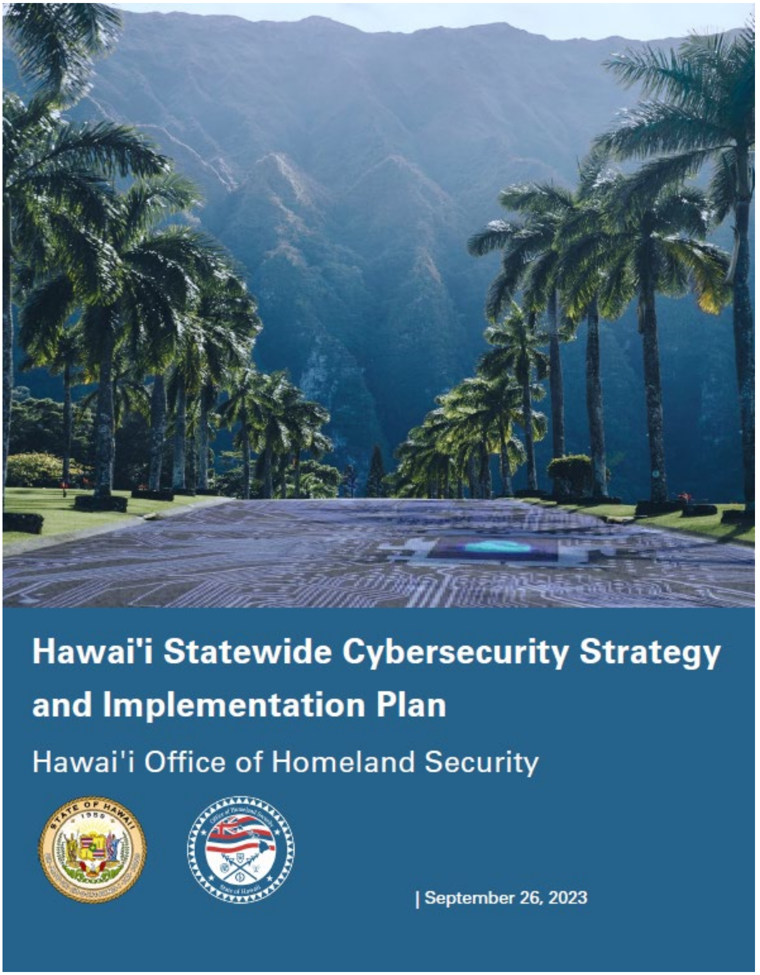
Develop Statewide Cyber Workforce Development Strategy and County/Entity Level Implementation Plans:

- Establish continuous testing, evaluation, and structured assessments approach
- Define data gathering schema and metrics
- Establish strategic relationships with ongoing Hawaii workforce efforts

Obj. 3 Project Scope

Develop Statewide Cybersecurity Strategy and Implementation Plan:

- Aligned with DHS guidance for the State and Local Cybersecurity Grant Program (SLCGP)
- Articulated multi-year vision for building and strengthening cybersecurity capabilities across the state
- Proposed 16 cybersecurity projects for potential future SLCGP funding
- Submitted prior to 29 September deadline; approved by DHS in October



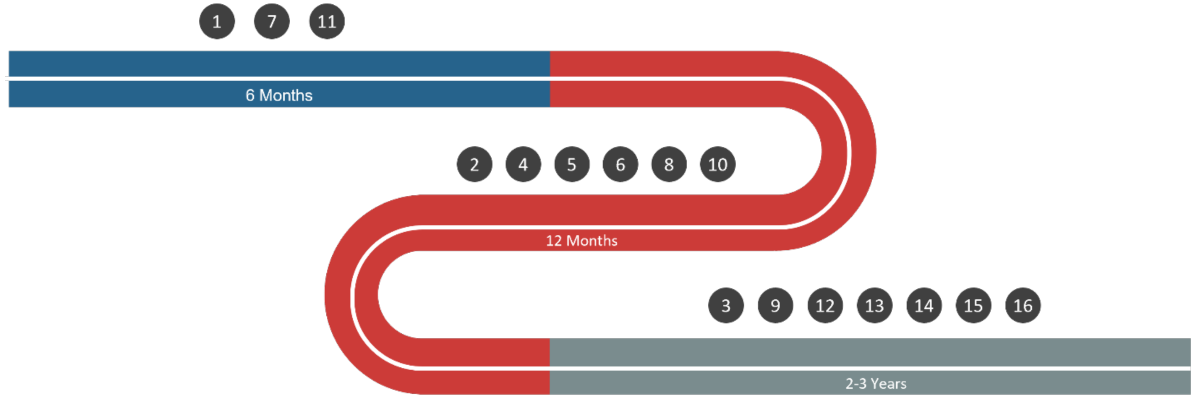
Hawai'i Statewide Cybersecurity Strategy and Implementation Plan

Hawai'i Office of Homeland Security

| September 26, 2023

Obj. 3 Implementation Plan

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.



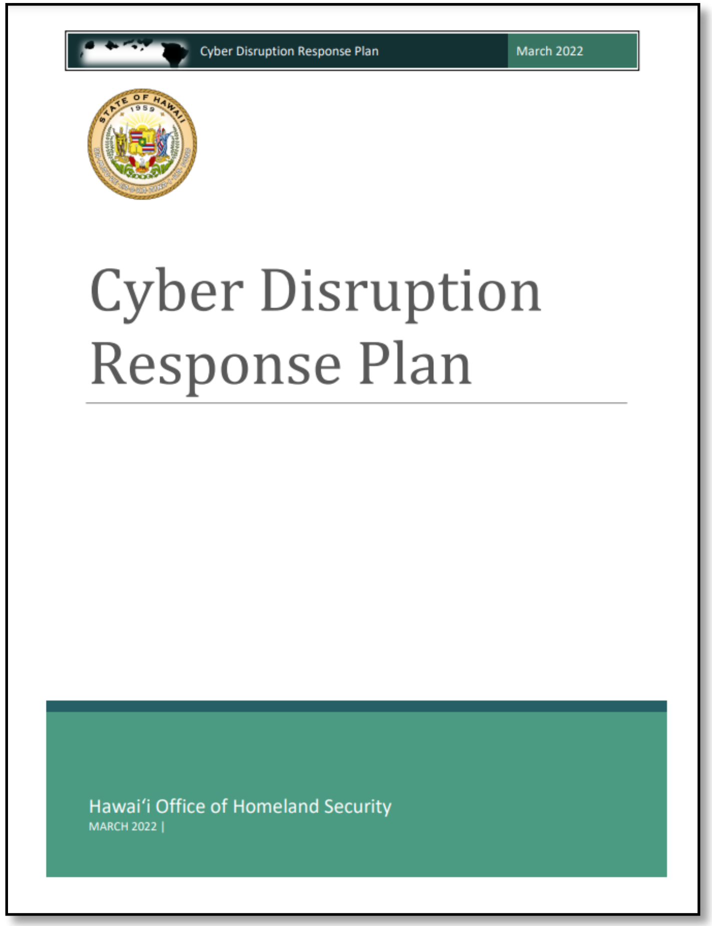
#	Project Name	Timeframe
1	Expansion and Formalization of the Roles and Responsibilities of the SLCGP Subcommittee	6 Months
2	Enhance Cybersecurity Workforce Recruitment and Staffing	12 Months
3	Develop Purchasing Standards for Cybersecurity Third-Party Vendors	2-3 Years
4	Continue the Development and Deployment of the CRT Team	12 Months
5	Support Funding of Cybersecurity Projects at the County Level	12 Months
6	Develop a Framework, Process, and Associated Platforms to Promote Threat Intelligence and Information Sharing Across Hawai'i	12 Months
7	Expand Existing and Develop New Relationships With Critical Infrastructure Partners and Private Infrastructure Owners Across Hawai'i	6 Months
8	Integrate State Executive Leaders and Decision Makers Into Cybersecurity Planning Efforts	12 Months

#	Project Name	Timeframe
9	Integrate County, Legislative, Judicial Partners, and Decision Makers Into Cybersecurity Planning Efforts	2 Years
10	Expand Existing and Develop New Relationships With Academic Partners Across Hawai'i	12 Months
11	Develop Educational Materials on Cybersecurity Insurance	6 Months
12	Develop and Provide Tailored Cybersecurity Planning Resources to State and County Partners	2 Years
13	Implement an Annual Assessment Process for Cybersecurity Plans	3 Years
14	Develop and Implement a Robust Cybersecurity Training Program	2 Years
15	Develop and Implement a Mature Exercise Program	2 Years
16	Secure and Enhance Connections in Cybersecurity Infrastructure	3 Years

Obj. 4 Project Scope

Develop Subrecipient Cyber Incident Response Plans:

1. Synchronize to the State Cyber Disruption Response Plan and model after the Office of Enterprise Technology Services Cyber Incident Response Plan
2. Develop and implement field county/entity Cyber Incident Response Plan Exercises



Cyber Disruption Response Plan March 2022

Cyber Disruption Response Plan

Hawaiʻi Office of Homeland Security
MARCH 2022 |

Next Steps: CIRP Plan

- **Complete:** Working Group review and comment on draft plan
- **In-Progress:** Routing final draft for final approval/signature
- **October-November:** Technical assistance sessions for subrecipients

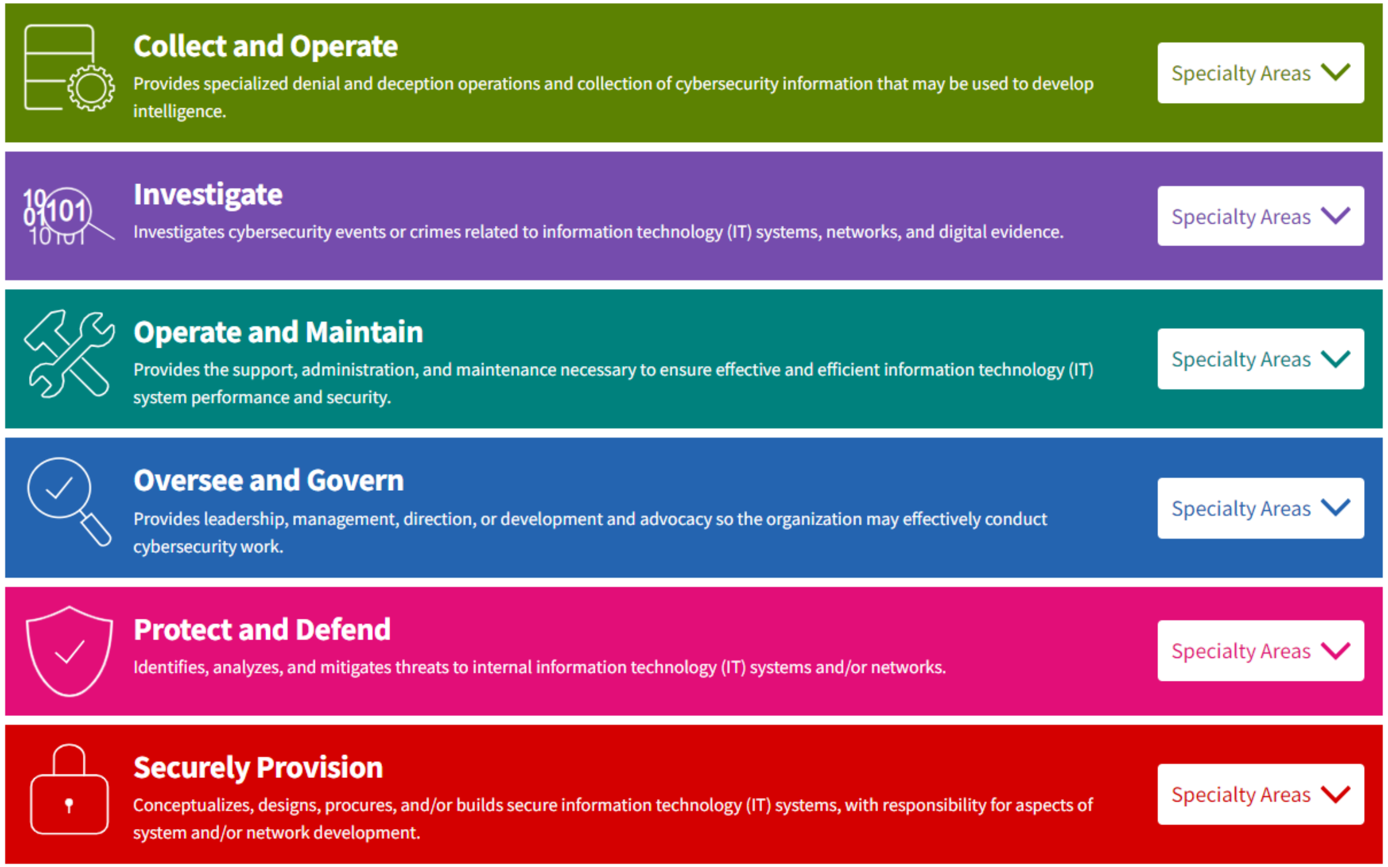
Next Steps: CIRP Exercises

- **In-Progress:** Logistical planning (e.g., venue search, etc.)
- **October-November:** Participant outreach
- **November-January:** Exercise Planning
- **January:** Tabletop exercises targeted for last week in January 2025

Obj. 5 Project Scope

Develop Statewide Cyber Workforce Development Strategy and County/Entity Level Implementation Plans:

- Establish continuous testing, evaluation, and structured assessments approach
- Define data gathering schema and metrics
- Establish strategic relationships with ongoing Hawaii workforce efforts



Collect and Operate

Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.

Specialty Areas

Investigate

Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

Specialty Areas

Operate and Maintain

Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.

Specialty Areas

Oversee and Govern

Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.

Specialty Areas

Protect and Defend

Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.

Specialty Areas

Securely Provision

Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.

Specialty Areas

Workforce Strategy Contents

EDUCATION AND TRAINING

Defining programs for education, training, and certifications to equip individuals with the necessary cybersecurity skills.

RECRUITMENT AND RETENTION

Developing strategies to attract and retain talent in the cybersecurity field.

CONTINUOUS LEARNING AND DEVELOPMENT

Promoting ongoing learning and professional development within the cybersecurity workforce to keep pace with evolving threats and technologies.

PARTNERSHIPS AND COLLABORATION

Engaging with industry partners, government agencies, academic institutions, and professional organizations to share knowledge, best practices, and resources for collective growth and development.

ADAPTABILITY AND FLEXIBILITY

Creating a workforce that can adapt to changing cybersecurity landscapes and emerging technologies by fostering a culture of innovation, agility, and adaptability.

DIVERSITY AND INCLUSION

Encouraging diversity and inclusivity in the cybersecurity workforce to bring in different perspectives and ideas.

Next Steps: Cyber Workforce Development Strategy

- **In-Progress:** OHS review of first draft
- **September 27:** Working Group review of first draft
- **October 2:** Next Working Group meeting
- **November:** Finalize workforce strategy

State and Local Cybersecurity Grant Program

Purpose

Provide a forward-looking overview of coming activities under the Statewide Cybersecurity Program, founded on recent SLCGP Subcommittee decisions regarding Eligible Subrecipients, Central Provisioning, and Funds Distribution Allocation Targets.

Eligible Subrecipients

- State Departments, Offices, and Agencies (Executive Branch and otherwise), to include:
  - Enterprise Technology Services
  - University of Hawaii
  - Department of Education
  - Office of Hawaiian Affairs
  - Judiciary, House, Senate
- Other State Entities, such as:
  - Hawaii Health Systems Corporation (HHSC)
  - Hawaii Housing Finance and Development Corporation (HHFDC)
  - Hawai'i Community Development Authority (HCDA)
- Counties and their Departments, Offices, and Agencies

Central Provisioning

Note: Grant requires each/all Subrecipient agreement to centrally held funds (Subrecipient Retention Agreement)

- ETS open for subrecipients to take advantage of ‘what ETS already offers’
  - These offers may or may not amount to requiring funding, as such OHS expects both parties to come back with project proposal if it does
- Objective 1: Governance and Planning, Project 6: Threat Intelligence and Information Sharing*
- Objective 4: Workforce Development, Project 4: Develop and Deploy CRT*
- Objective 4: Workforce Development, Project 10: Develop and Expand Relationships With Academic Partners (PISCES) *
- Objective 4: Workforce Development, Project 14: Develop and Implement a Robust Cybersecurity Training Program*

*Project identified in Statewide Cybersecurity Strategy and Implementation Plan

Fund Allocation Across Objective/Project/Year

	FY 2022	**%**	**FY 2023***	**%**	**FY 2024***	**%**	**FY 2025***	**%**
Federal Allocation	$2,243,539.00	100	$4,567,336.00	80	$3,362,000.00	70	$1,121,000.00	60
** State Match	Waived		$1,141,834.00	20	$1,440,857.14	30	$747,333.33	40
Total Available	$2,243,539.00	100	$5,709,170.00	100	$4,802,857.14	100	$1,868,333.33	100
Grant Administration	$112,176.95	5	$285,458.50	5	$240,142.86	5	$93,416.67	5
Objective 1: Governance and Planning	$641,249.05	29	$570,917.00	10	$480,285.71	10	$373,666.67	20
Objective 2: Assessment and Evaluation	$213,750.00	10	$1,427,292.50	25	$1,200,714.29	25	$280,250.00	15
Objective 3: Mitigation	$848,863.00	38	$2,283,668.00	40	$1,921,142.86	40	$747,333.33	40
Objective 4: Workforce Development	$427,500.00	19	$1,141,834.00	20	$960,571.43	20	$373,666.67	20

OHS Project Proposals (Admin + Central)

	FY 2022	%	FY 2023*	%	FY 2024*	%	FY 2025*	%
Federal Allocation	$2,243,539.00	100	$4,567,336.00	80	$3,362,000.00	70	$1,121,000.00	60
** State Match	Waived		$1,141,834.00	20	$1,440,857.14	30	$747,333.33	40
Total Available	$2,243,539.00	100	$5,709,170.00	100	$4,802,857.14	100	$1,868,333.33	100
Grant Administration	**$112,176.95**	**5**	**$285,458.50**	**5**	**$240,142.86**	**5**	**$93,416.67**	**5**
Objective 1: Governance and Planning	**$641,249.05**	**29**	**$570,917.00**	**10**	**$480,285.71**	**10**	**$373,666.67**	**20**
Statewide Cybersecurity Plan	$450,000.00	20	$0.00	0	$0.00	0	**$186,833.33**	**10**
Cyber Incident Response Plans	$100,000.00	14	$0.00	0	$0.00	0	$0.00	0
Cyber Incident Response Exercises	$91,249.05	4	$0.00	0	$0.00	0	$0.00	0
6. Threat Intelligence and Information Sharing		0	**$570,917.00**	**10**	**$480,285.71**	**10**	**$186,833.33**	**10**
Objective 2: Assessment and Evaluation	**$213,750.00**	**10**	**$1,427,292.50**	**25**	**$1,200,714.29**	**25**	**$280,250.00**	**15**
Develop asset protections and recovery actions.								
Continuous testing, education, evaluation, and structured assessments.								
Statewide inventory of devices, systems, software platforms, and applications.								
Foster understanding of organizational cybersecurity risks to operations and assets.								
Perform vulnerability scans; develop and implement a risk-based vulnerability management plan.								
Objective 3: Mitigation	**$848,863.00**	**38**	**$2,283,668.00**	**40**	**$1,921,142.86**	**40**	**$747,333.33**	**40**
5. Support Funding of Cybersecurity Projects at the County Level								
11. Develop Educational Materials on Cybersecurity Insurance								
3. Develop Purchasing Standards for Cybersecurity Third-Party Vendors								
16. Secure and Enhance Connections in Cybersecurity Infrastructure								
Objective 4: Workforce Development	**$427,500.00**	**19**	**$1,141,834.00**	**20**	**$960,571.43**	**20**	**$373,666.67**	**20**
Workforce Development Strategy/Implementation Plans	$427,500.00	19						
2. Enhance Cybersecurity Workforce Recruitment and Staffing		0						
4. Develop and Deploy CRT Team		0						
10. Develop and Expand Relationships With Academic Partners		0						
14. Develop and Implement a Robust Cybersecurity Training Program		0						

Open for Subrecipient Project Proposals

	FY 2022	%	FY 2023*	%	FY 2024*	%	FY 2025*	%
Federal Allocation	$2,243,539.00	100	$4,483,000.00	80	$3,362,000.00	70	$1,121,000.00	60
** State Match	Waived		$1,120,750.00	20	$1,440,857.14	30	$747,333.33	40
Total Available	$2,243,539.00	100	$5,603,750.00	100	$4,802,857.14	100	$1,868,333.33	100
Grant Administration	**$112,176.95**	**5**	**$280,187.50**	**5**	**$240,142.86**	**5**	**$93,416.67**	**5**
Objective 1: Governance and Planning	**$641,249.05**	**29**	**$560,375.00**	**10**	**$480,285.71**	**10**	**$373,666.67**	**20**
Statewide Cybersecurity Plan	$450,000.00	20	$0.00	0	$0.00	0	**$186,833.33**	**10**
Cyber Incident Response Plans	$100,000.00	14	$0.00	0	$0.00	0	$0.00	0
Cyber Incident Response Exercises	$91,249.05	4	$0.00	0	$0.00	0	$0.00	0
6. Threat Intelligence and Information Sharing		0	**$560,375.00**	**10**	**$480,285.71**	**10**	**$186,833.33**	**10**
Objective 2: Assessment and Evaluation	**$213,750.00**	**10**	**$1,400,937.50**	**25**	**$1,200,714.29**	**25**	**$280,250.00**	**15**
Develop asset protections and recovery actions.								
Continuous testing, education, evaluation, and structured assessments.								
Statewide inventory of devices, systems, software platforms, and applications.								
Foster understanding of organizational cybersecurity risks to operations and assets.								
Perform vulnerability scans; develop and implement a risk-based vulnerability management plan.								
Objective 3: Mitigation	**$848,863.00**	**38**	**$2,241,500.00**	**40**	**$1,921,142.86**	**40**	**$747,333.33**	**40**
5. Support Funding of Cybersecurity Projects at the County Level								
11. Develop Educational Materials on Cybersecurity Insurance								
3. Develop Purchasing Standards for Cybersecurity Third-Party Vendors								
16. Secure and Enhance Connections in Cybersecurity Infrastructure								
Objective 4: Workforce Development	**$427,500.00**	**19**	**$1,120,750.00**	**20**	**$960,571.43**	**20**	**$373,666.67**	**20**
Workforce Development Strategy/Implementation Plans	$427,500.00	19						
2. Enhance Cybersecurity Workforce Recruitment and Staffing		0						
4. Develop and Deploy CRT Team		0						
10. Develop and Expand Relationships With Academic Partners		0						
14. Develop and Implement a Robust Cybersecurity Training Program		0						

Subrecipient Investment Project Proposals Application Website

https://law.hawaii.gov/ohs/cybergrant/

Welcome to the homepage for the Hawaii Office of Homeland Security (OHS) State Local Cybersecurity Grant Program (SLCGP). Please review the information on this page carefully prior to completing an application.

Instructions are included here and in the downloadable guide. Should you have a question not covered in the material, please reach out using the contact form below.

Application deadline for FY 2022 funds is November 6th, 2024, at 5:00PM HST

How to apply

Step 1:

Download and read the Grant Application Guidance Document.

Step 2:

Download and complete the Grant Application and supporting documents (not all may be necessary, reference Grant Application Guidance Document).

Have your project information ready to go before you begin. Adobe Reader is Required. Ensure you have the most recent version of Adobe Reader installed. This can be downloaded from the Adobe website . The PDF form will not save unless opened in the official Adobe Reader application. Your web browser's default PDF viewer will not work.

a. **Gap Assessment Form**
   - For those that have in-house or 3rd party managing IT infrastructure and/or cybersecurity, that includes the detailed questions following the applicant information.
   - An Application Number will be sent to the email you provided in the Gap Assessment Form. After you submit your application, to include this form, check your email for your application number. Retain that email.

b. **Self-Certification**
   - Required for entities that have completed a cyber vulnerability assessment and/or cyber risk assessment within 365 calendar days of signing a grant application.

c. **Secure vendor quote** (only a single quote is required)**.**

d. **Budget Table**

e. **Project Narrative**

f. **Contact information for the authorizing official, project manager, and financial officer.**

g. **Locate or apply for your UEI and EIN numbers and register on SAM.gov**

Resources

UEI Number

UEI registration information is available on GSA.gov at: Unique Entity Identifier Update | GSA. Grants.gov registration information can be found at: https://www.grants.gov/web/grants/register.html

SAM.gov

- All applicants should be registered on sam.gov - https://www.sam.gov/SAM/

The SAM quick start guide for new recipient registration and SAM video tutorial for new applicants are tools created by the General Services Administration (GSA) to assist those registering with SAM. If applicants have questions or concerns about a SAM registration, please contact the Federal Support Desk at https://www.fsd.gov/fsd-gov/home.door or call toll free (866) 606-8220.

Point of Contact:

Ms. Jimmie L Collins
Chief, Planning and Operations
Hawaii Office of Homeland Security
jimmie.l.collins@hawaii.gov
office: 808-369-3570
cell: 808-223-2099