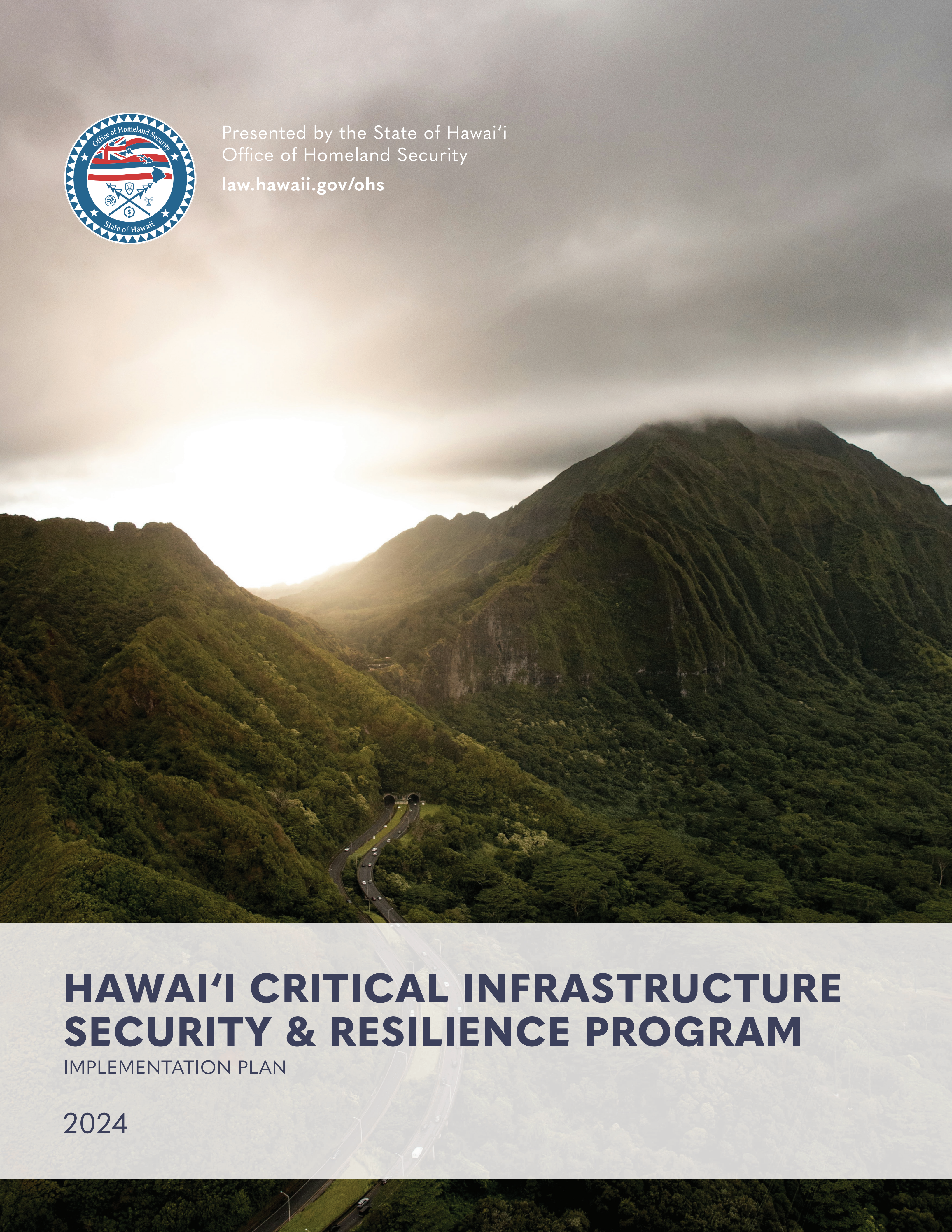


Presented by the State of Hawaiʻi
Office of Homeland Security

law.hawaii.gov/ohs

HAWAIʻI CRITICAL INFRASTRUCTURE SECURITY & RESILIENCE PROGRAM

IMPLEMENTATION PLAN

2024

TABLE OF CONTENTS

Appendices

THE ADMINISTRATOR'S MESSAGE

Frank J. Pace

The State of Hawaiʻi Office of Homeland Security (OHS) developed the Critical Infrastructure Security and Resilience Program (CISRP) Implementation Plan through extensive collaboration with relevant public, private, and non-profit stakeholders, experts, and agencies to ensure its comprehensiveness and effectiveness. OHS developed the CISRP Implementation Plan to facilitate the incorporation of security and resilience considerations in critical infrastructure (CI) planning activities statewide in the face of an ever-evolving threat landscape.

OHS recognizes the profound importance of safeguarding the CI that underpin our daily lives, economy, and security. Disruptions to individual CI entities and across CI sectors can have far-reaching and cascading impacts, making it imperative that we proactively address vulnerabilities and mitigate risks.

OHS welcomes and prioritizes active participation and teamwork in carrying out this plan and values community and stakeholder feedback and support during its implementation. By working together, we can strengthen the security and resilience of our state and nation, promoting a more secure and prosperous future.

Please feel free to reach out to the Hawaiʻi Office of Homeland Security for any further information or assistance regarding the OHS CISRP Implementation Plan.

Sincerely,

Frank J. Pace
Administrator, State of Hawaiʻi Office of Homeland Security

THIS PAGE INTENTIONALLY LEFT BLANK

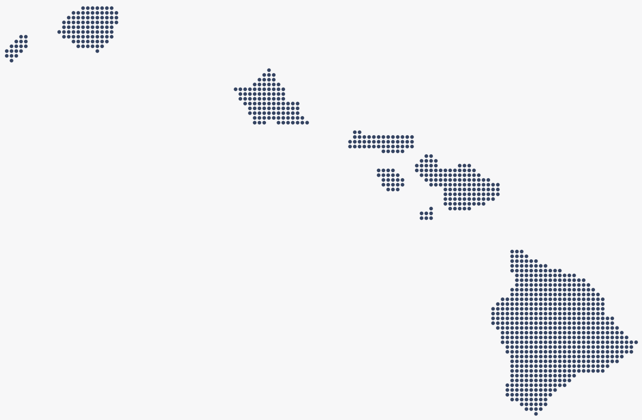
EXECUTIVE SUMMARY

The Hawaiʻi Office of Homeland Security (OHS) published the Hawaiʻi Critical Infrastructure Security & Resilience Program (CISRP): Strategy, Planning Framework, and Implementation Guide in March 2023 to enable the incorporation of security and resilience considerations in CI planning activities statewide. The Hawaiʻi Office of Homeland Security (OHS) recognizes the imperative to safeguard our CI systems, networks, data, and operations from evolving threats and has worked with CI owners, operators, and stakeholders to develop the CISRP Implementation Plan.

The CISRP defines CI as *"Interdependent systems and assets (existing, proposed, physical or virtual), of which, when compromised, incapacitated, or destroyed would negatively affect security, economic security, public health or safety, or any combination thereof."*[1] Driven by its purpose, this implementation plan encompasses all aspects of Hawaii's CI and seeks to achieve the goals displayed in **Figure ES-1**.

PURPOSE

The ultimate purpose of this project is to collect and document data and information that portrays the critical infrastructure ecosystem in Hawaiʻi, to better characterize and inform resource prioritization of reduction activities related to vulnerabilities and risk.



GOAL 1: MITIGATE

Reduce vulnerabilities in and risk to critical infrastructure.

GOAL 2: REDUCE

Reduce threat exposure for critical facilities.

GOAL 3: RESILIENCE

Plan for reboundable restoration of critical infrastructure.

GOAL 4: PLANNING

Establish mechanisms for incorporating resilience into planning

Figure ES-1: *Project Purpose and Goals*

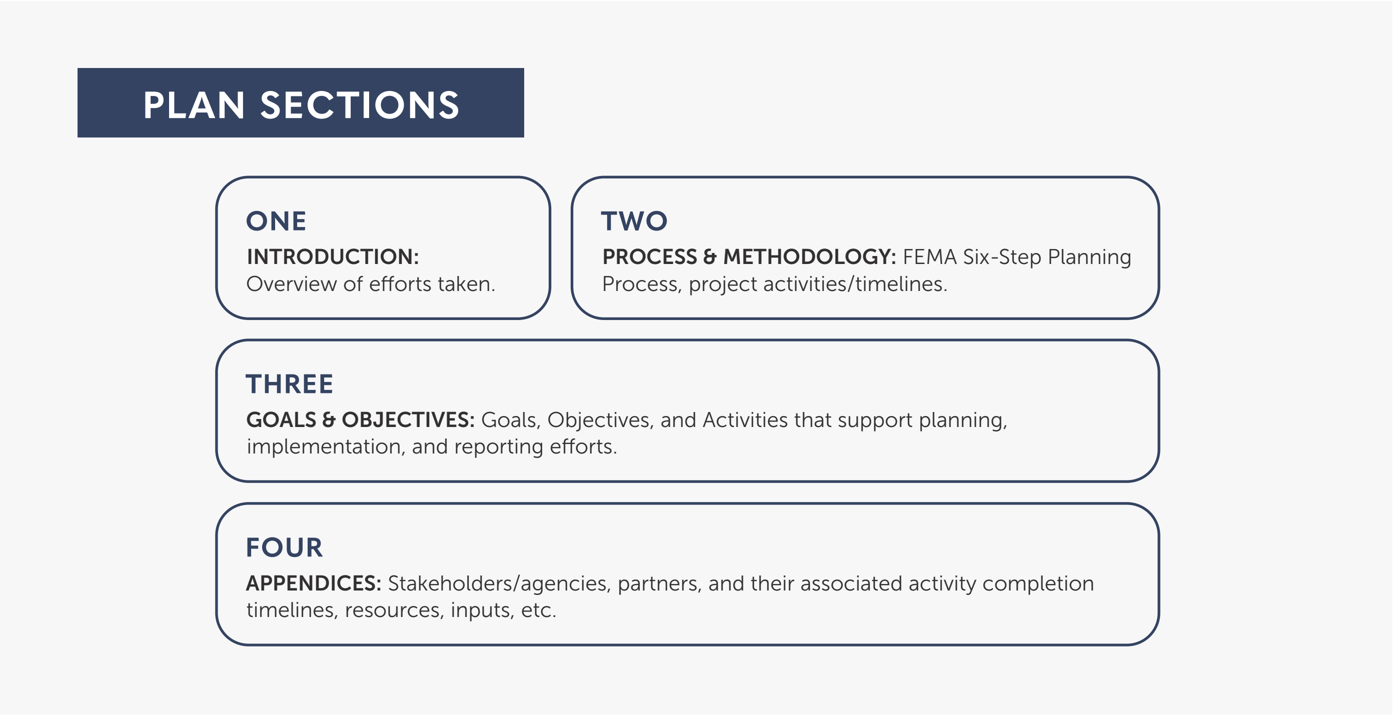
Completing these goals will help achieve OHS' project purpose and:

- Strengthen the resilience and security of CI against human and natural threats and hazards;
- Break down data silos and enhance data accuracy and transparency across Hawaiʻi;
- Enhance the continuous availability and reliability of CI systems and services; and
- Enhance situational awareness and incident response capabilities focused on CI.

[1] Hawaiʻi Critical Infrastructure Security and Resilience Program, pg. 11.

The Hawai'i CISRP Implementation Plan contains four sections (see **Figure ES-2**).

The challenges detailed in **Section 1: Introduction** underscore the urgency to commit resources and develop a comprehensive implementation plan to improve the reliability, security, and resilience of the CI upon which the State's residents, visitors, and businesses depend. **Section 2: Process and Methodology** highlights the approach for plan development, and **Section 3: Goals and Objectives** describes the approach for addressing the challenges stakeholders identified. **Section 4: Appendices** contains six appendices related to those stakeholder agencies or partners identified as Responsible, Accountable, Supportive, Consulted, and Informed (RASCI) and further identifies the associated activity completion timelines, resources, inputs, and expected outcomes.



PLAN SECTIONS

ONE

INTRODUCTION: Overview of efforts taken.

TWO

PROCESS & METHODOLOGY: FEMA Six-Step Planning Process, project activities/timelines.

THREE

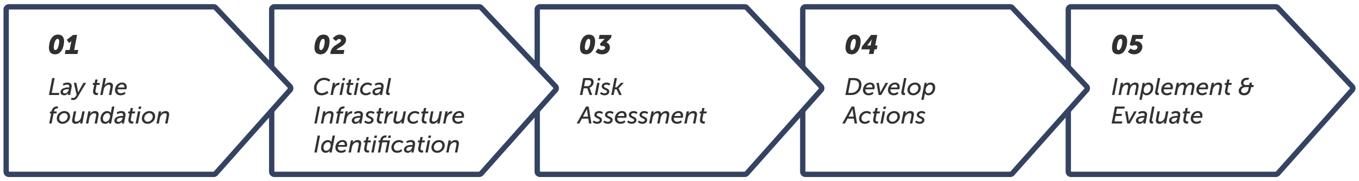
GOALS & OBJECTIVES: Goals, Objectives, and Activities that support planning, implementation, and reporting efforts.

FOUR

APPENDICES: Stakeholders/agencies, partners, and their associated activity completion timelines, resources, inputs, etc.

Figure ES-2: *Plan Sections*

The Hawai'i CISRP Implementation Plan describes a methodical process to enhance the posture of the State's CI by closely coordinating with federal, state, and local infrastructure stakeholders, owners, and operators to identify CI; examining dependencies and interdependencies; and enabling development of mitigation actions, prioritizing them, and implementing them to completion (see **Figure ES-3**).



01 Lay the foundation

02 Critical Infrastructure Identification

03 Risk Assessment

04 Develop Actions

05 Implement & Evaluate

Figure ES-3: *Planning Methodology*

The CISRP Implementation Plan is structured as a multi-year approach. It is important to note that OHS' initial effort is focused on the Communications, Information Technology, Transportation, Energy, and Water and Wastewater Sectors (referred to as Tier 1) due to their vital relationship to all CI sectors.

SECTION I: INTRODUCTION

OHS published the CISRP: Strategy, Planning Framework, and Implementation Guide (CISRP Guide) in March 2023 to enable the incorporation of security and resilience considerations in CI planning activities statewide. The CISRP Guide drew from key concepts of the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Infrastructure Resilience Planning Framework (IRPF) (see **Figure 1-1**). The development of the CISRP Guide was a major upshot from an initial stakeholder outreach event held in April of 2022, the Critical Infrastructure Security and Resilience Workshop. That event brought together more than 75 key leaders from law enforcement, military, state, and critical infrastructure entities in a half-day session focused on critical infrastructure vulnerabilities, security, and incident response.

As noted in the CISRP Guide, "a key element of OHS' purpose is to mobilize a collective defense of our State's CI." Starting in July of 2023, OHS began a series of formal working group (WG) sessions with CI stakeholders to coordinate to plan for the security and resilience of CI services in the face of multiple threats and challenges. These challenges underscore the urgency to commit resources and develop a comprehensive implementation plan for the CISRP to improve the reliability, security, and sustainability of the CI upon which the State's residents, visitors, and businesses depend and collect and document data that portrays the CI system in Hawai'i to better characterize vulnerabilities and risk to inform resource prioritization.

Threats to CI security are constantly evolving. In December of 2023, Governor Josh Green released his administration's "Mitigation Strategy and Priorities" (see **Figure 1-2**).[2] The strategy outlines the Governor's commitment to developing innovative mitigation initiatives to enhance the resilience of communities throughout the State. The publication highlights Governor Green's long-term policy and Hazard Mitigation Grant funding priorities.

Noting that OHS's project goals aligned with the Governor's strategy and priorities, OHS briefed these updates to the CI WG on 24 January 2024 and highlighted that the first grant funding priority for the Governor is to identify "projects that improve the resilience of critical facilities and critical infrastructure." In addition, the City and County of Honolulu 2022 Comprehensive Economic Development Strategy (CEDS) sets the direction for economic development, recovery, and long-term resilience for the island of O'ahu, and includes "Objective 4: Prioritize infrastructure resilience across the built environment with equitable, sustainable access to energy, water, waste, and services for residents and businesses, through reduced consumption and regenerative practices that enhance the island's natural systems."

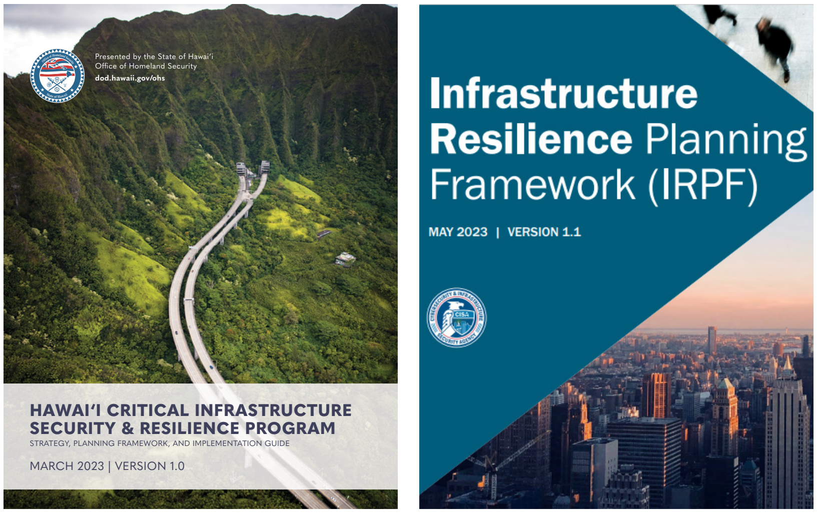
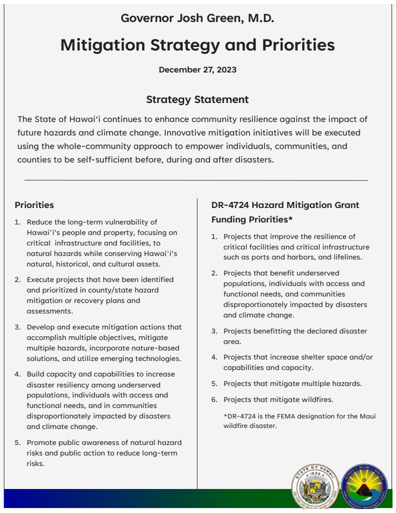

Presented by the State of Hawai'i
Office of Homeland Security
dod.hawaii.gov/ohs
HAWAI'I CRITICAL INFRASTRUCTURE
SECURITY & RESILIENCE PROGRAM
STRATEGY, PLANNING FRAMEWORK, AND IMPLEMENTATION GUIDE
MARCH 2023 | VERSION 1.0
Infrastructure
Resilience Planning
Framework (IRPF)
MAY 2023 | VERSION 1.1

Figure 1-1: *State and Federal CI Guidance*



Governor Josh Green, M.D.

Mitigation Strategy and Priorities

December 27, 2023

Strategy Statement

The State of Hawai'i continues to enhance community resilience against the impact of future hazards and climate change. Innovative mitigation initiatives will be executed using the whole-community approach to empower individuals, communities, and counties to be self-sufficient before, during and after disasters.

Priorities

1. Reduce the long-term vulnerability of Hawai'i's people and property, focusing on critical infrastructure and facilities, to natural hazards while conserving Hawai'i's natural, historical, and cultural assets.
2. Execute projects that have been identified and prioritized in county/state hazard mitigation or recovery plans and assessments.
3. Develop and execute mitigation actions that accomplish multiple objectives, mitigate multiple hazards, incorporate nature-based solutions, and utilize emerging technologies.
4. Build capacity and capabilities to increase disaster resiliency among underserved populations, individuals with access and functional needs, and in communities disproportionately impacted by disasters and climate change.
5. Promote public awareness of natural hazard risks and public action to reduce long-term risks.

DR-4724 Hazard Mitigation Grant Funding Priorities*

1. Projects that improve the resilience of critical facilities and critical infrastructure such as ports and harbors, and lifelines.
2. Projects that benefit underserved populations, individuals with access and functional needs, and communities disproportionately impacted by disasters and climate change.
3. Projects benefitting the declared disaster area.
4. Projects that increase shelter space and/or capabilities and capacity.
5. Projects that mitigate multiple hazards.
6. Projects that mitigate wildfires.

*DR-4724 is the FEMA designation for the Maui wildfire disaster.

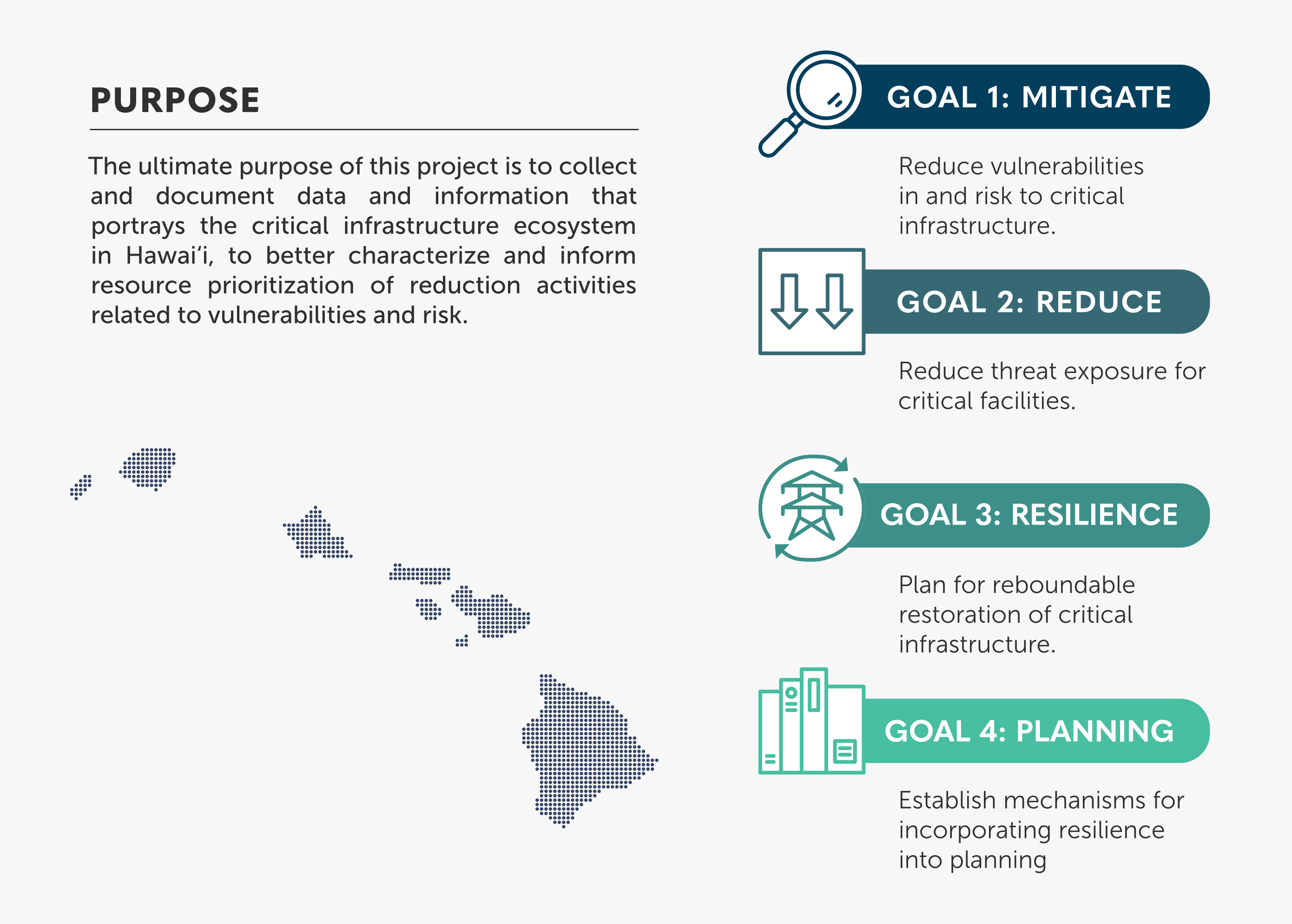
Figure 1-2: *Governor's Mitigation Strategy and Priorities*

[2] https://dod.hawaii.gov/hiema/files/2023/01/Govs-Mitigation-Strategy-v2.pdf

IMPLEMENTATION PLAN GOALS

OHS worked with stakeholders to identify four primary goals for the CISRP (see **Figure 1-3**).[3] This implementation plan describes the activities, inputs/resources, methods, timeframe, anticipated outputs, and implementing partners and collaborators to achieve the plan's goals and objectives.

The success of the implementation plan will rely on several factors, including the timely sharing of information and active participation from federal, state, and local government agencies, CI owners/operators, and other stakeholders.



PURPOSE

The ultimate purpose of this project is to collect and document data and information that portrays the critical infrastructure ecosystem in Hawai'i, to better characterize and inform resource prioritization of reduction activities related to vulnerabilities and risk.

GOAL 1: MITIGATE

Reduce vulnerabilities in and risk to critical infrastructure.

GOAL 2: REDUCE

Reduce threat exposure for critical facilities.

GOAL 3: RESILIENCE

Plan for reboundable restoration of critical infrastructure.

GOAL 4: PLANNING

Establish mechanisms for incorporating resilience into planning

Figure 1-3: *Goals*

[3] Section 3 provides detailed descriptions of the project goals and their associated objectives and activities.

SECTION II: METHODOLOGY & PLANNING PROCESS

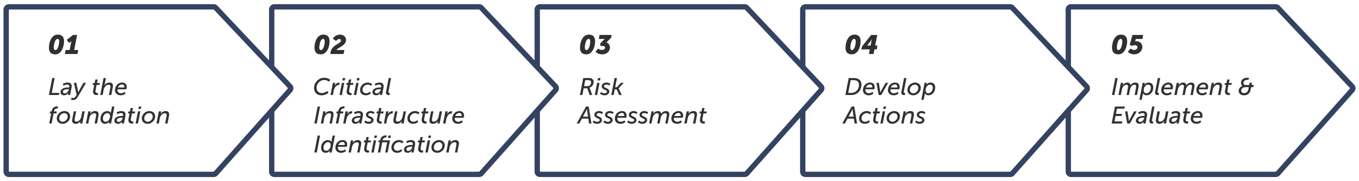


Figure 2-1: *IRPF Steps*

The IRPF and CISRP Guide both describe a stepwise process (see **Figure 2-1**) designed to assist stakeholders with identifying and prioritizing CI, analyzing threats and vulnerabilities, and developing and implementing risk reduction solutions. OHS incorporated key concepts from both documents in creating this implementation plan, starting with the first step of "Lay the Foundation" to define and scope the implementation planning effort, form a collaborative planning team with multiple stakeholders, and review existing data, plans, studies, maps, and other resources.

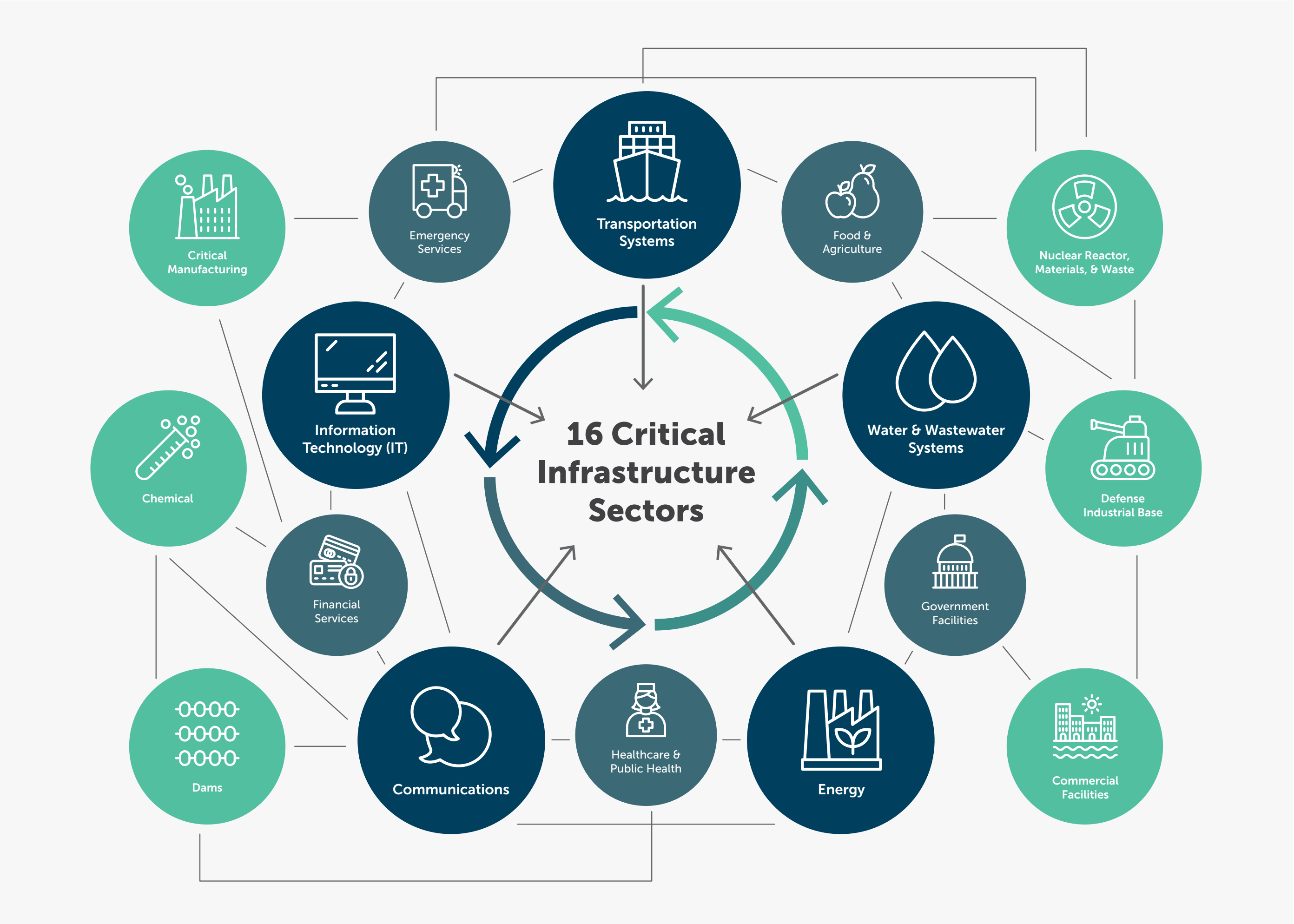


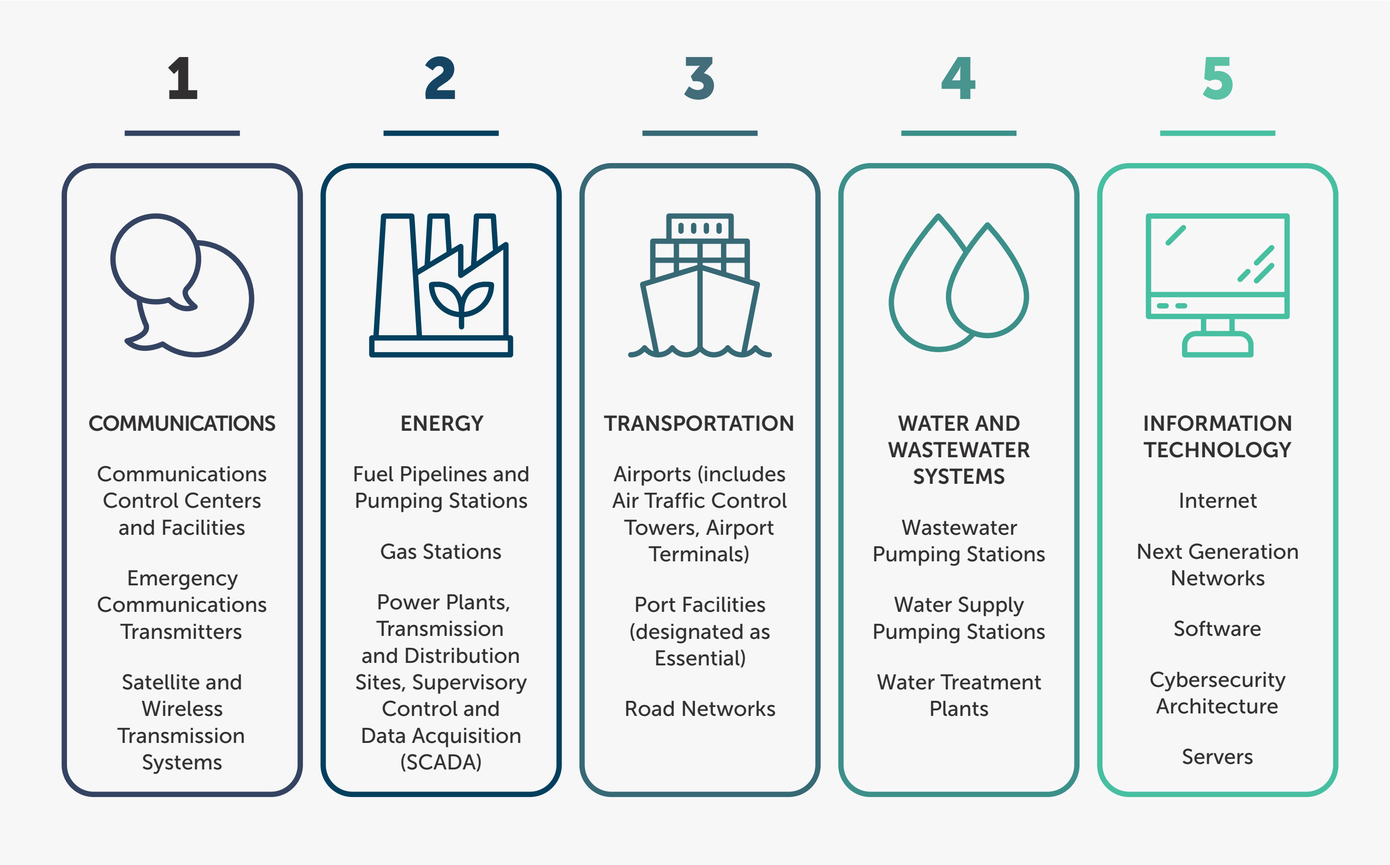
Figure 2-2: *16 Critical Infrastructure Sectors*

CRITICAL INFRASTRUCTURE SECTORS

The National Infrastructure Protection Plan (NIPP) categorizes CI into 16 distinct sectors as described in Presidential

Decision Directive (PPD) 21, Critical Infrastructure Security and Resilience (see **Figure 2-2**).[4,5]

OHS identified five priority sectors (Communications, Energy, Information Technology, Transportation, and Water & Wastewater systems) – referred to as Tier 1 sectors – for the initial implementation planning effort. Nearly all sectors rely on Communications, Energy, Information Technology, Transportation, and Water & Wastewater systems to operate. **Figure 2-3** lists some examples of asset types comprising each of the Tier 1 sectors.



1

COMMUNICATIONS

Communications Control Centers and Facilities

Emergency Communications Transmitters

Satellite and Wireless Transmission Systems

2

ENERGY

Fuel Pipelines and Pumping Stations

Gas Stations

Power Plants, Transmission and Distribution Sites, Supervisory Control and Data Acquisition (SCADA)

3

TRANSPORTATION

Airports (includes Air Traffic Control Towers, Airport Terminals)

Port Facilities (designated as Essential)

Road Networks

4

WATER AND WASTEWATER SYSTEMS

Wastewater Pumping Stations

Water Supply Pumping Stations

Water Treatment Plants

5

INFORMATION TECHNOLOGY

Internet

Next Generation Networks

Software

Cybersecurity Architecture

Servers

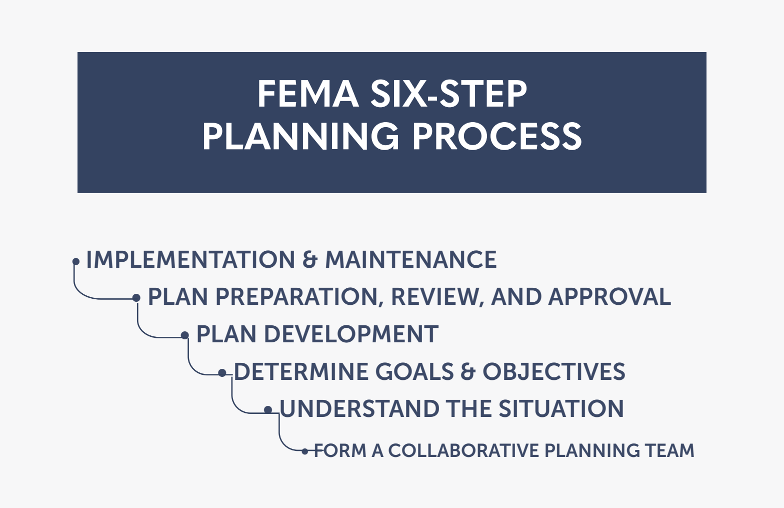
Figure 2-3: *Tier 1 Sectors and Asset Examples*

PLANNING PROCESS

Developing the Implementation Plan

OHS developed this plan over the course of one year using the Federal Emergency Management Agency's (FEMA) Six-Step Planning Process (see **Figure 2-4**).[6]

Figure 2-5 highlights the major project activities aligned with the FEMA Six-Step Planning Process. The first formal WG meeting took place in July 2023.



FEMA SIX-STEP PLANNING PROCESS

IMPLEMENTATION & MAINTENANCE

PLAN PREPARATION, REVIEW, AND APPROVAL

PLAN DEVELOPMENT

DETERMINE GOALS & OBJECTIVES

UNDERSTAND THE SITUATION

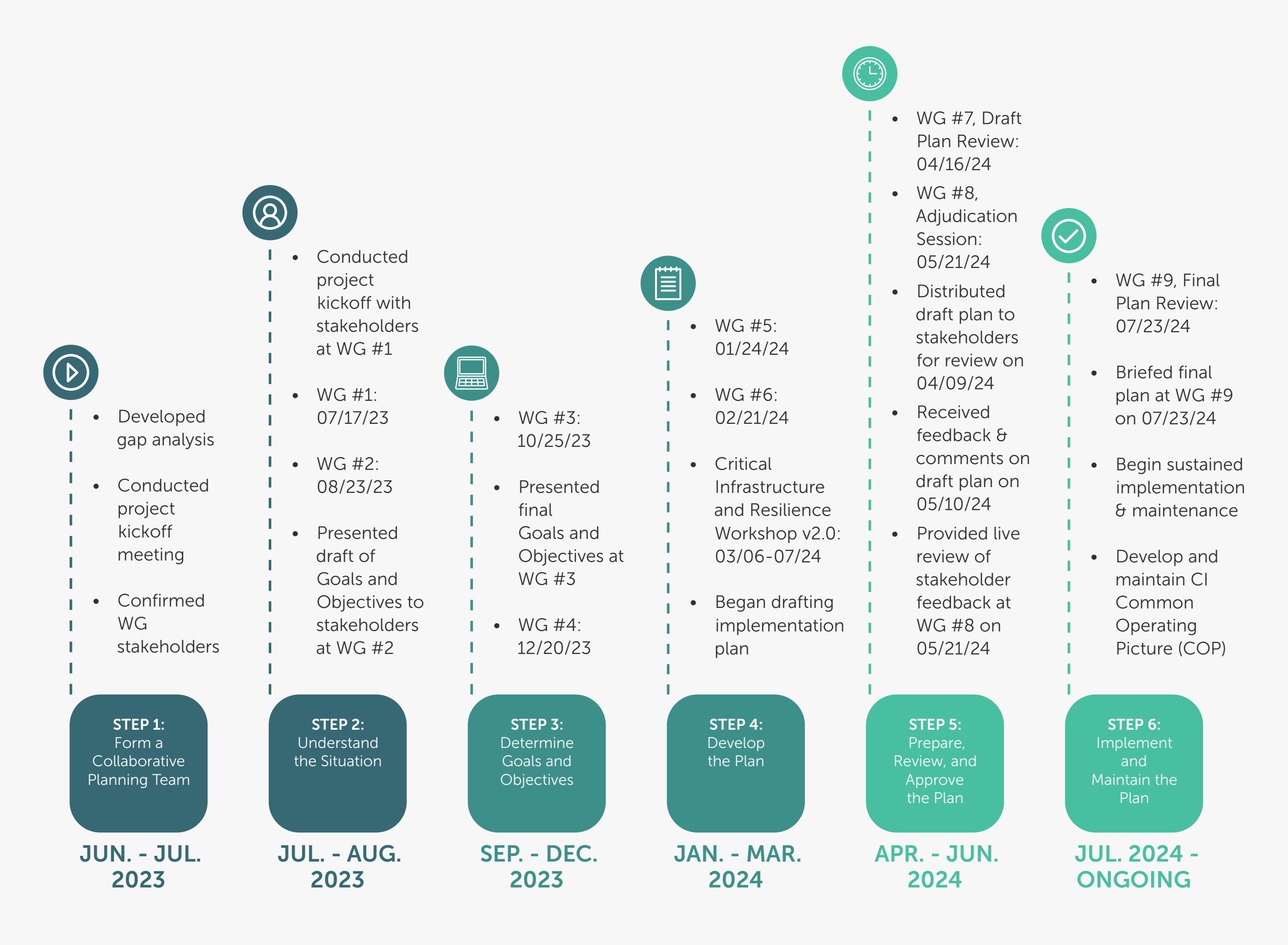
FORM A COLLABORATIVE PLANNING TEAM

Figure 2-4: *FEMA Six-Step Planning Process*

[4] NOTE: The Nuclear Reactor, Materials and Waste sector is not present in Hawaiʻi

[5] https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf, pg. 13

[6] https://www.fema.gov/sites/default/files/documents/fema_cpg-101-v3-developing-maintaining-eops.pdf


STEP 1: Form a Collaborative Planning Team
JUN. - JUL. 2023

- Developed gap analysis
- Conducted project kickoff meeting
- Confirmed WG stakeholders

STEP 2: Understand the Situation
JUL. - AUG. 2023

- Conducted project kickoff with stakeholders at WG #1
- WG #1: 07/17/23
- WG #2: 08/23/23
- Presented draft of Goals and Objectives to stakeholders at WG #2

STEP 3: Determine Goals and Objectives
SEP. - DEC. 2023

- WG #3: 10/25/23
- Presented final Goals and Objectives at WG #3
- WG #4: 12/20/23

STEP 4: Develop the Plan
JAN. - MAR. 2024

- WG #5: 01/24/24
- WG #6: 02/21/24
- Critical Infrastructure and Resilience Workshop v2.0: 03/06-07/24
- Began drafting implementation plan

STEP 5: Prepare, Review, and Approve the Plan
APR. - JUN. 2024

- WG #7, Draft Plan Review: 04/16/24
- WG #8, Adjudication Session: 05/21/24
- Distributed draft plan to stakeholders for review on 04/09/24
- Received feedback & comments on draft plan on 05/10/24
- Provided live review of stakeholder feedback at WG #8 on 05/21/24

STEP 6: Implement and Maintain the Plan
JUL. 2024 - ONGOING

- WG #9, Final Plan Review: 07/23/24
- Briefed final plan at WG #9 on 07/23/24
- Begin sustained implementation & maintenance
- Develop and maintain CI Common Operating Picture (COP)

Figure 2-5: *Project Timeline*

PROJECT RESEARCH

The project team conducted a gap analysis to identify local, state, national, and international CI resources and references, to gather best practices, and to gain insight into other CI planning efforts. The OHS project team reviewed over 300 documents and reference materials (see **Figure 2-6**) and engaged with representatives from other states to foster knowledge exchange and information sharing between CI programs.[7]

OHS also invited subject matter experts (SMEs) to facilitate discussions and improve understanding of the operations of each Tier 1 sector over the course of several WG meetings.

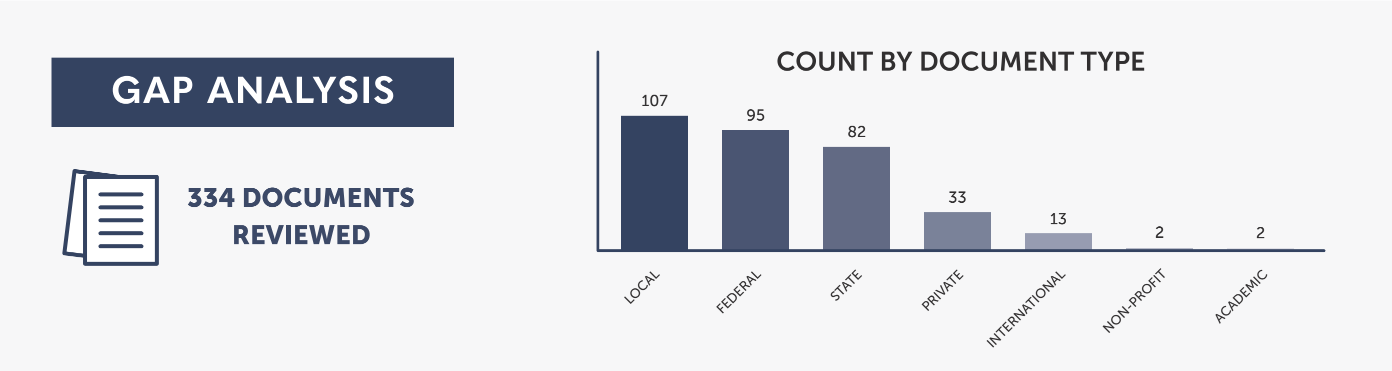


Figure 2-6: *Gap Analysis Summary*

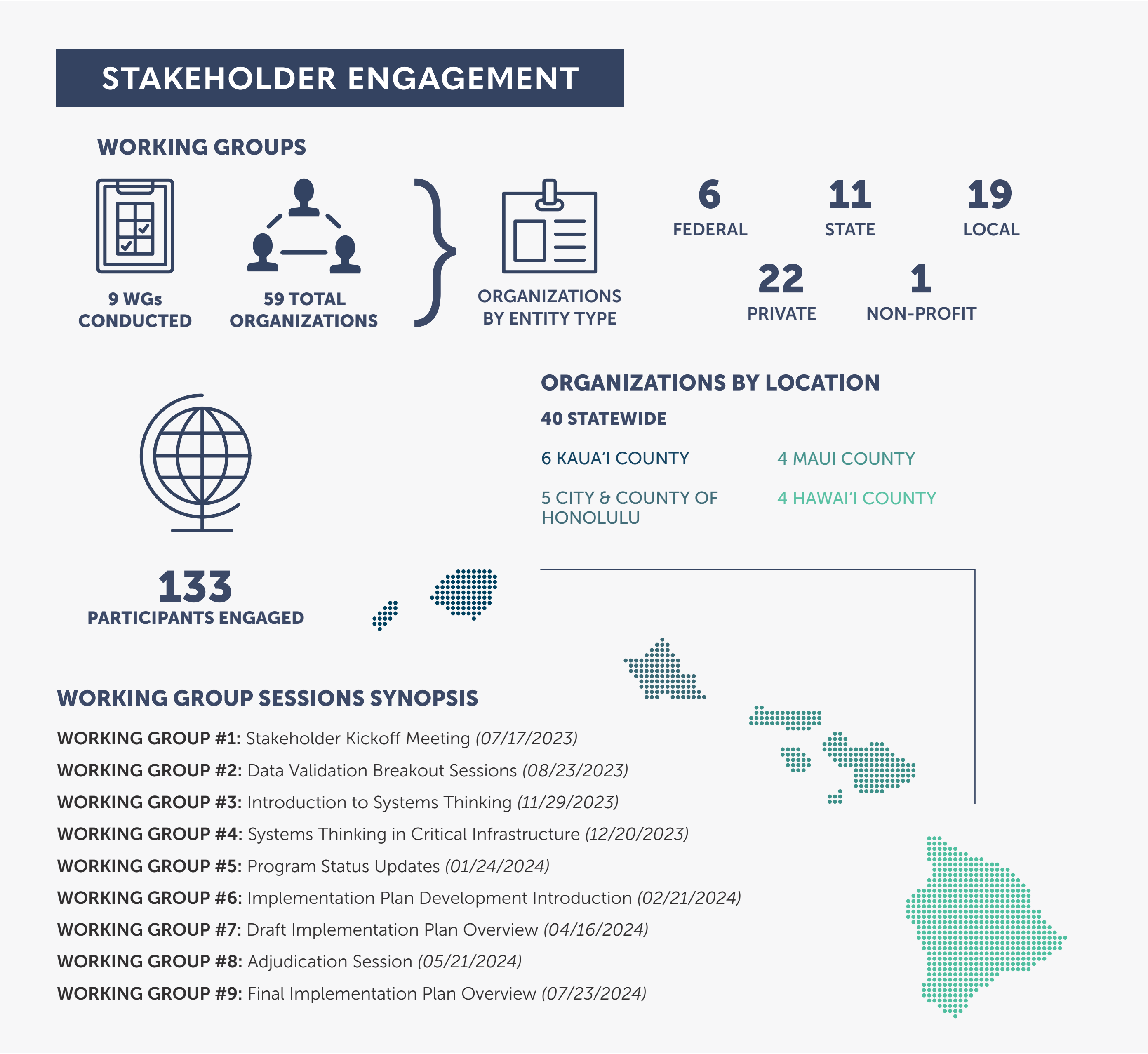
[7] See Appendix E for a detailed list of project references.

STAKEHOLDER OUTREACH

Outreach to stakeholders to develop this implementation plan utilized a collaborative whole community approach consisting of extensive communication including email, surveys, interviews, product reviews, and formal and informal meetings. Although the primary focus was to engage with stakeholders from Tier 1 Sectors, OHS did not limit the CI WG participation to Tier 1 stakeholders only.[8]

To reach the widest audience, OHS welcomed stakeholders to identify other organizations and/or points of contact (POCs) that were not already involved in the planning effort. Once identified, the project team contacted these partners and provided project familiarization briefings whenever appropriate. **Figure 2-7** summarizes the stakeholder engagement that took place during the development of this implementation plan. **See Appendix D, Figure D-1** for further details related to the CI WG meetings.

OHS also cohosted the Critical Infrastructure Security and Resilience Workshop v2.0 on 6 and 7 March 2024. See **Figure 2-8** for a synopsis of the workshop participants and objectives.



STAKEHOLDER ENGAGEMENT

WORKING GROUPS

9 WGs CONDUCTED

59 TOTAL ORGANIZATIONS

ORGANIZATIONS BY ENTITY TYPE

6 FEDERAL

11 STATE

19 LOCAL

22 PRIVATE

1 NON-PROFIT

133 PARTICIPANTS ENGAGED

ORGANIZATIONS BY LOCATION

40 STATEWIDE

6 KAUA'I COUNTY

4 MAUI COUNTY

5 CITY & COUNTY OF HONOLULU

4 HAWAI'I COUNTY

WORKING GROUP SESSIONS SYNOPSIS

WORKING GROUP #1: Stakeholder Kickoff Meeting *(07/17/2023)*

WORKING GROUP #2: Data Validation Breakout Sessions *(08/23/2023)*

WORKING GROUP #3: Introduction to Systems Thinking *(11/29/2023)*

WORKING GROUP #4: Systems Thinking in Critical Infrastructure *(12/20/2023)*

WORKING GROUP #5: Program Status Updates *(01/24/2024)*

WORKING GROUP #6: Implementation Plan Development Introduction *(02/21/2024)*

WORKING GROUP #7: Draft Implementation Plan Overview *(04/16/2024)*

WORKING GROUP #8: Adjudication Session *(05/21/2024)*

WORKING GROUP #9: Final Implementation Plan Overview *(07/23/2024)*

Figure 2-7: *Stakeholder Engagement Summary*

[8] See Appendix A for a detailed list of project stakeholders.

CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE WORKSHOP 2.0

74 TOTAL ATTENDEES

4	8	9	37	16
FEDERAL	STATE	LOCAL	DEFENSE	PRIVATE

46 TOTAL ORGANIZATIONS

6 PROJECT CONCEPTS

WORKSHOP SYNOPSIS

OBJECTIVE 1:

Identify critical infrastructure assets in key sectors, such as energy, water/wastewater, information/communications technology, and transportation.

OBJECTIVE 2:

Develop a shared understanding of critical infrastructure dependencies and interdependencies amongst sectors.

OBJECTIVE 3:

Categorize essential components of select critical infrastructure systems based on risk of cascading failure and catastrophic impacts to nation, state, county.

OBJECTIVE 4:

Identify potential solutions to enhance safety, security, and resilience on O'ahu and Kaua'i.

Figure 2-8: *Critical Infrastructure Security and Resilience Workshop v2.0 Summary*

THIS PAGE INTENTIONALLY LEFT BLANK

SECTION III: CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE PROGRAM IMPLEMENTATION GOALS

This section describes the goals, objectives, and activities that will support planning efforts and inform the reporting of implementation milestones and outcomes. The tables on the following pages outline goals, objectives, activities, inputs/resources, methods, timeframes, and anticipated outputs as described below. The Implementation Table uses the key term definitions listed in **Table 1** below.

Table 1: *Implementation Table Definitions*

TABLE ELEMENT	DEFINITION
Goal	One of the four goals identified within this plan
Objectives	Specific, measurable statement that supports the achievement of the goal
Activities	Actions taken through which inputs and resources are used to achieve specific outputs
Input/Resources	The inputs and resources needed to implement a project activity and achieve project outputs
Methods	Methods and tools used to collect quantitative or qualitative information for each performance measure and target
Time Frame	Identifies the expected time frame (quarter, year) for each activity
Anticipated Outputs	A direct, tangible, and measurable anticipated product of a project activity

See **Appendix A** for an overview of the implementing partners and their respective roles related to this implementation plan. The timeframe for this implementation plan is three years aligned to the fiscal year (FY), starting in October 2024 (See **Table 2**).

Table 2: *Summary of Activities by FY*

YEAR 1 (2024 - 2025)			
Q-1 (OCT - DEC)	**Q-2 (JAN - MAR)**	**Q-3 (APR - JUN)**	**Q-4 (JUL - SEP)**
1.1.1 Review existing Critical Infrastructure information	1.1.2 Identify data gaps and collect/refine basic and sector-specific Critical Infrastructure information	1.2.1 Identify Critical Infrastructure system vulnerabilities and risks	1.3.1 Identify dependencies/interdependencies amongst Critical Infrastructure systems 2.1.1 Identify threats to Critical Infrastructure to include cyber threats
3.1.1 Define and scope resilience planning efforts	3.2.2 Identify existing Critical Infrastructure resources and capabilities		4.2.1 Assemble a task force to build a Critical Infrastructure common operating picture
YEAR 2 (2025 - 2026)			
Q-1 (OCT - DEC)	**Q-2 (JAN - MAR)**	**Q-3 (APR - JUN)**	**Q-4 (JUL - SEP)**
3.1.2 Form a collaborative planning group including technology/security officers or experts that understand the interconnectivity of the cyber infrastructure with the physical infrastructure	2.1.2 Develop and implement a methodology to prioritize risks to Critical Infrastructure	1.2.3 Identify opportunities to reduce vulnerabilities and risks to Critical Infrastructure	1.4.1 Identify vulnerability and risk reduction solutions for Critical Infrastructure
1.2.2 Assess consequences/impacts to Critical Infrastructure	4.2.2 Ingest collected Critical Infrastructure data into common operating picture platform	1.4.2 Develop and implement a methodology to prioritize Critical Infrastructure vulnerability and risk reduction solutions	
YEAR 3 (2026 - 2027)			
Q-1 (OCT - DEC)	**Q-2 (JAN - MAR)**	**Q-3 (APR - JUN)**	**Q-4 (JUL - SEP)**
2.2.1 Review guidance and updates to prevent, protect from, and reduce identified vulnerabilities in and risk to Critical Infrastructure	4.1.1 Develop strategies for implementing Critical Infrastructure resilience solutions	3.2.1 Define goals and objectives for COOP plans, training sessions, and exercises	2.2.2 Disseminate guidance and updates to prevent, protect from, and reduce identified vulnerabilities in and risk to Critical Infrastructure
4.1.3 Share guidance and tools, and facilitate discussions to help support stakeholders with updating their plans			4.1.2 Monitor, evaluate, and assess effectiveness of resilience solutions 4.2.3 Update and maintain Critical Infrastructure common operating picture

GOAL ONE: REDUCE VULNERABILITIES IN AND RISK TO CRITICAL INFRASTRUCTURE

OHS recognizes the ever-evolving landscape of threats to CI and is determined to identify and address vulnerabilities that could compromise the resiliency of essential CI systems. Goal 1 aligns with OHS' commitment to safeguarding the continuity of critical operations and improving the reliability of infrastructure services. Goal 1 consists of four objectives and eight activities (**see Figure 3.1-1**). The lead for Goal 1 is OHS with support from the implementing partners identified in **Appendix A: Table A-2**. OHS will continue to engage with identified potential collaborators about opportunities for their participation in activities to which they are aligned. OHS intends to employ a comprehensive approach with activities that aim to assess, prioritize, and remediate vulnerabilities strengthening the State's defenses and enhancing the overall security and resiliency of its CI. OHS will identify and address current vulnerabilities, as well as anticipate and adapt to emerging threats in this dynamic environment through strategic planning efforts and continued collaboration with its partners.

GOAL

01

4 TOTAL OBJECTIVES

8 TOTAL ACTIVITIES

FOCUS AREA

MITIGATION			

OBJECTIVE 1.1: Conduct a comprehensive inventory of the State's Critical Infrastructure

OBJECTIVE 1.2: Support risk assessment efforts to identify and reduce vulnerabilities in Critical Infrastructure Systems

OBJECTIVE 1.3: Support the analysis of dependencies/interdependencies to assess the the potential for cascading, escalating, and common-cause failures throughout infrastructure systems

OBJECTIVE 1.4: Support development and prioritization of potential projects to reduce identified vulnerabilities in and risk to Critical Infrastructure systems

Figure 3.1-1: *Goal 1 Overview*

Table 3.1-1: *Goal 1 Implementation Table*

OBJECTIVE 1.1: Conduct of a comprehensive inventory of the State's Critical Infrastructure				
ACTIVITY	**INPUTS/RESOURCES**	**METHOD**	**TIME FRAME**	**ANTICIPATED OUTPUTS**
Activity 1.1.1: *Review existing Critical Infrastructure information*	Existing Datasets Meeting Minutes Plans Stakeholder Meetings	Research Stakeholder Review Survey(s) Interviews	Y1-Q1	Preliminary inventory of CI information Gap Analysis Basic/sector-specific data attributes

(Activities continue on next page)

ACTIVITY	INPUTS/RESOURCES	METHOD	TIME FRAME	ANTICIPATED OUTPUTS
Activity 1.1.2: *Identify data gaps and collect/refine basic and sector-specific Critical Infrastructure information*	Preliminary inventory of CI information Basic/sector-specific data attributes	Stakeholder Submissions Stakeholder Reviews	Y1-Q2	Revised inventory of CI information with basic and sector-specific data elements
OBJECTIVE 1.2: Support risk assessment efforts to identify and reduce vulnerabilities in Critical Infrastructure systems				
Activity 1.2.1: *Identify Critical Infrastructure system vulnerabilities and risks*	CI asset list Threat and Hazard Identification Risk Assessment (THIRA) Hazard Mitigation Plan Document Review (eg., AARs) SME input	Research Survey(s) Interviews Stakeholder Meetings/ Workshop Stakeholder Review	Y1-Q3	Inventory of all CI assets and their associated vulnerabilities by sector
Activity 1.2.2: *Assess consequences/impacts to Critical Infrastructure*	Risk Assessment CI List Dependency/ Interdependency Analysis	Interdependency Risk Assessment Stakeholder Meetings Stakeholder Reviews Focus Groups Workshops	Y2-Q1	Documented consequences/ impacts to CI
Activity 1.2.3: *Identify opportunities to reduce vulnerabilities and risks to Critical Infrastructure*	Inventory of all CI assets and their associated vulnerabilities	Document Review Research Vulnerability Assessments	Y2-Q3	List of Vulnerabilities by Sector/ Aggregate
OBJECTIVE 1.3: Support the analysis of dependencies/ interdependencies to assess the potential for cascading, escalating, and common-cause failures throughout infrastructure systems				
Activity 1.3.1: *Identify dependencies/ interdependencies amongst Critical Infrastructure systems*	Revised inventory of CI information	Research Stakeholder Meetings Stakeholder Reviews Survey(s)	Y1-Q4	Inventory of all CI assets and their identified dependencies/ interdependencies
OBJECTIVE 1.4: Support development and prioritization of potential projects to reduce identified vulnerabilities in and risk to Critical Infrastructure systems				
Activity 1.4.1: *Identify vulnerability and risk reduction solutions for Critical Infrastructure*	Dependency Analysis Past Risk Assessments	Stakeholder Meetings WGs	Y2-Q4	Draft vulnerability and risk reduction solutions for consideration of implementation
Activity 1.4.2: *Develop and implement methodology to prioritize Critical Infrastructure vulnerability and risk reduction solutions*	Draft resilience solutions for consideration of implementation	Solution Ranking/ Prioritization	Y2-Q3	Prioritized list of infrastructure vulnerability and risk reduction solutions

OHS will measure Goal 1 progress using the following metrics identified in the Goal 1 Measurement Plan in **Table 3.1-2**. Outputs for this goal include the following: 1.) An inventory of Tier 1 CI information and their associated vulnerabilities by sector, and 2.) A methodology to prioritize infrastructure resilience solutions.

Table 3.1-2: *Goal 1 Measurement Plan*

GOAL	EXEMPLARY MEASURE(S)	HOW OHS WILL MEASURE THIS GOAL
Goal 1: Reduce Vulnerabilities in and risk to Critical Infrastructure	Completion of a comprehensive inventory of the State's Tier 1 CI	Initial inventory of CI is available in the Common Operating Picture (COP)
	Conduct at least one workshop with Tier 1 stakeholders to identify and reduce vulnerabilities in CI systems	Attendance rosters Presentations Meeting minutes
	Conduct a workshop with stakeholders to identify dependencies/interdependencies to assess the potential for cascading, escalating, and common-cause failures throughout infrastructure systems	Attendance rosters Presentations Meeting minutes Quick Look Reports Surveys
	Completion of a methodology to prioritize CI vulnerability and risk reduction solutions	Approved methodology to prioritize CI vulnerability and risk reduction solutions for consideration of implementation Prioritized list of infrastructure vulnerability and risk reduction solutions

THIS PAGE INTENTIONALLY LEFT BLANK

GOAL TWO: REDUCE THREAT EXPOSURE FOR CRITICAL FACILITIES

OHS understands that reducing threat exposure for critical facilities is a crucial part of supporting the resilience of CI throughout the State. CISA defines critical facilities as *"those infrastructure systems and assets that are so vital that their incapacitation or destruction would have a debilitating effect on security, the economy, public health, public safety, or any combination thereof."*[9]

Goal 2 consists of two objectives and four activities (see **Figure 3.2-1**). The Lead for Goal 2 is OHS with support from the implementing partners identified in **Appendix A: Table A-2**. OHS will continue to engage with identified potential collaborators about possible opportunities for their participation in activities to which they are aligned. OHS will use a prioritization method focused on the impacts each CI system can have on the community to determine its criticality and priority. Finally, OHS will support risk assessment efforts that include identifying threats and the consequences they pose on CI systems and then comparing each threat, vulnerability, and consequence based on which threat poses the most risk.[10]

GOAL
02
2 TOTAL OBJECTIVES
4 TOTAL ACTIVITIES
FOCUS AREA
THREAT REDUCTION

OBJECTIVE 2.1: Support risk assessment efforts to identify, deter, detect, disrupt, and prepare for threats to critical facilities and systems

OBJECTIVE 2.2: Identify and share information on methods to prevent, protect from, and reduce identified vulnerabilities in and risk to Critical Infrastructure facilities and systems

Figure 3.2-1: *Goal 2 Overview*

[9] Critical Infrastructure Sectors | CISA

[10] https://law.hawaii.gov/ohs/wp-content/uploads/sites/2/2024/01/cisrp-2023-final-web.pdf

Table 3.2-1: *Goal 2 Implementation Table*

ACTIVITY	INPUTS/RESOURCES	METHOD	TIME FRAME	ANTICIPATED OUTPUTS
OBJECTIVE 2.1: Support risk assessment efforts to identify, deter, detect, disrupt, and prepare for threats to critical facilities and systems				
Activity 2.1.1: *Identify threats to Critical Infrastructure to include cyber threats*	Information Sharing Analysis Centers (ISACs) Forums/Conferences Homeland Security Information Network (HSIN)/other threat reporting mechanisms WGs Hawai'i State Fusion Center (HSFC) THIRA SME input	Research Survey(s) Interviews Stakeholder Meetings Stakeholder Review	Y1-Q4	List of identified threats
Activity 2.1.2: *Develop and implement a methodology to prioritize risks to Critical Infrastructure*	Risk Assessment CI List Dependency/ Interdependency Analysis CISA Guidance	Stakeholder Meetings Stakeholder Reviews Focus Groups Workshops	Y2-Q2	List of prioritized risks by sector
OBJECTIVE 2.2: Identify and share information on methods to prevent, protect from, and reduce identified vulnerabilities in and risk to Critical Infrastructure				
Activity 2.2.1: *Review guidance and updates to prevent, protect from, and reduce identified vulnerabilities in and risk to Critical Infrastructure*	Vulnerability Assessments Risk Assessments CI Asset List Hazard Mitigation Plans Guidance from Centers of Excellence	Research Survey(s) Interviews Stakeholder Meetings Stakeholder Review	Y3-Q1	Prioritized list of guidance and updates to share with stakeholders that supports preventing, protecting from, and mitigating threats
Activity 2.2.2: *Disseminate guidance and updates to prevent, protect from, and reduce identified vulnerabilities in and risk to Critical Infrastructure*	Prioritized list of information to share with stakeholders that supports preventing, protecting from, and mitigating threats	Homeland Security Forum CI WG Public Service Announcements	Y3-Q4	Ongoing dialogue with CI owners/operators OHS and stakeholders are aware of latest methods to prevent, protect from, and reduce identified vulnerabilities in and risk to CI

OHS will measure Goal 2 progress using the following metrics identified in the Goal 2 Measurement Plan in **Table 3.2 2**

Outcomes for this goal include the following: 1.) A prioritization method for CI Systems in Hawai'i and 2.) Information on methods to prevent, protect from, and mitigate threats to critical facilities and systems to be shared with stakeholders regularly.

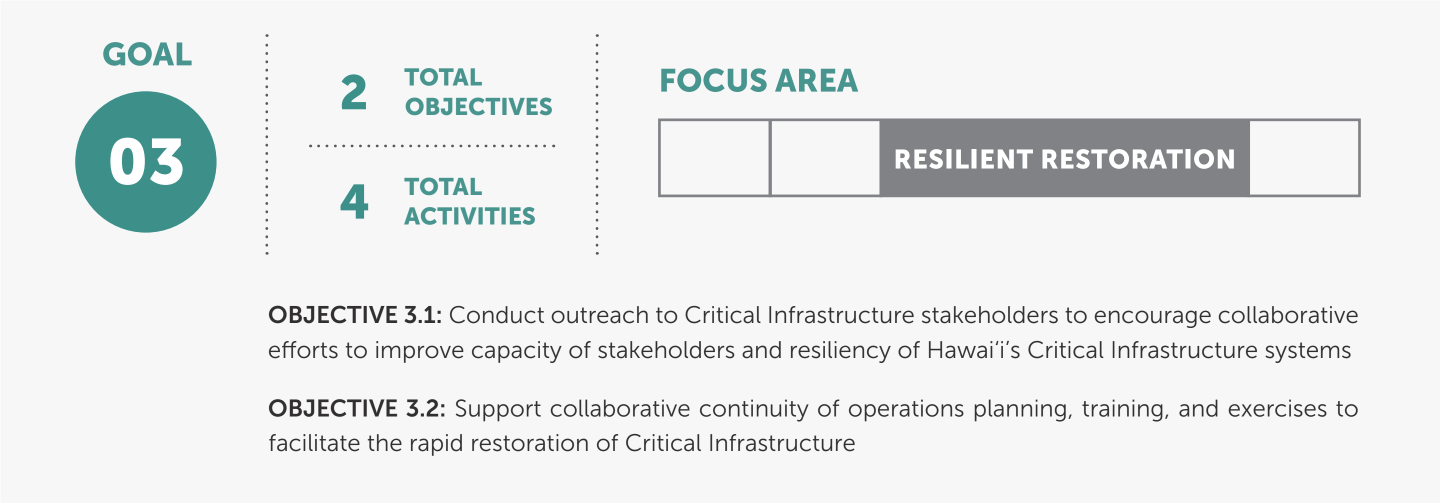
Table 3.2-2: *Goal 2 Measurement Plan*

GOAL	EXEMPLARY MEASURE(S)	HOW OHS WILL MEASURE THIS GOAL
Goal 2: Reduce threat exposure for critical facilities	Stakeholder input from each Tier 1 sector to update threats to CI to include cyber threats	Stakeholder feedback forms Survey RFI responses Conduct training to ensure stakeholders are aware of identified threats Engaged Stakeholders to identify threats
	Stakeholders are aware of prioritized risks to their sector	WG sessions Surveys
	Stakeholder awareness of threat reduction activities	Planning documents Stakeholder feedback forms Meeting minutes Conduct training to ensure stakeholders are aware of threat reduction activities
	Stakeholder awareness of guidance and updates to prevent, protect from, and reduce identified vulnerabilities in and risk to Critical Infrastructure	Comprehensive list of guidance and updates shared with stakeholders that supports preventing, protecting from, and mitigating threats Surveys Stakeholder feedback forms Meeting presentations Meeting minutes Attendance rosters

THIS PAGE INTENTIONALLY LEFT BLANK

GOAL THREE: PLAN FOR REBOUNDABLE RESTORATION OF CRITICAL INFRASTRUCTURE

OHS understands that planning for reboundable CI restoration is vital to ensure that essential services throughout the State are quickly reinstated following disruptions. Planning for resilient CI restoration protects public safety and economic stability and contributes to the overall resilience of everyday operations in Hawaiʻi. Goal 3 consists of two objectives and four activities (see **Figure 3.3-1**). The lead for Goal 3 is OHS with support from the implementing partners identified in **Appendix A: Table A-2**. OHS will continue to engage with identified potential collaborators about possible opportunities for their participation in activities to which they are aligned.



OBJECTIVE 3.1: Conduct outreach to Critical Infrastructure stakeholders to encourage collaborative efforts to improve capacity of stakeholders and resiliency of Hawaiʻi's Critical Infrastructure systems

OBJECTIVE 3.2: Support collaborative continuity of operations planning, training, and exercises to facilitate the rapid restoration of Critical Infrastructure

Figure 3.3-1: *Goal 3 Overview*

Table 3.3-1: *Goal 3 Implementation Table*

OBJECTIVE 3.1: Conduct outreach to Critical Infrastructure stakeholders to encourage collaborative efforts to improve capacity of stakeholders and resiliency of Hawaii's Critical Infrastructure systems

ACTIVITY	INPUTS/RESOURCES	METHOD	TIME FRAME	ANTICIPATED OUTPUTS
Activity 3.1.1: *Define and scope resilience planning efforts*	Project Scope Guidance Document Pre-identified Stakeholders Contact List Stakeholder Input OHS Guidance	Stakeholder Meetings Stakeholder Reviews Interviews Workshops Research	Y1-Q1	Defined and scoped resilience efforts
Activity 3.1.2: *Form a collaborative planning group including technology/security officers or experts that understand the interconnectivity of the cyber infrastructure with the physical infrastructure*	Pre-Identified Stakeholders Contact list	Pre-Identified Stakeholders Contact list	Y2-Q1	CI stakeholders engaged to attend WG sessions and support planning

OBJECTIVE 3.2: Support collaborative continuity of operations planning, training and exercises to facilitate the rapid restoration of Critical Infrastructure				
ACTIVITY	**INPUTS/RESOURCES**	**METHOD**	**TIME FRAME**	**ANTICIPATED OUTPUTS**
Activity 3.2.1: *Define Goals and Objectives for Continuity of Operations (COOP) plans, training sessions, and exercises*	Hazard Mitigation Plan Capability Survey Gap Analysis ISACs	Research External Outreach	Y3-Q3	Updated goals and objectives for COOP plans, training sessions, and exercises
Activity 3.2.2: *Identify existing Critical Infrastructure resources and capabilities*	CISA Plans Sector-Specific Plans	Research External Outreach	Y1-Q2	List of existing CI resources and capabilities

OHS will measure Goal 3 progress using the following metrics identified in the Goal 3 Measurement Plan in **Table 3.3-2**.

Outcomes for this goal include the following: 1.) A diverse group of stakeholders at various levels, that have access to resources, expertise, and commitment to enhance the overall resilience and security of the CI environment in the state. 2.) Improved focus and alignment of stakeholder materials, a chance to review and refine the scope of their projects, and increased accountability of stakeholders.

Table 3.3-2: *Goal 3 Measurement Plan*

GOAL	EXEMPLARY MEASURE(S)	HOW OHS WILL MEASURE THIS GOAL
Goal 3: Plan for reboundable restoration of Critical Infrastructure	Stakeholder input from each Tier 1 sector to update threats to CI to include cyber threats	Stakeholder feedback forms Survey RFI responses Conduct training to ensure stakeholders are aware of identified threats Engaged Stakeholders to identify threats
	Stakeholders are aware of prioritized risks to their sector	WG sessions Surveys
	Stakeholder awareness of threat reduction activities	Planning documents Stakeholder feedback forms Meeting minutes Conduct training to ensure stakeholders are aware of threat reduction activities
	Stakeholder awareness of guidance and updates to prevent, protect from, and reduce identified vulnerabilities in and risk to CI	Comprehensive list of guidance and updates shared with stakeholders that supports preventing, protecting from, and mitigating threats Surveys Stakeholder feedback forms Meeting presentations Meeting minutes Attendance rosters

THIS PAGE INTENTIONALLY LEFT BLANK

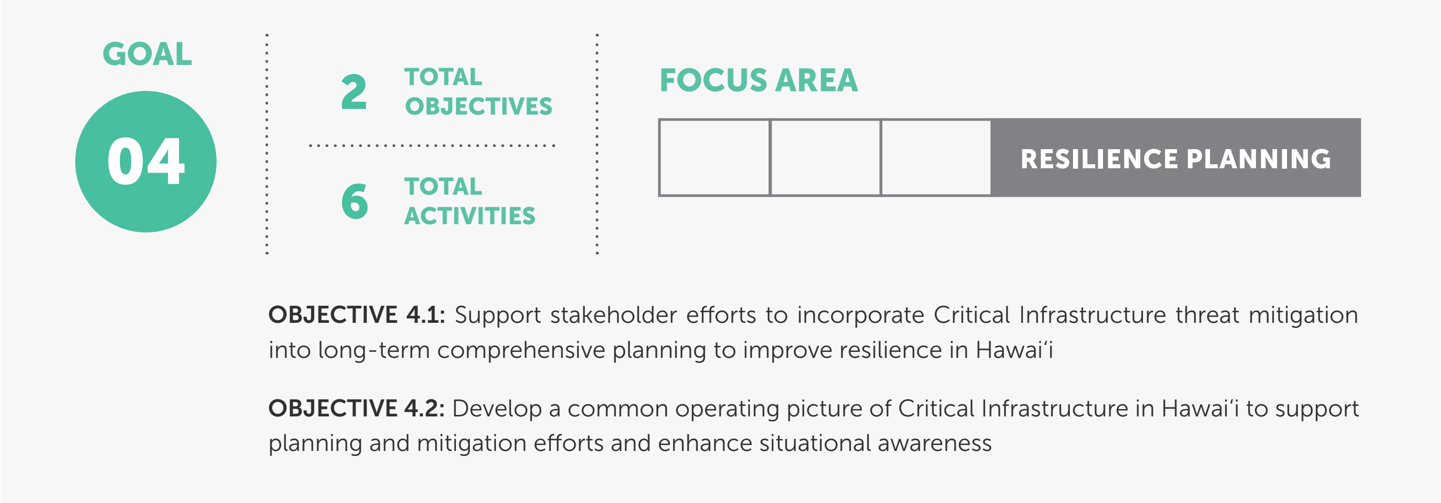
GOAL FOUR: ESTABLISH MECHANISMS FOR INCORPORATING RESILIENCE INTO PLANNING

OHS understands that establishing mechanisms for incorporating resilience into CI planning is essential for safeguarding public safety, maintaining economic stability, and ensuring the continued functioning of essential services. Goal 4 consists of two objectives and six activities (see **Figure 3.4-1**). The lead for Goal 4 is OHS with support from the implementing partners identified in **Appendix A: Table A-2**:

OHS will continue to engage with identified potential collaborators about possible opportunities for their participation in activities to which they are aligned.

OHS will support the development of implementation strategies that incorporate the following items into planning:

- A responsible party
- Collaborators/partner agencies/private sector partners
- Preliminary implementation steps
- An estimated timeline
- Resources required for implementation to include funding estimates as appropriate
- Potential barriers to implementation and potential solutions
- Information to support prioritization of projects



GOAL

04

2 TOTAL OBJECTIVES

6 TOTAL ACTIVITIES

FOCUS AREA

RESILIENCE PLANNING

OBJECTIVE 4.1: Support stakeholder efforts to incorporate Critical Infrastructure threat mitigation into long-term comprehensive planning to improve resilience in Hawai'i

OBJECTIVE 4.2: Develop a common operating picture of Critical Infrastructure in Hawai'i to support planning and mitigation efforts and enhance situational awareness

Figure 3.4-1: *Goal 4 Overview*

Table 3.4-1: *Goal 4 Implementation Table*

<table>
<tr><th colspan="5">OBJECTIVE 4.1: Support stakeholder efforts to incorporate Critical Infrastructure threat mitigation into long-term comprehensive planning to improve resilience in Hawai‘i</th></tr>
<tr><th>ACTIVITY</th><th>INPUTS/RESOURCES</th><th>METHOD</th><th>TIME FRAME</th><th>ANTICIPATED OUTPUTS</th></tr>
<tr><td><b><i>Activity 4.1.1:</i></b> <i>Develop strategies for implementing Critical Infrastructure resilience solutions</i></td><td>Identified existing CI resources and capabilities
Doctrine/Guidance
CISA</td><td>Research
Stakeholder Meetings
Stakeholder Reviews
Focus Groups
Workshops
Interviews
Survey(s)</td><td>Y3-Q2</td><td>Identified CI resilience solution strategies</td></tr>
<tr><td><b><i>Activity 4.1.2:</i></b> <i>Monitor, evaluate, and assess effectiveness of resilience solutions</i></td><td>Stakeholder Feedback
Plan Review
Past Assessment Results</td><td>Stakeholder Meetings
Focus Groups
Workshops
Survey(s)</td><td>Y3-Q4</td><td>Periodic status updates from CI providers</td></tr>
<tr><td><b><i>Activity 4.1.3:</i></b> <i>Share guidance and tools, and facilitate discussions to help support stakeholders with updating their plans</i></td><td>Resilience Solutions Status
Regulatory Requirements
Doctrine/Guidance
Compliance Matrix</td><td>Stakeholder Meetings
Survey(s)
Focus Groups</td><td>Y3-Q1</td><td>Completion of stakeholder plan updates</td></tr>
<tr><th colspan="5">OBJECTIVE 4.2: Develop a common operating picture of Critical Infrastructure in Hawai‘i to support planning and mitigation efforts and enhance situational awareness</th></tr>
<tr><td><b><i>Activity 4.2.1:</i></b> <i>Assemble a task force to build a Critical Infrastructure common operating picture</i></td><td>Design Concept
User Story Requirements</td><td>Research
Stakeholder Meetings
Focus Groups
Workshops</td><td>Y1-Q4</td><td>Development and implementation of a functional COP platform informed by user input</td></tr>
<tr><td><b><i>Activity 4.2.2:</i></b> <i>Ingest collected Critical Infrastructure data into common operating picture platform</i></td><td>Existing Datasets
Revised inventory of CI information</td><td>Geographic Information Systems (GIS) Upload
Data Review</td><td>Y2-Q2</td><td>CI data from public and private entities available within COP platform</td></tr>
<tr><td><b><i>Activity 4.2.3:</i></b> <i>Update and maintain Critical Infrastructure common operating picture</i></td><td>COP
Updated CI Lists</td><td>Stakeholder Reviews
Survey(s)
WGs</td><td>Y3-Q4</td><td>Periodic review and revision of COP data</td></tr>
</table>

OHS will measure Goal 4 progress using the following metrics identified in the Goal 4 Measurement Plan in **Table 3.4-2**

Outcomes for this goal include the following: 1.) A COP for OHS and its stakeholders to effectively monitor, analyze, and manage CI systems. 2.) Regular dialogue with CI providers focused on threat mitigation and resilience planning.

Table 3.4-2: *Goal 4 Measurement Plan*

GOAL	EXEMPLARY MEASURE(S)	HOW OHS WILL MEASURE THIS GOAL
Goal 4: Establish mechanisms for incorporating resilience into planning	Developed strategies for implementing CI Resilience Solutions	Documented strategies and solutions by sector Implementing timeline Published strategy development guidance Meeting minutes Presentations Attendance rosters
	Developed and disseminated guidance establishing methods to incorporate resilience into planning	Updated plans Stakeholder feedback Implementation reports Site assessment reports Disseminated guidance Meeting presentations Training
	Shared guidance, tools, and facilitated discussions to help sup-port stakeholders with updating their plans	Stakeholder feedback/interviews Presentations Attendance roster Disseminated guidance Updated plans
	Assembled a task force to build a CI COP	List of task force members Meeting minutes Surveys
	Ingested CI data into COP platform	Number of datasets in the COP Data source tracking Stakeholder feedback Compliance rate (list of organizations with ingested/not-ingested datasets)
	Updated and Maintained CI COP	COP update schedule COP Plans Stakeholder input Meeting minutes

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A: IMPLEMENTING PARTNERS AND IDENTIFIED POTENTIAL COLLABORATORS

The Hawai'i CISRP Implementation Plan outlines the roles and responsibilities using a matrix called the Responsibility Assignment Matrix (RAM). This matrix aids in determining each stakeholder's specific roles and responsibilities related to the goals and objectives outlined within the CI Implementation Plan. The RAM lists the organizations who volunteer to assist, offer advice, and receive information, as well as those who are accountable and liable for certain responsibilities. OHS is considered both Responsible and Accountable for all identified goals, objectives, and activities. The RAM includes the roles and definitions accepted by the CI WG in **Figure A-1**.[11]

RASCI ROLES AND DEFINITIONS

R: RESPONSIBLE

The organization that is assigned to track the completion of activities within the implementation plan. OHS is identified as the "Responsible" party within this plan.

A: ACCOUNTABLE

Refers to the organization that has ultimate control over tracking the objectives and activities in the CI implementation plan.

S: SUPPORTIVE

Supportive members may provide help by providing resources to the Responsible organization. They actively work with the Responsible organization to support the completion of activities.

C: CONSULTED

The 'Consulted' are there to help the Responsible finish their tasks successfully. They are experts who you can go to for relevant advice, help, or opinion. They offer valuable subject matter expertise.

I: INFORMED

The 'Informed' category includes the people who are to be kept in the loop over the course of the project. They need to be informed about the progress of the project every step of the way, up until it reaches completion.

Figure A-1: *RASCI Roles and Definitions*

See **Table A-1** for a list of implementation plan goals, objectives, and activities.

[11] WG #6, 21 Feb 2024

Table A-1: *Goals, Objectives, and Activities*

GOAL 1: REDUCE VULNERABILITIES IN AND RISK TO CRITICAL INFRASTRUCTURE
Objective 1.1: Conduct of a comprehensive inventory of the State's Critical Infrastructure
1.1.1: Review existing CI information
1.1.2: Identify data gaps and collect/refine basic and sector-specific CI information
Objective 1.2 Support risk assessment efforts to identify and reduce vulnerabilities in Critical Infrastructure systems
1.2.1: Identify CI system vulnerabilities and risks
1.2.2: Assess consequences/impacts to CI
1.2.3: Identify opportunities to reduce vulnerabilities and risks to CI
Objective 1.3: Support the analysis of dependencies/ interdependencies to assess the potential for cascading, escalating, and common-cause failures throughout infrastructure systems
1.3.1: Identify dependencies/interdependencies amongst CI systems
Objective 1.4: Support development and prioritization of potential projects to reduce identified vulnerabilities in and risk to Critical Infrastructure systems
1.4.1: Identify vulnerability and risk reduction solutions for CI
1.4.2: Develop and implement a methodology to prioritize Critical Infrastructure vulnerability and risk reduction solutions
GOAL 2: REDUCE THREAT EXPOSURE FOR CRITICAL FACILITIES
Objective 2.1: Support risk assessment efforts to identify, deter, detect, disrupt, and prepare for threats to critical facilities and systems
2.1.1: Identify threats to CI to include Cyber threats
2.1.2: Develop and implement a methodology to prioritize risks to CI
Objective 2.2: Identify and share information on methods to prevent, protect from, and reduce identified vulnerabilities in and risk to Critical Infrastructure
2.2.1: Review guidance and updates to prevent, protect from, and reduce identified vulnerabilities in and risk to CI
2.2.2: Disseminate guidance and updates to prevent, protect from, and reduce identified vulnerabilities in and risk to CI
GOAL 3: PLAN FOR REBOUNDABLE RESTORATION OF CRITICAL INFRASTRUCTURE
Objective 3.1: Conduct outreach to Critical Infrastructure stakeholders to encourage collaborative efforts to improve capacity of stakeholders and resiliency of Hawaii's Critical Infrastructure systems
3.1.1: Define and scope resilience planning efforts
3.1.2: Form a collaborative planning group including technology/security officers or experts that understand the interconnectivity of the cyber infrastructure with the physical infrastructure
Objective 3.2: Support collaborative continuity of operations planning, training and exercises to facilitate the rapid restoration of Critical Infrastructure
3.2.1: Define Goals and Objectives for COOP plans, training sessions, and exercises
3.2.2: Identify existing CI resources and capabilities
GOAL 4: ESTABLISH MECHANISMS FOR INCORPORATING RESILIENCE INTO PLANNING
Objective 4.1: Support stakeholder efforts to incorporate Critical Infrastructure threat mitigation into long-term comprehensive planning to improve resilience in Hawai'i
4.1.1: Develop strategies for implementing Critical Infrastructure resilience solutions
4.1.2: Monitor, evaluate, and assess effectiveness of resilience solutions
4.1.3: Share guidance and tools, and facilitate discussions to help support stakeholders with updating their plans
Objective 4.2: Develop a common operating picture of Critical Infrastructure in Hawai'i to support planning and mitigation efforts and enhance situational awareness
4.2.1: Assemble a task force to build a CI common operating picture
4.2.2: Ingest collected CI data into common operating picture platform
4.2.3: Update and Maintain CI common operating picture

Table A-2: *Responsibility Assignment Matrix (RAM)*

ORGANIZATIONS	GOAL 1 OBJECTIVES							
	1.1		1.2			1.3	1.4	
	1.1.1	1.1.2	1.2.1	1.2.2	1.2.3	1.3.1	1.4.1	1.4.2
Aloha Petroleum	I	C	C	I	I	C	C	C
American Savings Bank	C	C	C	C	C	C	C	C
AT&T	C	C	C	C	C	C	C	C
City and County of Honolulu Board of Water Supply (BWS)	I	C	I	C	I	C	I	I
City and County of Honolulu Department of Emergency Management (DEM)	S	S	S	S	S	S	S	S
County of Hawaii Department of Environmental Management (ENV)	I	I	I	I	I	I	I	I
County of Hawaii Department of Information Technology	I	I	I	I	I	I	I	I
County of Hawaii Department of Water	I	I	I	I	I	I	I	I
County of Kauai, Information Technology Division	S	S	S	S	S	S	S	S
County of Kauai, Department of Water	S	S	S	S	S	S	S	S
Cybersecurity and Infrastructure Security Agency (CISA)	C	C	C	C	C	C	C	C
DRFortress	C	C	C	C	C	C	C	C
Federal Aviation Administration (FAA)	C	C	C	C	C	C	C	C
Hawaii Broadband and Digital Equity Office	I	I	I	I	I	I	I	I
Hawaii Department of Transportation - Highways (HDOT)	C	C	C	C	C	C	C	C
Hawaii Department of Transportation - Airports	S	S	S	S	S	S	S	S
Hawaii Department of Transportation - Harbors	S	S	S	S	S	S	S	S
Hawaii Department of Water Supply (DWS)	I	I	I	I	I	I	I	I
Hawaii State Energy Office (HSEO)	S	S	S	S	S	S	S	S
Hawaii Gas	C	C	C	C	C	C	C	C
Hawaii Healthcare Emergency Management (HHEM)	C	C	C	C	C	C	C	C
Hawaii National Guard (HING)	S	S	S	S	S	S	S	S
Hawaii Stevedores	C	C	C	C	C	C	C	C
Hawaiian Airlines	S	S	S	S	S	S	S	S
Hawaiian Electric Company	S	C	S	S	C	S	C	C
Kauai Emergency Management Agency (KEMA)	S	S	S	S	S	S	S	S
Navy Region Hawaii (NavREGHI)	I	I	I	C	C	C	C	S
Public Utilities Commission (PUC)	C	C	C	C	C	C	C	C
State of Hawaii, Office of Planning and Sustainable Development, Statewide GIS Program	I	S	I	I	I	I	I	I
United States Army Pacific Command (USARPAC)	I	I	I	I	I	I	I	I
US Coast Guard (USCG)	C	C	C	C	C	C	C	C
US Department of Energy (DOE) (ESF#12)	I	I	I	I	I	I	I	I
Verizon Wireless	C	C	C	C	C	C	C	C
Young Brothers, LLC	I	I	C	C	S	C	S	I

ORGANIZATIONS	GOAL 2 OBJECTIVES			
	2.1		2.2	
	2.1.1	2.1.2	2.2.1	2.2.2
Aloha Petroleum	I	I	I	I
American Savings Bank	C	C	C	C
AT&T	C	C	C	C
City and County of Honolulu Board of Water Supply (BWS)	I	I	I	I
City and County of Honolulu Department of Emergency Management (DEM)	I	C	C	I
County of Hawaii Department of Environmental Management (ENV)	*Opted Out*			
County of Hawaii Department of Information Technology	I	I	I	I
County of Hawaii Department of Water	I	I	I	I
County of Kauai, Information Technology Division	S	C	S	S
County of Kauai, Department of Water	S	S	S	S
Cybersecurity and Infrastructure Security Agency (CISA)	C	C	C	C
DRFortress	C	C	C	C
Federal Aviation Administration (FAA)	C	C	C	C
Hawaii Broadband and Digital Equity Office	I	I	I	I
Hawaii Department of Transportation - Highways (HDOT)	C	C	C	C
Hawaii Department of Transportation - Airports	S	S	S	S
Hawaii Department of Transportation - Harbors	S	S	S	S
Hawaii Department of Water Supply (DWS)	I	I	I	I
Hawaii State Energy Office (HSEO)	S	S	S	S
Hawaii Gas	C	C	C	C
Hawaii Healthcare Emergency Management (HHEM)	C	C	C	C
Hawaii National Guard (HING)	S	S	S	S
Hawaii Stevedores	C	C	C	C
Hawaiian Airlines	C	C	C	C
Hawaiian Electric Company	S	S	C	C
Kauai Emergency Management Agency (KEMA)	S	S	S	S
Navy Region Hawaii (NavREGHI)	C	C	C	C
Public Utilities Commission (PUC)	C	C	C	C
State of Hawaii, Office of Planning and Sustainable Development, Statewide GIS Program	I	I	I	I
United States Army Pacific Command (USARPAC)	I	I	I	I
US Coast Guard (USCG)	C	C	C	C
US Department of Energy (DOE) (ESF#12)	I	I	I	I
Verizon Wireless	C	C	C	C
Young Brothers, LLC	C	I	I	C

ORGANIZATIONS	GOAL 3 OBJECTIVES			
	3.1		3.2	
	3.1.1	3.1.2	3.2.1	3.2.2
Aloha Petroleum	I	I	I	I
American Savings Bank	C	C	C	C
AT&T	C	C	C	C
City and County of Honolulu Board of Water Supply (BWS)	I	I	I	I
City and County of Honolulu Department of Emergency Management (DEM)	C	C	S	C
County of Hawaii Department of Environmental Management (ENV)	I	I	I	I
County of Hawaii Department of Information Technology	I	I	I	I
County of Hawaii Department of Water	I	I	I	I
County of Kauai, Information Technology Division	C	C	I	C
County of Kauai, Department of Water	S	S	S	S
Cybersecurity and Infrastructure Security Agency (CISA)	C	C	C	C
DRFortress	I	I	I	C
Federal Aviation Administration (FAA)	C	C	S	S
Hawaii Broadband and Digital Equity Office	C	C	C	C
Hawaii Department of Transportation - Highways (HDOT)	C	C	C	C
Hawaii Department of Transportation - Airports	S	S	S	S
Hawaii Department of Transportation - Harbors	S	S	S	S
Hawaii Department of Water Supply (DWS)	I	I	I	I
Hawaii State Energy Office (HSEO)	S	S	S	S
Hawaii Gas	C	C	C	C
Hawaii Healthcare Emergency Management (HHEM)	C	C	C	C
Hawaii National Guard (HING)	S	S	S	S
Hawaii Stevedores	C	C	C	C
Hawaiian Airlines	C	I	I	C
Hawaiian Electric Company	C	S	C	S
Kauai Emergency Management Agency (KEMA)	S	S	S	S
Navy Region Hawaii (NavREGHI)	C	C	I	C
Public Utilities Commission (PUC)	C	C	C	C
State of Hawaii, Office of Planning and Sustainable Development, Statewide GIS Program	I	C	I	I
United States Army Pacific Command (USARPAC)	I	I	I	I
US Coast Guard (USCG)	C	C	C	C
US Department of Energy (DOE) (ESF#12)	I	I	I	I
Verizon Wireless	C	C	C	C
Young Brothers, LLC	I	C	C	I

ORGANIZATIONS	GOAL 4 OBJECTIVES					
	4.1			4.2		
	4.1.1	4.1.2	4.1.3	4.2.1	4.2.2	4.2.3
Aloha Petroleum	I	I	I	I	I	I
American Savings Bank	C	I	C	I	I	I
AT&T	C	C	C	C	C	C
City and County of Honolulu Board of Water Supply (BWS)	I	I	I	I	I	I
City and County of Honolulu Department of Emergency Management (DEM)	S	C	C	S	S	S
County of Hawaii Department of Environmental Management (ENV)	I	I	I	I	I	I
County of Hawaii Department of Information Technology	I	I	I	I	I	I
County of Hawaii Department of Water	I	I	I	I	I	I
County of Kauai, Information Technology Division	C	C	C	I	I	C
County of Kauai, Department of Water	S	S	S	S	S	S
Cybersecurity and Infrastructure Security Agency (CISA)	C	C	C	C	C	C
DRFortress	I	I	I	I	I	I
Federal Aviation Administration (FAA)	S	S	S	C	C	S
Hawaii Broadband and Digital Equity Office	C	C	C	C	C	C
Hawaii Department of Transportation - Highways (HDOT)	C	C	C	C	C	C
Hawaii Department of Transportation - Airports	C	C	C	C	C	C
Hawaii Department of Transportation - Harbors	S	S	S	S	S	S
Hawaii Department of Water Supply (DWS)	I	I	I	I	I	I
Hawaii State Energy Office (HSEO)	S	S	S	S	S	S
Hawaii Gas	C	C	C	C	C	C
Hawaii Healthcare Emergency Management (HHEM)	C	C	C	C	C	C
Hawaii National Guard (HING)	S	S	S	S	S	S
Hawaii Stevedores	C	C	C	C	C	C
Hawaiian Airlines	C	C	C	I	I	I
Hawaiian Electric Company	S	C	S	S	S	S
Kauai Emergency Management Agency (KEMA)	S	S	S	S	S	S
Navy Region Hawaii (NavREGHI)	I	I	C	C	I	I
Public Utilities Commission (PUC)	C	C	C	C	C	C
State of Hawaii, Office of Planning and Sustainable Development, Statewide GIS Program	I	I	C	I	C	C
United States Army Pacific Command (USARPAC)	I	I	I	I	I	I
US Coast Guard (USCG)	C	C	C	C	C	C
US Department of Energy (DOE) (ESF#12)	I	I	I	I	I	I
Verizon Wireless	C	C	C	C	C	C
Young Brothers, LLC	I	C	C	C	I	I

Table A-3 displays a comprehensive summary of the identified potential collaborators for the four goals in this plan. Identified potential collaborators may be aligned to as few as one or as many as all the activities associated with the goals; however, as of the publishing date of this plan, they have not confirmed their role in the RAM goal tables above.

Table A-3: *Identified Potential Collaborators*

IDENTIFIED POTENTIAL COLLABORATORS
Hawai'i Office of Enterprise Technology Services
Hawai'i Department of Defense
Hawai'i Emergency Management Agency
Hawai'i Transportation Association
Island Energy Services
Kaua'i Fire Department
Kaua'i Island Utility Cooperative
Maui Emergency Management Agency
Statewide Interoperability Coordinator
T-Mobile

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B: ACRONYMS

Table B-1 displays acronyms used throughout this document.

Table B-1: *Acronyms*

ACRONYMS	
BWS	City and County of Honolulu Board of Water Supply
CI	Critical Infrastructure
CISA	Cybersecurity and Infrastructure Security Agency
CISRP	Critical Infrastructure Security and Resilience Program
COOP	Continuity of Operations
COP	Common Operating Picture
CRS	Community Rating System
DCCA	Hawaiʻi Department of Commerce and Consumer Affairs
CCHNL DEM	City and County of Honolulu Department of Emergency Management
DEM	County of Hawaiʻi Department of Environmental Management
DEM	County of Maui Department of Environmental Management
DTS	City and County of Honolulu Department of Transportation Services
DHS	U.S. Department of Homeland Security
DOD	U.S. Department of Defense
DOE	Hawaiʻi Department of Energy
DOT	U.S. Department of Transportation
ETS	Hawaiʻi Office of Enterprise Technology Services
ENV	City and County of Honolulu Department of Environmental Services
FAA	Federal Aviation Administration
FEMA	Federal Emergency Management Agency
GDSS	Geospatial Decision Support System
GIS	Geospatial Information System
HCCDA	Hawaiʻi County Civil Defense Agency
HDOD	Hawaiʻi Department of Defense
HDOT	Hawaiʻi State Department of Transportation
HDOT-Airports	Hawaiʻi State Department of Transportation Airports
HDOT-Harbors	Hawaiʻi State Department of Transportation Harbors
HDOT-Highways	Hawaiʻi State Department of Transportation Highways
HECO	Hawaiian Electric Company
HHEM	Hawaiʻi Healthcare Emergency Management

ACRONYMS	
HIAT	Hawai'i Interdependency Analysis Tool
HI-EMA	Hawai'i Emergency Management Agency
HING	Hawai'i National Guard
HSEO	Hawai'i State Energy Office
HSFC	Hawai'i State Fusion Center
HSIN	Homeland Security Information Network
HTA	Hawai'i Transportation Association
IES	Island Energy Services
IMP	Implementation and Measurement Plan
IRPF	Infrastructure Resilience Planning Framework
ISAC	Information Sharing Analysis Center
ITD	County of Kaua'i Information Technology Division
ITSD	County of Maui Information Technology Services Division
KEMA	Kaua'i Emergency Management Agency
KFD	Kaua'i Fire Department
KIUC	Kaua'i Island Utility Cooperative
MEMA	Maui Emergency Management Agency
NIPP	National Infrastructure Protection Plan
OHS	Hawai'i Office of Homeland Security
POC	Point of Contact
RAM	Responsibility Assignment Matrix
RASCI	Responsible, Accountable, Supportive, Consulted, Informed
SMART	Specific, Measurable, Achievable, Relevant, and Time-bound
SME	Subject Matter Expert
SWIC	Statewide Interoperability Coordinator
THIRA	Threat and Hazard Identification Risk Assessment
USCG	U.S. Coast Guard
WG	Working Group

APPENDIX C: KEY TERMS

Table C-1 displays Key Terms that OHS used throughout this document.

Table C-1: *Key Terms*

TERM	DEFINITION
Accountable	Refers to the organization that has ultimate control over tracking the objectives and activities in the CI implementation plan.
Assets	A person, structure, facility, information, material, equipment, network, or process, whether physical or virtual, that enables an organization's services, functions, or capabilities.[12]
Capability	The ability of an organization or system to perform specific tasks or functions effectively during a crisis or disaster.
Community	One or more local jurisdictions or special districts representing a region or shared infrastructure corridor.[13]
Consequence	The effect of an event, incident, or occurrence, which is commonly measured in four ways: Human, Economic, Mission, and Psychological.[14]
Consulted	The 'Consulted' are there to help the Responsible finish their tasks successfully. They are the experts who you can go to for relevant advice, help, or opinion. They offer valuable subject matter expertise.
Contamination	The undesirable deposition of a chemical, biological, or radiological material on the surface of structures, areas, objects, or people.[15]
Critical Asset	Person, structure, facility, information, material, or process that has value.[16] Hawai'i CI Implementation Plan Definition: Components of state-based critical infrastructure systems that, if disrupted or destroyed, would have a debilitating impact on Hawai'i's security, economic security, public health or safety, or any combination thereof.
Critical Facility	Those infrastructure systems and assets that are so vital that their incapacitation or destruction would have a debilitating effect on security, the economy, public health, public safety, or any combination thereof.[17]
Critical Infrastructure	Hawai'i CISRP Definition: Interdependent systems and assets (existing, proposed, physical or virtual), of which when compromised, incapacitated, or destroyed would negatively affect security, economic security, public health or safety, or any combination thereof.[18] Federal Definition: Physical or virtual assets, systems, and networks so vital to the United States that the incapacity or destruction of such assets, systems, or networks would have a debilitating impact on security, national economic security, public health or safety, or any combination of those matters.[19]
Criticality	A measure of the importance associated with the loss or degradation of infrastructure.[20]

[12] https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/

[13] https://law.hawaii.gov/ohs/wp-content/uploads/sites/2/2024/01/cisrp-2023-final-web.pdf

[14] Ibid.

[15] https://www.fema.gov/pdf/plan/glo.pdf

[16] https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf

[17] Critical Infrastructure Sectors | CISA

[18] https://law.hawaii.gov/ohs/wp-content/uploads/sites/2/2024/01/cisrp-2023-final-web.pdf

[19] https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf

[20] https://law.hawaii.gov/ohs/wp-content/uploads/sites/2/2024/01/cisrp-2023-final-web.pdf

TERM	DEFINITION
Cultural Resources	The remains or records of districts, sites, structures, buildings, networks, neighborhoods, objects, and events from the past. These resources may be historic, prehistoric, archaeological, or architectural in nature. Cultural resources are irreplaceable and nonrenewable aspects of our national heritage.[21]
Cultural Significance	Aesthetic, historic, scientific, social, or spiritual value for past, present, or future generations. Cultural significance is embedded in places themselves, their fabric, settings, uses, associations, meanings, records, related places, and related objects.[22]
Cyber Infrastructure	Electronic information and communications systems and services.[23]
Dependency	Relationship of reliance within and among infrastructure systems must be maintained for those systems to function or provide services. Dependencies can be bi-directional in nature.[24]
Economic Consequence	Refers to the effect of an incident, event, or occurrence on the value of property or on the production, trade, distribution, or use of income, wealth, or commodities.[25]
Economic Security	The ability of individuals, households, and communities to meet their basic and essential needs sustainably, including food, shelter, clothing, health care, education information, livelihoods, and social protection.[26]
Evaluation	Assessing the effectiveness of planning at achieving its stated goals, objectives, and performance measures.[27]
Hazard	Natural or manmade source or cause of harm or difficulty.[28]
Health	A state of complete physical, mental, and social well-being and not merely the absence of disease or infirmity.[29]
Implementing Partner	The organization (federal, state, academic, local, nonprofit, faith-based, or private) that provides support, resources, subject matter expertise, etc. to carry out/support activities within the implementation plan.
Informed	The 'Informed' category includes the people who are to be kept in the loop over the course of the project. They need to be informed about the progress of the project every step of the way, up until it reaches completion.
Information Sharing	The bi-directional sharing of timely and relevant information concerning risks to critical infrastructure.[30]
Interdependency	Mutually reliant relationship between entities (objects, individuals, or groups); the degree of interdependency does not need to be equal in both directions.[31]
Livability	Principles that act as a foundation for interagency coordination.[32] Examples include: Provide more transportation choices; promote equitable, affordable housing; enhance economic competitiveness; support existing communities; coordinate policies and leverage investment; and value communities and neighborhoods.
Mitigation	The capabilities necessary to reduce loss of life and property by lessening the impact of disasters[33] The capabilities necessary to reduce loss of life and property by lessening the impact of threats[34]
Monitoring	Tracking the implementation of the prioritized resilience solutions.[35]
Objective	Specific, measurable statement that supports the achievement of a goal.[36]

[21] https://www.ecfr.gov/current/title-7/subtitle-B/chapter-XXXI/part-3100

[22] https://australia.icomos.org/wp-content/uploads/The-Burra-Charter-2013-Adopted-31.10.2013.pdf

[23] https://law.hawaii.gov/ohs/wp-content/uploads/sites/2/2024/01/cisrp-2023-final-web.pdf

[24] https://law.hawaii.gov/ohs/wp-content/uploads/sites/2/2024/01/cisrp-2023-final-web.pdf

[25] https://iadclexicon.org/economic-consequence/

[26] https://gsdi.unc.edu/our-work/economic-security/

[27] https://law.hawaii.gov/ohs/wp-content/uploads/sites/2/2024/01/cisrp-2023-final-web.pdf

[28] Ibid.

[29] https://www.who.int/data/gho/data/major-themes/health-and-well-being

[30] https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/

[31] https://law.hawaii.gov/ohs/wp-content/uploads/sites/2/2024/01/cisrp-2023-final-web.pdf

[32] https://www.hud.gov/program_offices/economic_development/six_livability_principles

[33] https://law.hawaii.gov/ohs/wp-content/uploads/sites/2/2024/01/cisrp-2023-final-web.pdf

[34] OHS Definition specific to OHS mission space

[35] Ibid.

[36] Ibid

TERM	DEFINITION
Physical Infrastructure	Tangible structures or facilities and components that provide infrastructure sector services to communities or regions providing services.[37]
RASCI	The RASCI Matrix is a project management tool to assign roles and responsibilities. RASCI stands for Responsible, Accountable, Support, Consulted, and Informed.
Resilience	The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions; includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.[38]
Resource	Personnel, equipment, teams, supplies, and facilities available or potentially availa-ble for assignment to incident operations and for which status is maintained. Resources are described by kind and type and may be used in operational support or supervisory capacities at an incident or at an emergency operations center (EOC).[39]
Responsible	The organization that is assigned to track the completion of activities within the implementation plan. OHS is identified as the "Responsible" party within this plan.
Risk	The potential for an adverse outcome assessed as a function of threats, vulnerabilities, and consequences associated with an incident, event, or occurrence, often measured, and used to compare different future situations.[40]
Risk Assessment	An evaluation that considers the types of threats and hazards that threaten community infrastructure systems and weighs vulnerable community infrastructure.[41]
Sector	A collection of assets, systems, networks, entities, or organizations that provide or enable a common function for national security (including national defense and continuity of Government), national economic security, national public health or safety, or any combination thereof.[42]
Security	Reducing the risk to critical infrastructure by physical means or defensive cyber measures to intrusions, attacks, or the effects of natural or man-made threats/disasters.[43]
Stakeholder	A party or entity that delivers depends on, or is affected by infrastructure service or facility operations, plans, or decisions under consideration.[44]
Subsector	A subset of a sector comprised of critical infrastructure grouped by common resources, common equities, or common functions.[45]
Supportive	"Supportive" members may provide help by providing resources to the Responsible organization. They actively work with the Responsible organization to support the completion of activities.
Threat	A natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.[46]
Vulnerability	Characteristic of design, location, security posture, operation, or any combination thereof, that enters an entity, asset, system, network, or geographic area susceptible to disruption, destruction, or exploitation.[47]

[37] Ibid.

[38] Ibid.

[39] https://training.fema.gov/emiweb/is/icsresource/assets/glossary%20of%20related%20terms.pdf

[40] https://law.hawaii.gov/ohs/wp-content/uploads/sites/2/2024/01/cisrp-2023-final-web.pdf

[41] Ibid.

[42] https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/

[43] Ibid.

[44] Ibid.

[45] https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/

[46] https://law.hawaii.gov/ohs/wp-content/uploads/sites/2/2024/01/cisrp-2023-final-web.pdf

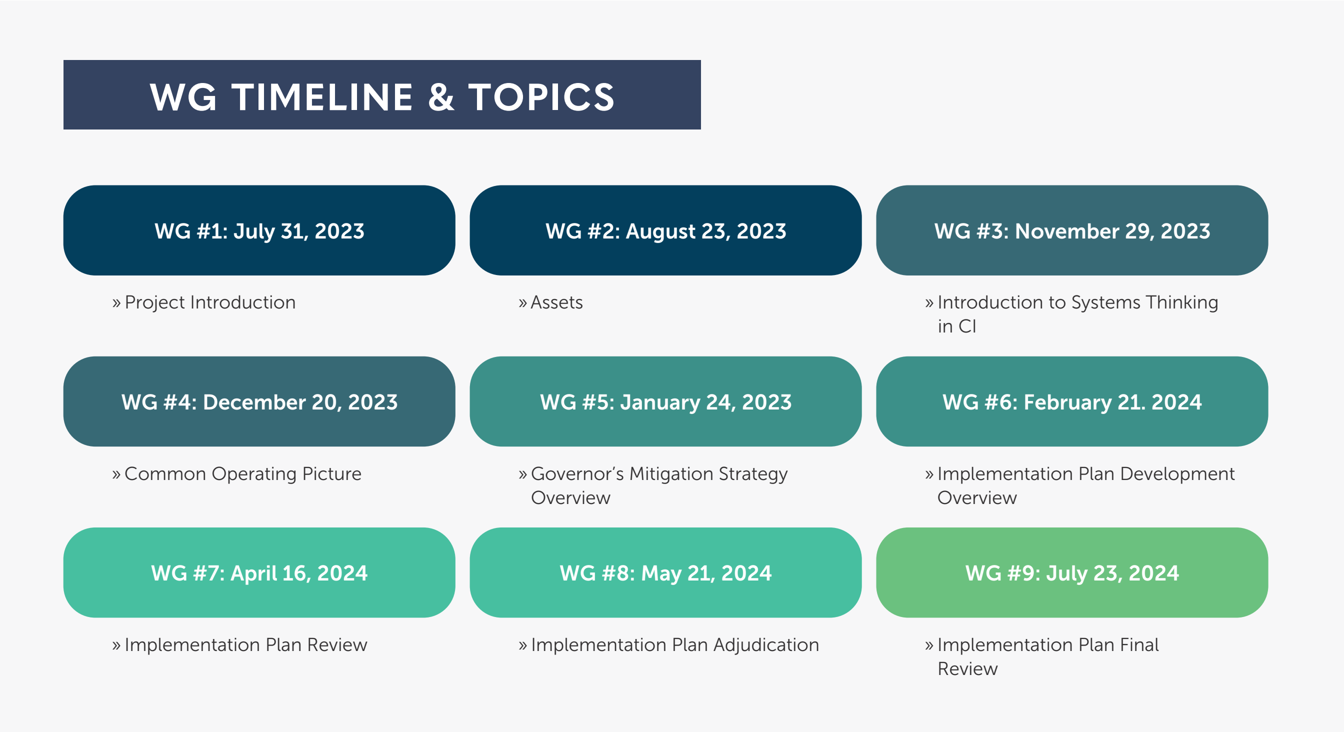
[47] https://law.hawaii.gov/ohs/wp-content/uploads/sites/2/2024/01/cisrp-2023-final-web.pdf

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D: STAKEHOLDER ENGAGEMENT

Appendix D documents the coordination meetings that took place in accordance with the development of this implementation plan.

OHS hosted a series of WGs to engage stakeholders in the implementation planning process. **Figure D-2** summarizes the planning meetings that took place.



WG TIMELINE & TOPICS

WG #1: July 31, 2023

- » Project Introduction

WG #2: August 23, 2023

- » Assets

WG #3: November 29, 2023

- » Introduction to Systems Thinking in CI

WG #4: December 20, 2023

- » Common Operating Picture

WG #5: January 24, 2023

- » Governor's Mitigation Strategy Overview

WG #6: February 21. 2024

- » Implementation Plan Development Overview

WG #7: April 16, 2024

- » Implementation Plan Review

WG #8: May 21, 2024

- » Implementation Plan Adjudication

WG #9: July 23, 2024

- » Implementation Plan Final Review

Figure D-1: *Working Group Timeline & Topics*

In addition to the WG meetings, OHS also conducted over 30 separate meetings (see **Table D-1**) to address the focus topics shown in **Figure D-1**.

Table D-1: *Information Sharing and Collaboration Meetings*

INFORMATION SHARING AND COLLABORATION MEETINGS	
JULY 20, 2023	OHS Quarterly HLS Forum
AUGUST 31, 2023	GIS Advantage Program Meeting
	Idaho National Laboratory (INL) All Hazards Analysis (AHA) Discussion
SEPTMBER 1, 2023	Maui County GIS Briefing
SEPTEMBER 6, 2023	CISA Gateway Meeting
SEPTEMBER 15, 2023	Department of Transportation (DOT) Briefing
SEPTEMBER 18, 2023	Verizon Briefing
OCTOBER 4, 2023	OHS Quarterly HLS Forum
OCTOBER 21, 2023	Statewide Interoperability Coordinators (SWIC) Briefing
OCTOBER 17, 2023	GIS Coordination Briefing with County GIS Representatives
OCTOBER 30, 2023	Minnesota Geospatial Advisory Council (MGAC) Introductory Meeting
NOVEMBER 13, 2023	Systems-Level Maps Discussion: Department of Transportation
	Systems-Level Maps Discussion: Department of Energy
NOVEMBER 14, 2023	MGAC Follow-Up Meeting
NOVEMBER 21, 2023	Systems-Level Briefing - SWIC
	Systems-Level Briefing - AT&T
	Systems-Level Briefing - Honolulu Board of Water Supply (HBWS)
NOVEMBER 22, 2023	Systems-Level Briefing - University of Hawaiʻi
NOVEMBER 27, 2023	Systems-Level Briefing - California Governor's Office of Emergency Services Briefing
NOVEMBER 28, 2023	Systems-Level Briefing - Chief Information Security Officer
NOVEMBER 30, 2023	HI-EMA GIS Briefing
DECEMBER 7, 2023	City and County of Honolulu DEM Infrastructure Coordination
	South Carolina GIS Briefing
DECEMBER 8, 2023	CISA Gateway Training/Intro
	City and County of Honolulu Wastewater Systems Discussion
DECEMBER 11, 2023	Kauaʻi County GIS Discussion
DECEMBER 14, 2023	COP Demo #1
JANUARY 3, 2024	COP Demo #2
JANUARY 4, 2024	Converge/INL Workshop Status Update
JANUARY 10, 2024	COP Discussion
FEBRUARY 16, 2024	Hawaiʻi County GIS Discussion
FEBRUARY 23, 2024	Chief Data Officer (CDO) Meeting
FEBRUARY 28, 2024	Maui County GIS Discussion
MARCH 6-7, 2024	CI Workshop
MARCH 14, 2024	City & County of Honolulu GIS Meeting
APRIL 4, 2024	CISRP Implementation Plan Design Meeting
MAY 23, 2024	CISA Brief
	Utah Critical Infrastructure Prioritization (UCP) Introduction

APPENDIX E: REFERENCES

The City and County of Honolulu (Oahu) Comprehensive Economic Development Strategy (CEDS) 2022 https://www.oedb.biz/ceds#:~:text=our%20island%20home.-,The%20City%20and%20County%20of%20Honolulu%20(Oahu)%20Comprehensive%20Economic%20Development,for%20the%20island%20of%20Oahu.%E2%80%9D

Cybersecurity and Infrastructure Security Agency. (2013). National Infrastructure Protection Plan. https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf

Cybersecurity and Infrastructure Security Agency. (2023). Infrastructure Resilience Planning Framework. https://www.cisa.gov/resources-tools/resources/infrastructure-resilience-planning-framework-irpf

Federal Emergency Management Agency. (n.d.). Community Rating System Self-Assessment Tool. https://crsselfassessment.us/what-is-a-critical-facility/

Federal Emergency Management Agency. (1996). State and Local Guide (SLG) 101: Guide for All-Hazard Emergency Operations Planning. https://www.fema.gov/pdf/plan/glo.pdf

Federal Emergency Management Agency. (2010). Developing and Maintaining Emergency Operations Plans: Comprehensive Preparedness Guide (CPG) 101. https://www.fema.gov/sites/default/files/documents/fema_cpg-101-v3-developing-maintaining-eops.pdf

Federal Emergency Management Agency. (2018). Glossary of Related Terms: Extracted from E/L/G 0300 Intermediate Incident Command System for Expanding Incidents. https://training.fema.gov/emiweb/is/icsresource/assets/glossary%20of%20related%20terms.pdf

Federal Emergency Management Agency. (2020). Unified Federal Review (UFR) Glossary. https://www.fema.gov/sites/default/files/2020-06/ufr_glossary.pdf

Federal Emergency Management Agency. (2023). 2023-2027 FEMA Data Strategy. https://www.fema.gov/sites/default/files/documents/fema_data-strategy-2023-2027.pdf

Global Social Development Innovatations. (2024). Economic Security. https://gsdi.unc.edu/our-work/economic-security/

GoodCore. (2019). A Comprehensive Guide to the RACI/RASCI Model. https://www.goodcore.co.uk/blog/a-guide-to-the-raci-rasci-model/

Hawaiʻi Emergency Management Agency. (2023). Hawaiʻi State Hazard Mitigation Plan: Section 4.12 Terrorism. https://dod.hawaii.gov/hiema/final-2023-hazard-mitigation-plan/

International Association of Drilling Contractors. (2024). Oil and Gas Drilling Glossary: Economic Consequence. https://iadclexicon.org/economic-consequence/

International Council on Monuments and Sites (ICOMOS). (2013). The Burra Charter: The Australia ICOMOS Charter for Places of Cultural Significance. https://australia.icomos.org/wp-content/uploads/The-Burra-Charter-2013-Adopted-31.10.2013.pdf

National Archives and Records Administration. (2024). Code of Federal Regulations. https://www.ecfr.gov/current/title-7/subtitle-B/chapter-XXXI/part-3100

National Security Memorandum on Critical Infrastructure Security and Resilience. (2024). The White House. https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/

State of Hawaiʻi Office of Homeland Security. (2023). Hawaiʻi Critical Infrastructure Security and Resilience Program. https://law.hawaii.gov/ohs/wp-content/uploads/sites/2/2024/01/cisrp-2023-final-web.pdf

United States Department of Housing and Urban Development. (n.d.). Six Livability Principles. https://www.hud.gov/program_offices/economic_development/six_livability_principles

World Health Organization Global Health Observatory. (n.d.). Health and Well-Being. https://www.who.int/data/gho/data/major-themes/health-and-well-being

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX F: PLAN MAINTENANCE

OHS is responsible for maintaining this Implementation Plan and coordinating revisions on a recurring basis. OHS' maintenance responsibilities include:

- Maintaining a plan review schedule (which may include stakeholders)
- Reviewing all plan components and proposed changes for consistency
- Obtaining approvals for changes from the appropriate authorities and notifying stakeholders of approved changes
- Maintaining a record of changes

This plan requires two types of reviews, each with a distinct purpose: the CI Implementation Plan review and the CI dataset review. The Implementation Plan review focuses on the processes, procedures, and requirements within the Implementation Plan itself, while the dataset review ensures that the stakeholder datasets included within the CI COP are accurate and up to date.

The purpose of the COP is to provide a well-established and managed geospatial aspect to enhance situational awareness; however, CI data originates from various public and private sources, and the data attributes and quality are fragmented by nature. As a result, OHS will furnish decision-makers with a singular, geospatial tool, and coordinate with stakeholders throughout plan implementation to review and consolidate available datasets into an integrated geospatial data system, that forms the CI COP.

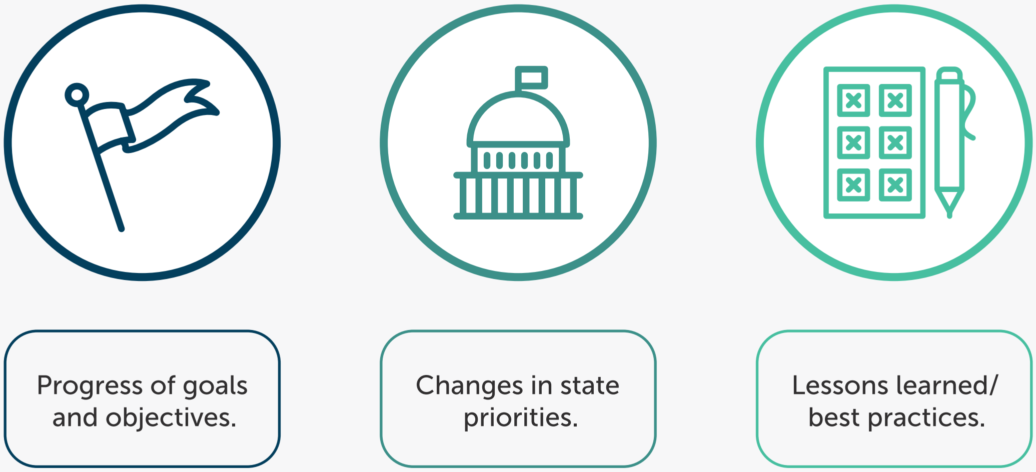
OHS will safeguard all information contained in the CI COP following the Cybersecurity Infrastructure and Security Agency (CISA) Protected Critical Infrastructure Information (PCII) Program (see **Figure F-1**).[48] OHS will create the CI COP to be a secure, permission-based, PCII-protected, cloud-based solution exclusively accessible to authorized personnel. This tool will allow OHS and stakeholders to rapidly visualize facilities, discern dependencies, and inform long-term resilience investment decisions. Success in this initiative will enhance OHS' overall situational awareness, interdepartmental coordination, and response, all contributing to comprehensive CI resilience efforts throughout Hawai'i.

Figure F-1: *CISA PCII Program*

PLAN REVIEW CYCLE

OHS will conduct an Implementation Plan review and update every three years and may conduct the plan review simultaneously with the CI dataset review. OHS will consider several factors during the plan review, to include those in **Figure F-2**.

[48] https://www.cisa.gov/resources-tools/programs/protected-critical-infrastructure-information-pcii-program



Progress of goals and objectives.

Changes in state priorities.

Lessons learned/ best practices.

Figure F-2: *Plan Review Considerations*

PLAN UPDATE PROCEDURES

OHS will follow the steps outlined in **Table F-1** to update the Implementation Plan on a six-month cycle.

Table F-1: *Information sharing and collaboration meetings timeline*

PLAN MAINTENANCE PROCEDURES	
TIMELINE	**ACTION**
APRIL 2027	Identify a plan review team.
MAY 2027	Review the existing plan to identify gaps, outdated information, or areas needing improvement.
JUNE 2027	Conduct plan review coordination meetings with stakeholders to gather their feedback on plan implementation.
JULY 2027	Collect feedback/proposed changes and adjudicate proposed changes.
AUGUST 2027	Make updates to the plan where necessary and present updated sections to stakeholders for their approval.
SEPTEMBER 2027	Finalize and document the updates.

OHS may consider whether the plan requires any updates based on several factors to include the following questions shown in **Table F-2**, which aim to assess the plan's effectiveness and identify required critical improvements or enhancements:

Table F-2: *OHS Plan Update Considerations*

QUESTIONS OHS WILL ASK	
01	Are the plan's goals and activities still representative of Hawai'i's/OHS' priorities?
02	Has there been meaningful progress toward achieving the goals and implementing the activities?
03	Has the completion of activities resulted in the expected outcomes?
04	Did the activity help achieve plan goals? If the activity was not completed, what were the barriers to implementation (e.g., political, financial, technical, etc.)?
05	Should the activity remain in the strategy for the updated plan?
06	How can lessons learned from implementation of these activities inform development and implementation of future strategies and actions to reduce risk and vulnerability?
07	Are the current capabilities and resources adequate to implement the plan as scheduled? If not, what are the key gaps or shortfalls?
08	Have there been any changes to federal or state laws, authorities, regulations, funding, technology, community dynamics, or other measures that necessitate specific revisions or amendments to the plan?
09	Are there new data, techniques, or approaches that must be considered and integrated into the existing solution?
10	Has there been any new developments or improvements in the areas susceptible to a threat that warrant an update?

CI IMPLEMENTATION PLAN REVIEW/UPDATE CHECKLIST

OHS will coordinate with stakeholders as needed to assist with a systematic assessment of the Implementation Plan to validate its relevance, progress, effectiveness, and impact. The following checklist contains prompts for consideration:

1. Review progress of Implementation Plan:

□ Review the existing plan to understand its components, objectives, and implementation status.

□ Identify any gaps, outdated information, or areas needing improvement.

2. Stakeholder Engagement:

□ Involve relevant stakeholders, including team members, subject matter experts, and external partners.

□ Seek input on what worked well, challenges faced, and potential updates.

3. Assess External Factors:

□ Consider changes in the external environment (e.g., regulations, technology, community dynamics).

□ Evaluate how these factors impact the plan's relevance and effectiveness.

4. Data Collection and Analysis:

□ Review data on plan performance, outcomes, and any emerging risks.

□ Analyze trends, patterns, and lessons learned.

5. Set Priorities:

□ Prioritize areas for improvement.

□ Focus on critical aspects that need immediate attention.

6. Update Goals and Objectives:

□ Revise or refine the plan's goals and objectives to align with current needs.

□ Ensure they remain specific, measurable, achievable, relevant, and time-bound (SMART).

7. Modify Activities:

□ Adjust existing activities or develop new ones.

□ Consider innovative approaches or best practices.

8. Resource Allocation:

□ Evaluate available resources (e.g., financial, human, technological).

□ Allocate resources effectively to support plan implementation.

9. Timeline and Milestones:

□ Update timelines for activities and milestones.

□ Ensure realistic deadlines and clear accountability.

10. Communication Plan:

□ Implement communication strategy to inform stakeholders about the plan update.

□ Share the revised plan and seek feedback.

11. Document Changes:

□ Adjudicate stakeholder feedback and clearly document all updates, including rationale and decision-making process.

□ Maintain version control to track changes over time/Update Change Control Log.

12. Training and Awareness:

□ Train stakeholders on the updated plan.

OUT OF CYCLE UPDATES

OHS may accelerate the update schedule following any events or concurrent with the development of a recovery or post-event recovery/redevelopment plan. Following an event, OHS can leverage the greater awareness and interest in resilience by engaging stakeholders to identify and address gaps and improve this plan. Additional funding sources may also be available after an incident that stakeholders can use for plan implementation and resilience solutions. An out of cycle update allows the CI community to address any changes in vulnerabilities and priorities, goals, and objectives. See **Figure F-3** for reasons that OHS may coordinate an "Out of Cycle" data update.

OUT OF CYCLE REASONING

- New guidance from senior leadership
- Changes to relevant county, state, and federal CI-related capabilities
- Changes to relevant county, state, and federal CI-related roles, and responsibilities
- Critical facility updates (e.g., new CI facilities, generators, etc.)
- Change in facility status (e.g., facility has shut down or moved)
- Administrative revisions such as updated terminology, POC information, or agency names
- Changes to risk and vulnerability analysis and planning assumptions
- Relevant changes in federal or state laws, policies, structures, capabilities, or other changes to emergency management standards or best practices
- Substantive lessons learned from exercises, incident analysis, or program evaluations

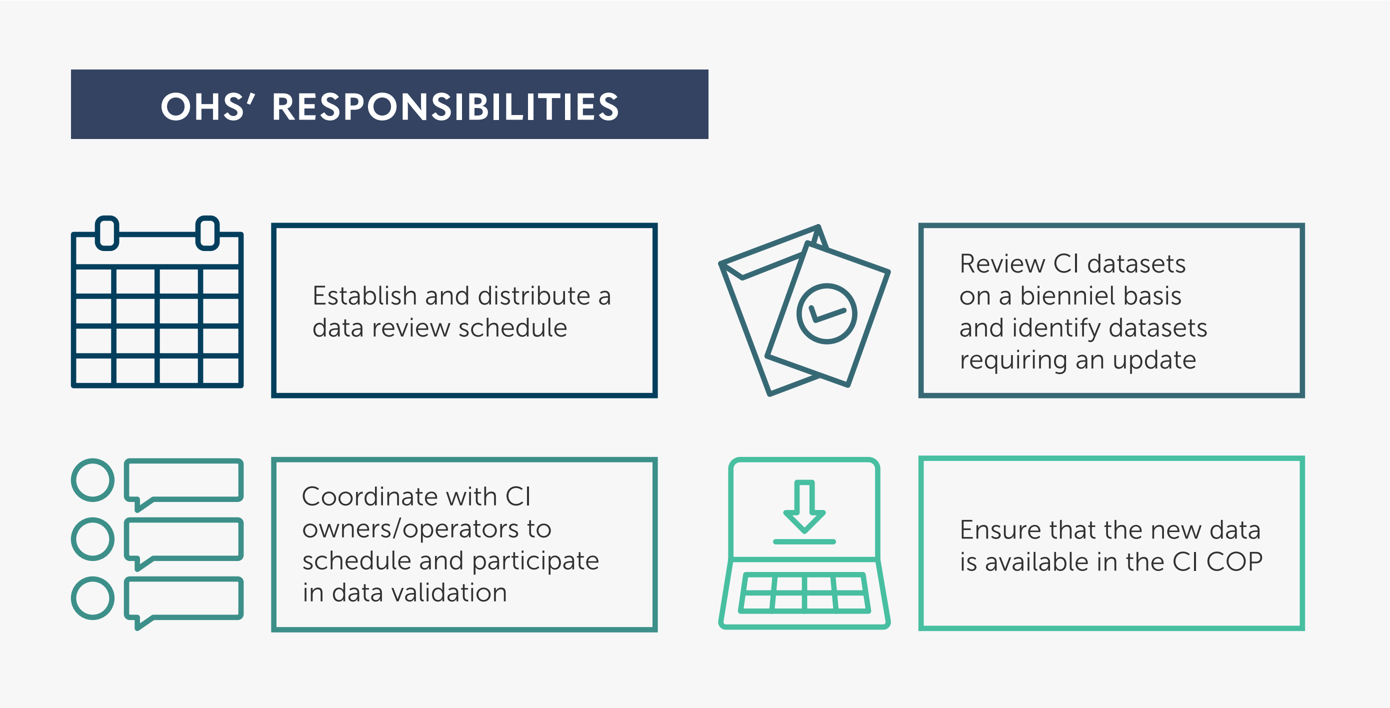
Figure F-3: *Out of Cycle Data Updates*

CI DATASET UPDATE PROCEDURES

OHS plans to rely on data sets that are maintained primarily by CI owner/operators. OHS will review the status of CI datasets every two years as shown in **Table F-3**. See **Figure F-4** for OHS' responsibilities related to data maintenance.

Table F-3: *OHS Plan Update Considerations*

TIER	CI LIST DEVELOPED	REVIEW
01	2024	2026
02	2025	2027
03	2026	2028



OHS’ RESPONSIBILITIES

Establish and distribute a data review schedule

Review CI datasets on a bienniel basis and identify datasets requiring an update

Coordinate with CI owners/operators to schedule and participate in data validation

Ensure that the new data is available in the CI COP

Figure F-3: *OHS’ Data Updates Responsibilities*