Homeland Security Forum

Office of Homeland Security

Ft. Ruger
Rm 113, Bldg 306
3949 Diamond Head Rd, Honolulu HI 96816
(and Teams)

19 Septmber 2024

For Your Convenience

RESTROOMS

Right out the meeting room doors, immediately past entrance hall on right

WIFI INFO

SSID Name: WiFi SOH-Guest

Username: Law.wifi@hawaii.gov

Password: D2faC

IN CASE OF EMERGENCY

Left out the meeting room doors, through double door exit, muster out pedestrian gate in visitor parking lot.

Agenda

08:00	***Networking***
08:30	**Welcome, Administrative Remarks** (Frank Pace, OHS Administrator)
08:45	**Threat Brief** (Kevin Baggs, Hawaii State Fusion Center Director)
09:15	**Elections Security Progress, Challenges, and Work Leading up to November** (Scott Nago, State Elections Officer)
10:00	***Break***
10:15	**OHS Planning Update** **Cyber Incident Response Plans and Exercises; Workforce Development** (Nick Matthews) **Critical Infrastructure Security and Resilience** (Michael Covert)
11:00	**Cybersecurity Program – Progress on grant allocations** (Jimmie Collins, OHS Chief Planning & Operations)
11:30	***Lunch Break***
12:30	**Fusion Liaison Officer Program** (Kevin Baggs, Hawaii State Fusion Center Director)
12:45	**Training & Exercises - Calendar of Events** (Jimmie Collins, OHS Chief Planning & Operations)
1:00	***Break***
1:15	**Impacts of Disinformation and Foreign Influence During Disaster Response** (Frank Pace, OHS Administrator)
2:00	~~**Targeted Violence and Conflict Resolution in Our Communities** (tentative; Dr. Michael Champion, Senior Advisor for Mental Health and the Justice System, Office of Governor)~~
2:45	***Open Discussion***
3:15	**Closing Comments** (Frank Pace, OHS Administrator)
3:20	***Adjourn***

Threat Brief

2024 Election Security

Mis-, Dis-, and Malinformation Threat Picture

- Physical Threats
  - Elected Officials, Political Candidates, Elections Workers & Volunteers
  - Voter Service Centers/Ballot Drop Boxes
- Election Process Threats
  - Confidence in democratic processes

48.7%	47 DAYS 18 HRS 05 MINS 13 SECS	**18+**
2022 Statewide Voter Turnout	**Time until the General Election** (November 5, 2024)	**Age required to vote in elections**

2024 Election Security

Mis-, Dis-, and Malinformation

- **Misinformation** – Information that is false, but not created or shared with the intention of causing harm.
- **Disinformation** – False information that is deliberately created to mislead, harm, or manipulate a person, organization, or county.
- **Malinformation** – Information that is based on fact, but used out of context to mislead, harm or manipulate a person, organization or country

2024 Election Security

Mis-, Dis-, and Malinformation

- WHO
  - Foreign Malign Influence
    - Russian, Chinese and Iranian state-sponsored
  - Social Media Influencers
  - Scammers
  - Cyber Criminals

- WHY
  - Create chaos
  - Generate division
  - Promote agendas
  - Manipulate opinion
  - Generate SM activity
  - Undermine confidence in election process

FBI & CISA Public Service Announcement

- FBI and CISA issued an announcement to raise awareness of attempts to undermine public confidence in the security of U.S. elections infrastructure through spread of disinformation and falsely claiming that cyber attacks compromised U.S. voter registration databases.
  - Do not accept claims of intrusion at face value, and remember that these claims may be meant to influence public opinion and undermine the American people's confidence in our democratic process.
  - Be cautious of social media posts, unsolicited emails from unfamiliar email addresses, or phone calls or text messages from unknown phone numbers that make suspicious claims about the elections process or its security.
  - If you have questions about election security and/or administration in your jurisdiction, rely on state and local government election officials as your trusted sources for election information.
  - Visit your state and local elections office websites for accurate information about the elections process. Many of these offices have websites that use a ".gov" domain, indicating they are an official government site.

Recent Election-Related Incidents Nationwide

- White Sands New Mexico
- June 20, 2024
- Marine Corps Veteran arrested and charged federally In New Mexico
- US Army Base had to cancel scheduled trainings

The El Paso Times

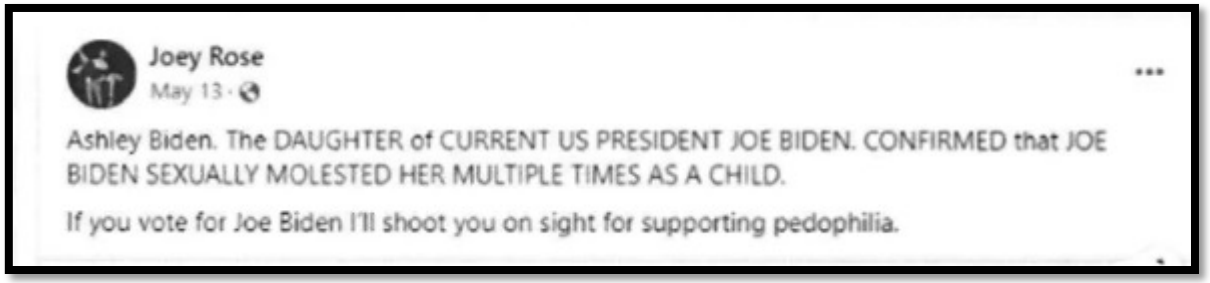
Veteran arrested for making threats against federal employees, President Biden supporters

Aaron Martinez, El Paso Times

Updated June 22, 2024 · 3 min read

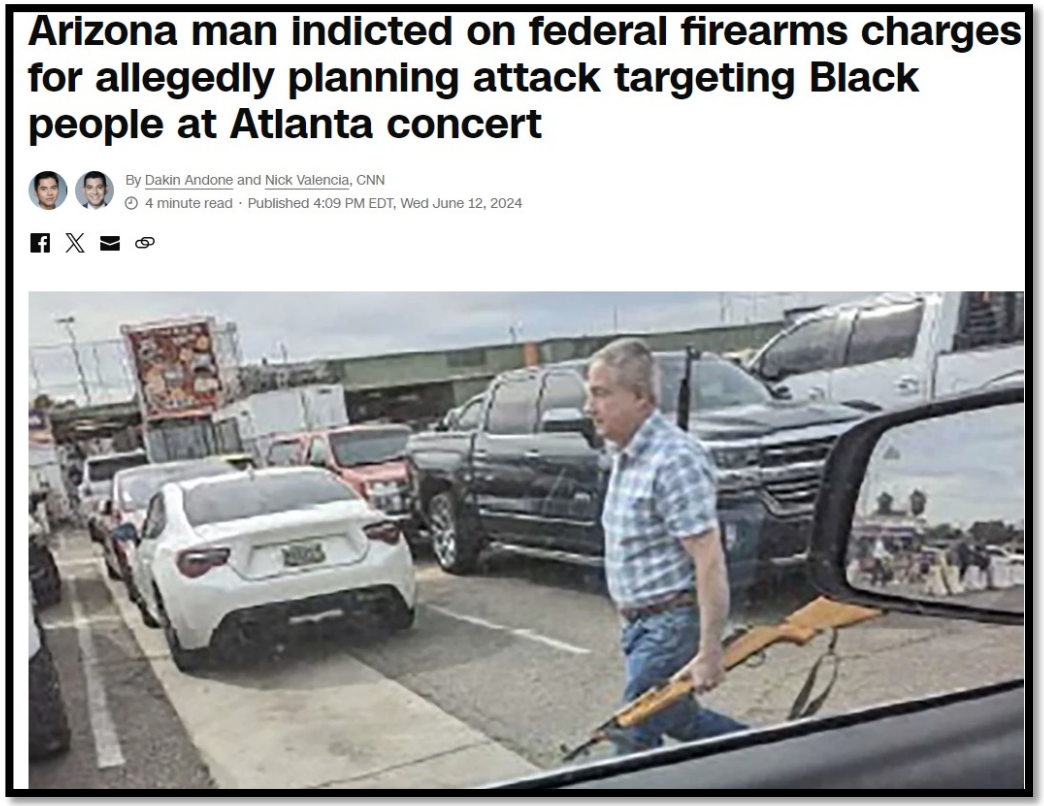
38

Social media posts declare war on U.S., threatens Biden supporters



Recent Election-Related Incidents Nationwide

- June 11, 2024 New Mexico
- Hoped to incite a race war prior to the upcoming presidential election
- Had 7 firearms at the time of his arrest
- He sold assault rifles to FBI informants whom he believed shared his racist ideologies
- Targeted a Rap concert because he believed there would be a high concentration African Americans
- Targeted Georgia because he perceived the politics were shifting as a result of the Black population



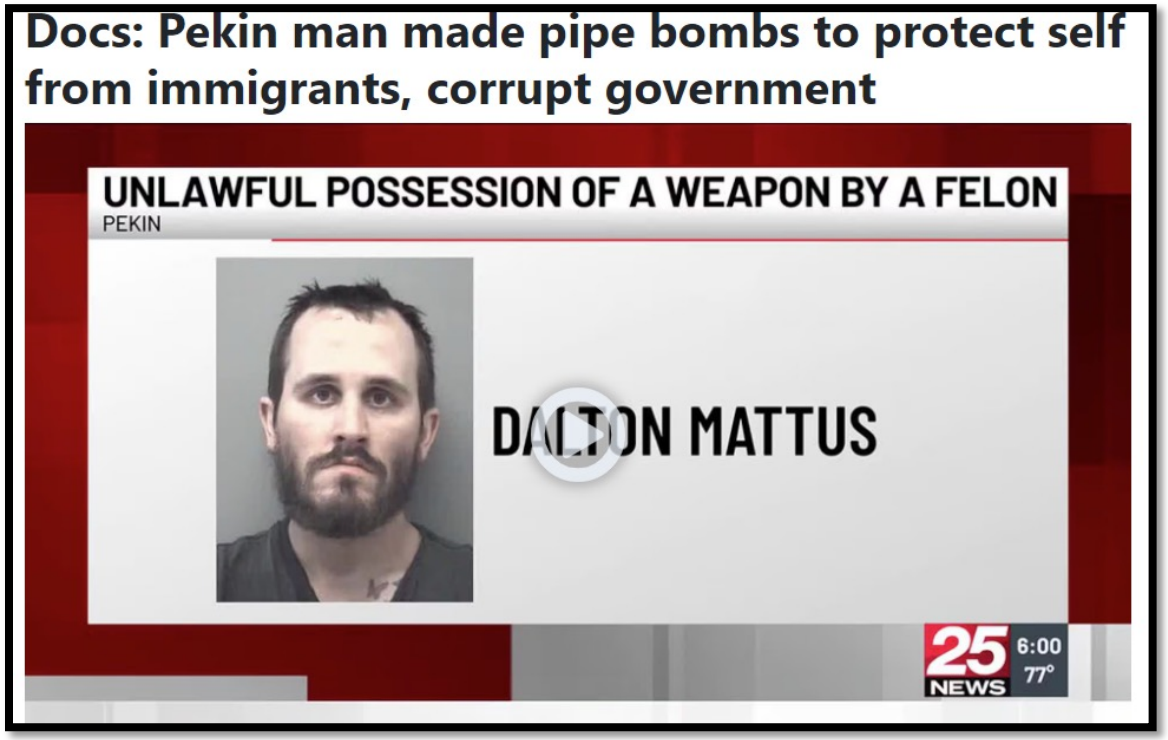
Arizona man indicted on federal firearms charges for allegedly planning attack targeting Black people at Atlanta concert

By Dakin Andone and Nick Valencia, CNN

4 minute read · Published 4:09 PM EDT, Wed June 12, 2024

Recent Election-Related Incidents Nationwide

- May 17, 2024 Pekin, Illinois
- Social media posts promoting a civil war to kill democrat politicians
- Perceived election fraud



Recent Election-Related Incidents Nationwide

- 11 March 2024 Waterville, Maine
- Threats to
  - President Biden
  - Former President Obama
  - George Soros
  - LGBTQ+ community
  - Mexican politicians
  - Manhattan District Attorney Alvin Bragg
  - FBI,
  - CIA
  - Stockpiling weapons in preparation of Civil War
  - Immigrants

Waterville man arrested by FBI over online threats suffers from mental illness, family says

Benjamin Brown, 45, was arrested March 11 by the FBI over online threats to gun down President Biden, other politicians and immigrants and is being held pending further appearance in U.S. District Court in Bangor.

Recent Election-Related Incidents Nationwide

- 30 January 2024 Levittown Pennsylvania
- Called for a civil war to "Fight the Democrats"
- Father was a federal employee
- Called his father a traitor
- Encouraged violence against government officials
- Fled to a National Guard Facility
- 20 minute video espoused numerous conspiracy theories
  - Biden Administration
  - Immigration and the border
  - Fiscal policy
  - Urban crime
  - War in Ukraine

Recent Election-Related Incidents Nationwide

Trump Assassination Attempts:

13 July 2024
- Butler, Pennsylvania
- One rally attendee killed and two critically wounded

15 September 2024
- West Palm Beach Florida
- Suspect resided in Hawaii

Violent threats and attacks escalate tensions in Trump-Harris race

The 2024 election season has been repeatedly marked by extraordinary acts and threats of violence, prompting heightened security measures at events.

11 min 3688

So, What Can Be Done?

- Rely on trusted sources:
  - State and local election authority websites
  - Verified social media accounts from government sources
- Understand warning signs of Pathway to Violence
- Threat Team Hawaii
- Report suspicious activity to the HSFC
- Go to the OHS Elections Website for more resources

Resources for Educators, Parents and Students

Resource	Link
Civic Online Reasoning Curriculum (Stanford)	Click Here to Visit
Poynter Institute Fact Checking Games for Youth	Click Here to Visit
GovTech: Libraries Fighting Election Disinformation	Click Here to Visit
American Library Association: Fighting Misinformation	Click Here to Visit
MIT: Talking to Teens about Misinformation	Click Here to Visit

Understanding AI

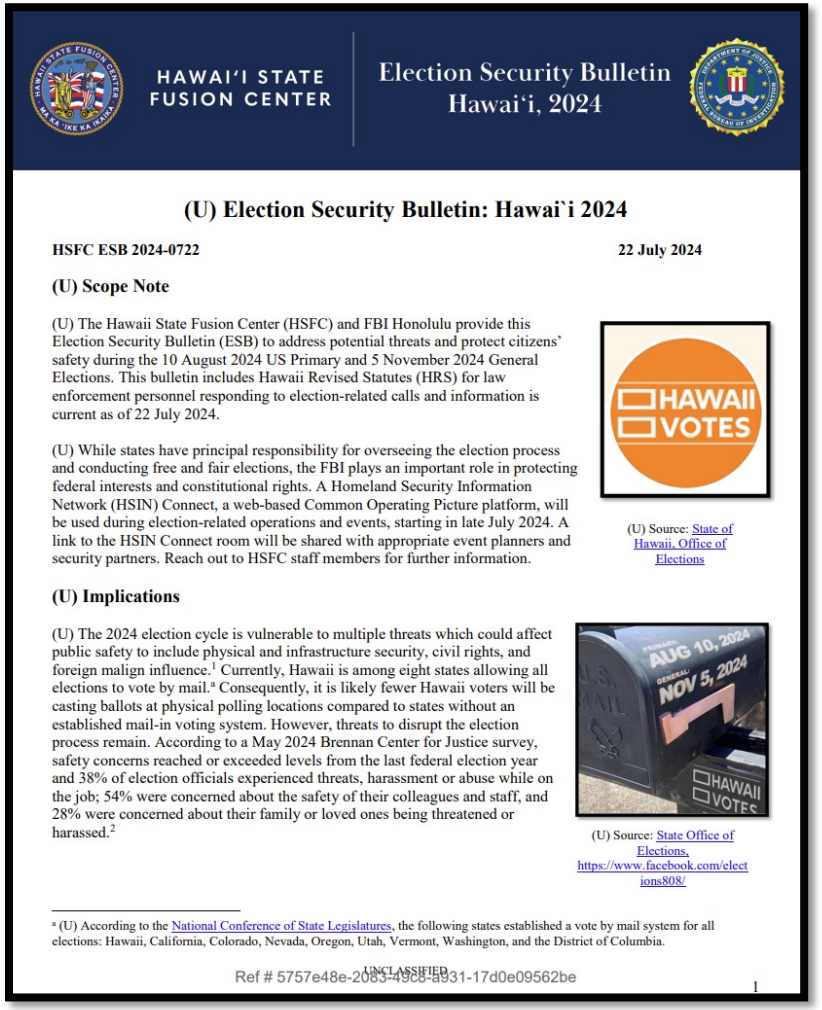
Resource	Link
IBM Definition of AI	Click Here to Visit
Google Definition of AI	Click Here to Visit
Microsoft: Artificial Intelligence (AI) vs Machine Learning (ML)	Click Here to Visit
CISA Roadmap for AI	Click Here to Visit
Sample AI Detector by Content at Scale	Click Here to Visit
Sample AI Detector by Scribbr	Click Here to Visit
Play an AI Drawing and Guessing Game by Google	Click Here to Visit

(U) Resources:
https://law.hawaii.gov/ohs/elections/

HSFC Election-Related Products

Important Date Reminders:

- 18 October 2024 Voters receive ballots (sent via mail)
- 22 October 2024 Voter Service Centers open
- 05 November 2024 Election Day General



HAWAI'I STATE FUSION CENTER

Election Security Bulletin Hawai'i, 2024

(U) Election Security Bulletin: Hawai`i 2024

HSFC ESB 2024-0722 **22 July 2024**

(U) Scope Note

(U) The Hawaii State Fusion Center (HSFC) and FBI Honolulu provide this Election Security Bulletin (ESB) to address potential threats and protect citizens' safety during the 10 August 2024 US Primary and 5 November 2024 General Elections. This bulletin includes Hawaii Revised Statutes (HRS) for law enforcement personnel responding to election-related calls and information is current as of 22 July 2024.

(U) While states have principal responsibility for overseeing the election process and conducting free and fair elections, the FBI plays an important role in protecting federal interests and constitutional rights. A Homeland Security Information Network (HSIN) Connect, a web-based Common Operating Picture platform, will be used during election-related operations and events, starting in late July 2024. A link to the HSIN Connect room will be shared with appropriate event planners and security partners. Reach out to HSFC staff members for further information.

HAWAII VOTES

(U) Source: State of Hawaii, Office of Elections

(U) Implications

(U) The 2024 election cycle is vulnerable to multiple threats which could affect public safety to include physical and infrastructure security, civil rights, and foreign malign influence.[1] Currently, Hawaii is among eight states allowing all elections to vote by mail.[a] Consequently, it is likely fewer Hawaii voters will be casting ballots at physical polling locations compared to states without an established mail-in voting system. However, threats to disrupt the election process remain. According to a May 2024 Brennan Center for Justice survey, safety concerns reached or exceeded levels from the last federal election year and 38% of election officials experienced threats, harassment or abuse while on the job; 54% were concerned about the safety of their colleagues and staff, and 28% were concerned about their family or loved ones being threatened or harassed.[2]

(U) Source: State Office of Elections, https://www.facebook.com/elections808/

[a] (U) According to the National Conference of State Legislatures, the following states established a vote by mail system for all elections: Hawaii, California, Colorado, Nevada, Oregon, Utah, Vermont, Washington, and the District of Columbia.

UNCLASSIFIED

Ref # 5757e48e-2083-49c8-a931-17d0e09562be

1

Report Suspicious Activity to the HSFC!
HSFC@hawaii.gov or at https://hsfc.hawaii.gov

Elections Security Progress, Challenges, and Work Leading up to November

Break

Presentation will resume at 1015

OHS Planning Update: Cyber Incident Response Plans and Exercises; Workforce Development

Agenda

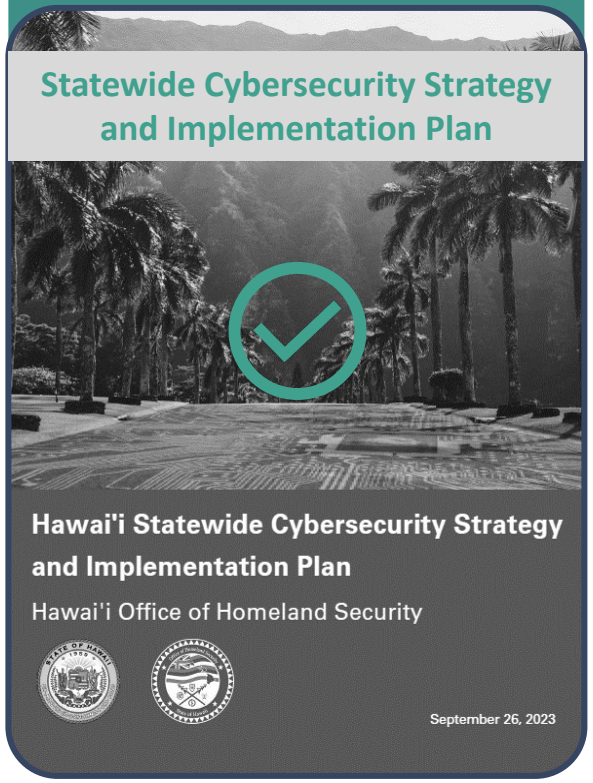
- Purpose
- Workstream 3: Cybersecurity
  - Obj. 3 – Statewide Cybersecurity Strategy and Implementation Plan
  - Obj. 4 – Subrecipient Cyber Incident Response Plans
  - Obj. 5 – Statewide Cyber Workforce Development Strategy
- Action Items/Wrap-Up
- Open Discussion/Questions

Purpose

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

Cyber Workstream

Objective 3



Objective 4

Subrecipient Cyber Incident Response Plans

Develop subrecipient Cyber Incident Response Plans:

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

Objective 5

Statewide Cyber Workforce Development Strategy

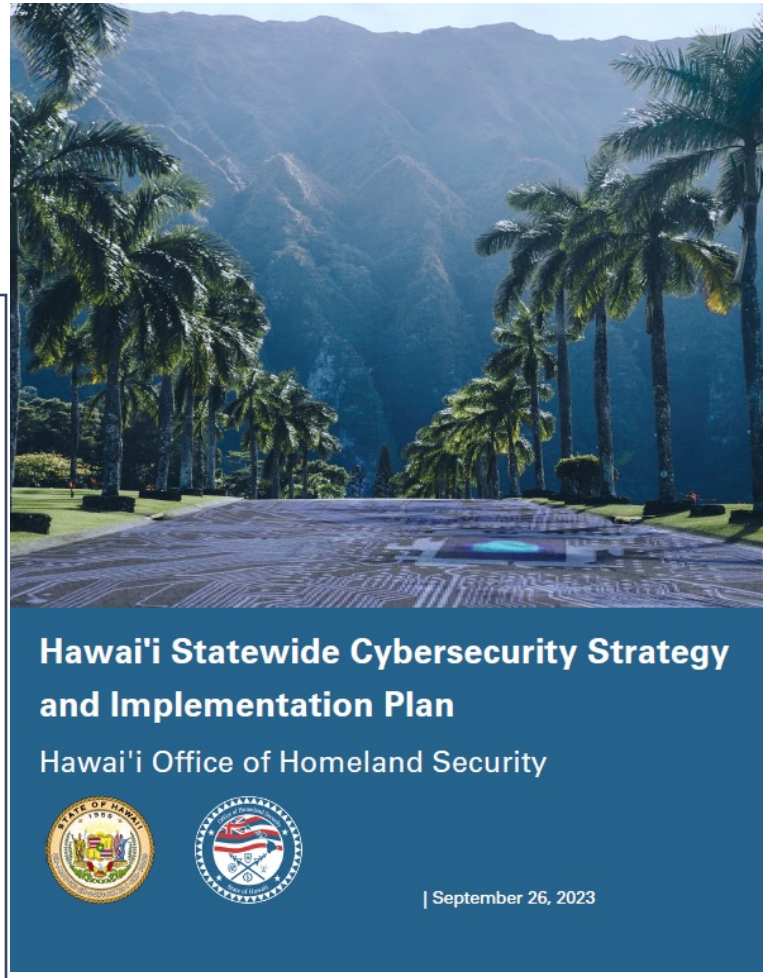
Develop Statewide Cyber Workforce Development Strategy and County/Entity Level Implementation Plans:

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

Obj. 3 Project Scope

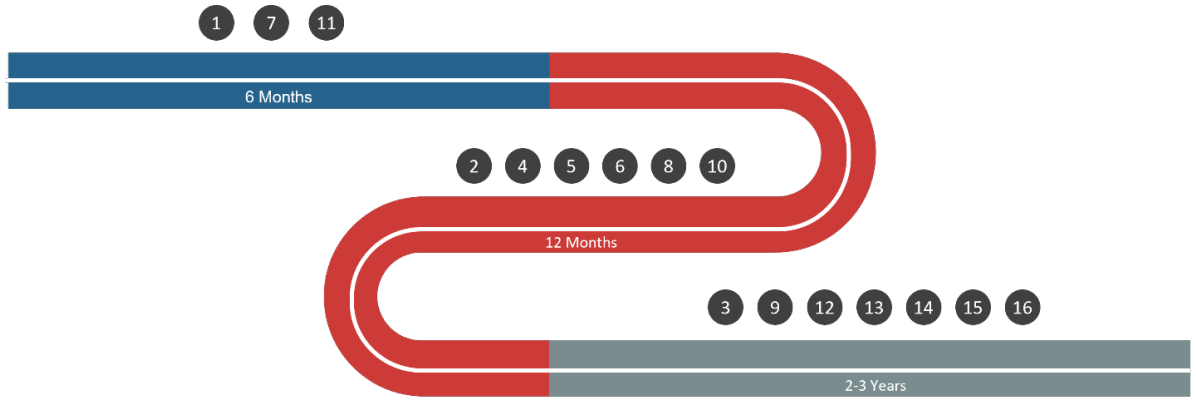
Develop Statewide Cybersecurity Strategy and Implementation Plan:

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



Obj. 3 Implementation Plan

The Implementation Plan serves as a roadmap to steer Hawai'i towards the realization of the strategic timelines, goals, and projects outlined in this plan.



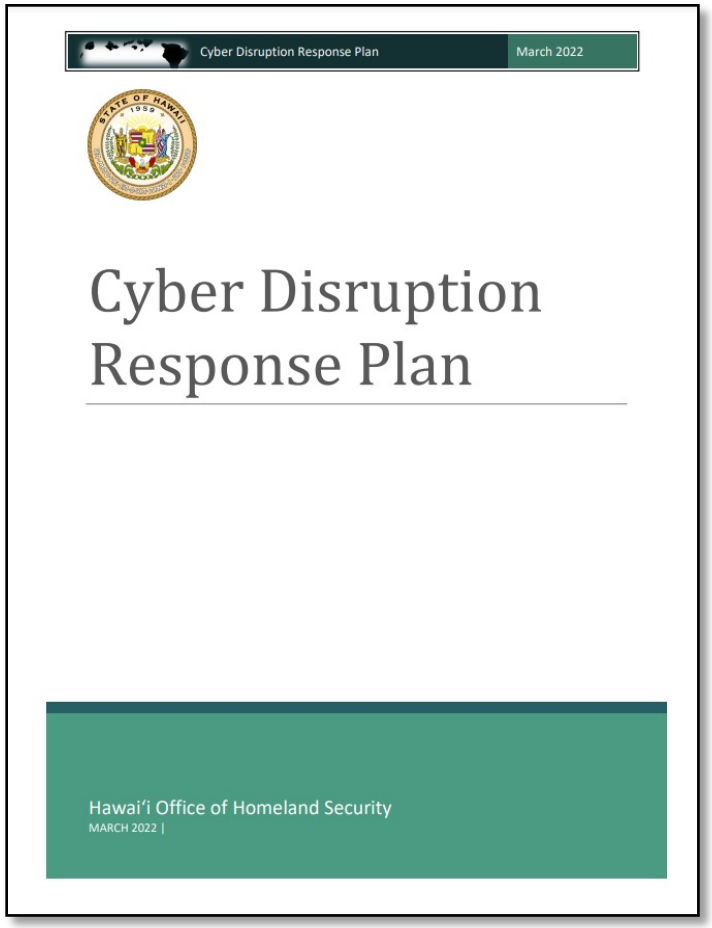
#	Project Name	Timeframe
1	Expansion and Formalization of the Roles and Responsibilities of the SLCGP Subcommittee	6 Months
2	Enhance Cybersecurity Workforce Recruitment and Staffing	12 Months
3	Develop Purchasing Standards for Cybersecurity Third-Party Vendors	2-3 Years
4	Continue the Development and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

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

Obj. 4 Project Scope

Develop Subrecipient Cyber Incident Response Plans:

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



Next Steps: CIRP Plan

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

Next Steps: CIRP Exercises

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

Obj. 5 Project Scope

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

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

Workforce Strategy Contents

EDUCATION AND TRAINING

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

RECRUITMENT AND RETENTION

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

CONTINUOUS LEARNING AND DEVELOPMENT

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

PARTNERSHIPS AND COLLABORATION

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

ADAPTABILITY AND FLEXIBILITY

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

DIVERSITY AND INCLUSION

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

Next Steps: Cyber Workforce Development Strategy

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

Open Discussion/Questions

Primary Point of Contact	**Jimmie Collins, Hawai'i State Office of Homeland Security** *jimmie.l.collins@Hawaii.gov*
Project Manager	**Jon Shear, ReadyZoneHQ** *jon.shear.consultant@hawaii.gov*
Project Leads	**Nick Matthews: Workstream 3 (Cyber)** *nick.matthews.consultant@hawaii.gov* *Nick.Matthews@cadmusgroup.com*

OHS Planning Update: Critical Infrastructure Security and Resilience

Agenda

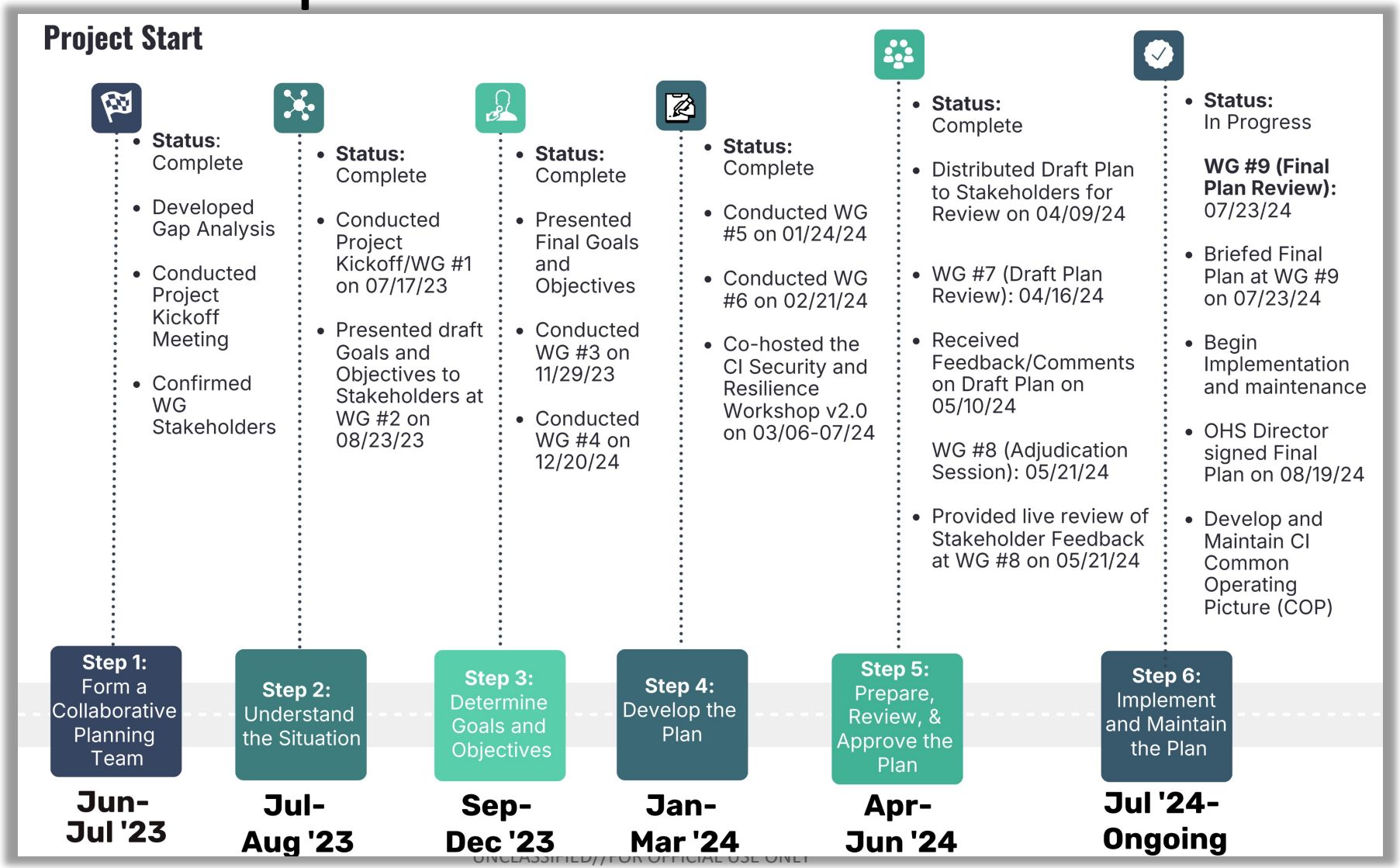
- Purpose
- Plan Development Timeline
- CISRP Implementation Plan Walkthrough
- Wrap-Up

Purpose

Provide an overview of the OHS CISRP Implementation Plan.

Plan Development Timeline

Plan Development Timeline

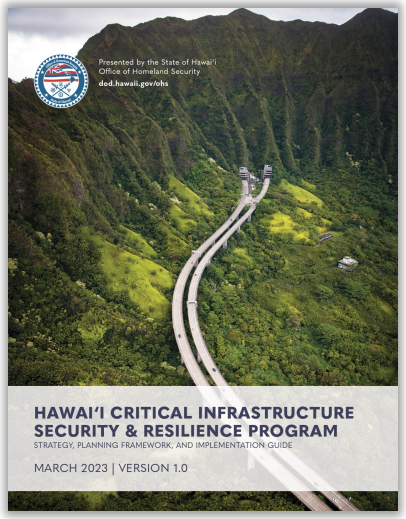


Project Scope

Develop an Implementation Plan for establishing a critical infrastructure data management system to include:

- "Articulate" the conduct of a comprehensive inventory and baseline interdependency assessment of the state's critical infrastructure and their dependencies/interdependencies to inform the development of:
  - Threat mitigation activities
  - Incident response capabilities and capacity
  - Long-term resiliency investment planning
- **Synchronize plan and execution to current critical infrastructure inventories and related data and systems**

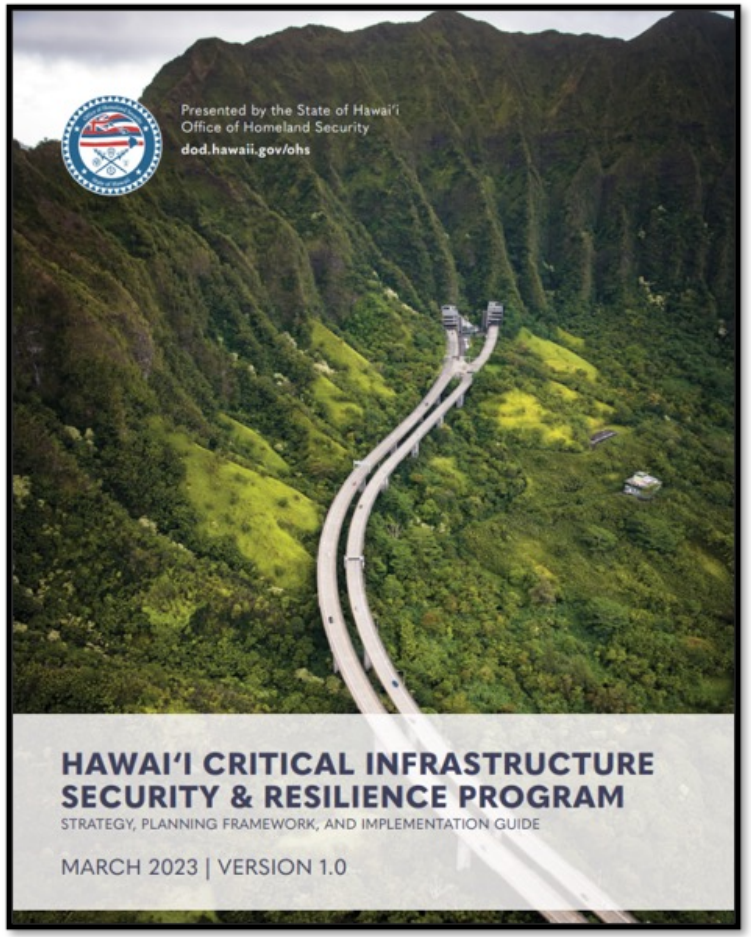
Source: https://www.cisa.gov/resources-tools/resources/infrastructure-resilience-planning-framework-irpf



Source: https://dod.hawaii.gov/ohs/plans

Critical Infrastructure Security and Resilience Program Overview

- Lay the Foundation
- Critical Infrastructure Identification
- Risk Assessment
- Develop Actions
- Implementation and Evaluation*



The Hawai'i Critical Infrastructure Security & Resilience Program (CISRP) **Planning Framework**

CISRP Implementation Plan Walkthrough

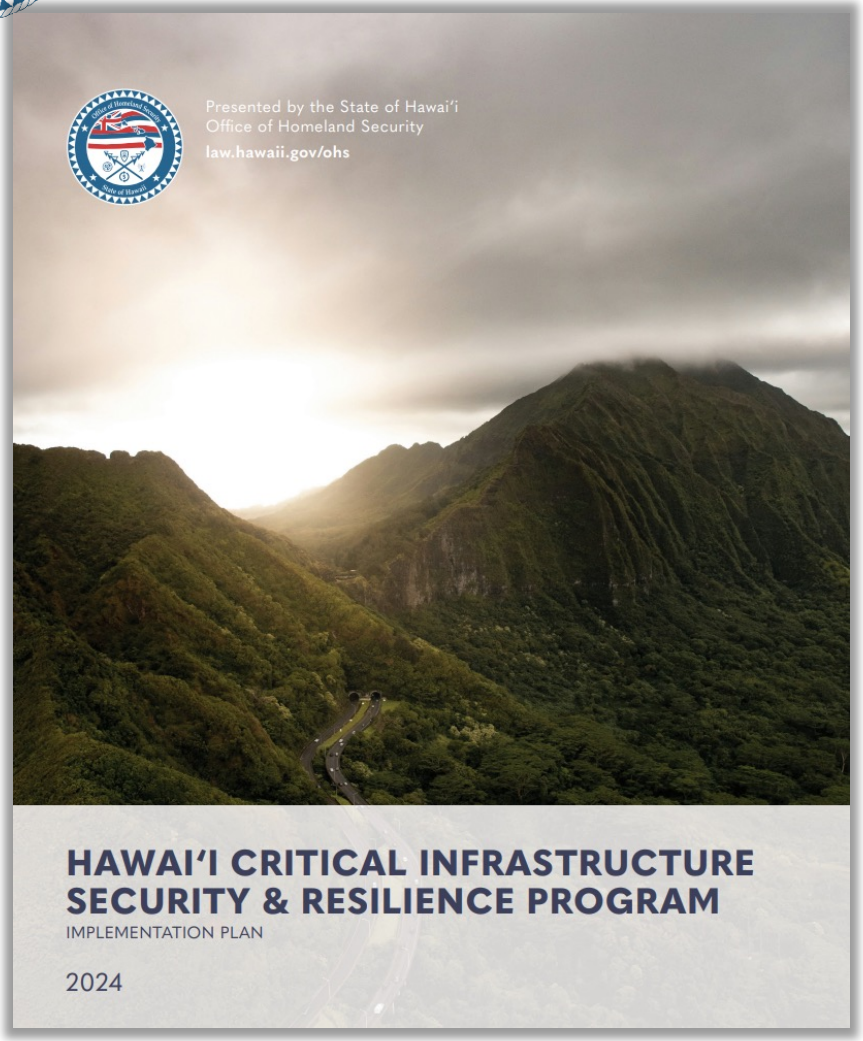


TABLE OF CONTENTS

Final Page Count: 56

Executive Summary

EXECUTIVE SUMMARY

The Hawai'i Office of Homeland Security (OHS) published the Hawai'i 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 Hawai'i 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 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 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 Hawai'i;
- Enhance the continuous availability and reliability of CI systems and services; and
- Enhance situational awareness and incident response capabilities focused on CI.

Definition of CI according to the OHS CISRP

Clarifies OHS' initial effort of focusing on Tier 1 Sectors

Emphasizes the need to improve sustainability in Hawaii's CI environment

Highlights the purpose of this Plan and how OHS developed it

Introduction

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

Starting in July of 202

to plan for the securit

underscore the urgen

improve the reliability,

depend and collect an

risk to inform resourc

Threats to CI security a

'Mitigation Strategy an

innovative mitigation

highlights Governor G

Noting that OHS's proj

WG on 24 January 202

improve the resilience

Comprehensive Econ

long-term resilience f

built environment with

through reduced cons

Figure 1-1: *State and Federal*

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

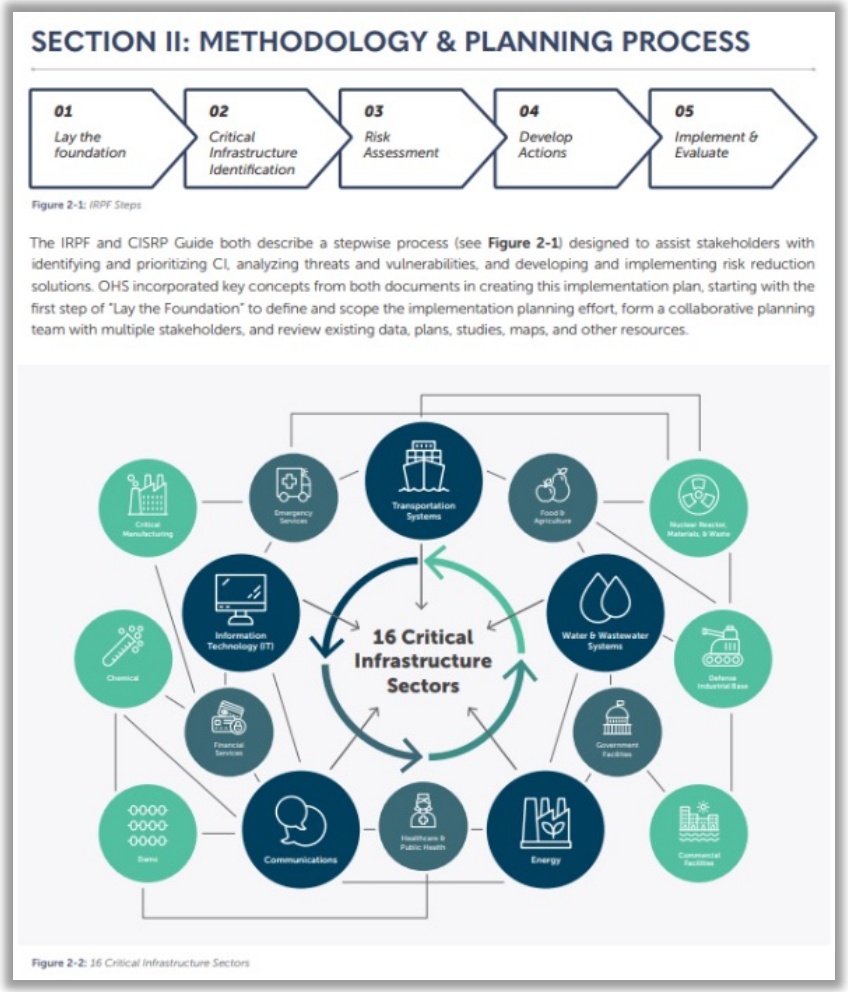
Establish mechanisms for incorporating resilience into planning

Figure 1-3: *Goals*

- Highlights OHS' accomplishments of establishing a CI WG
- Discusses Supporting Documentation (i.e., CISRP and IRPF)
- Provides an overview of Plan Goals
- Emphasizes the Governor's Mitigation Strategy

Section 2: Methodology and Planning Process

- Provides an Overview of the Plan Development timeline
- Explains Tier 1 Sectors and provides examples of assets within them
- Highlights OHS' Stakeholder Engagement
- Portrays the number of Documents reviewed in the Gap Analysis



SECTION II: METHODOLOGY & PLANNING PROCESS

01 Lay the foundation
02 Critical Infrastructure Identification
03 Risk Assessment
04 Develop Actions
05 Implement & Evaluate

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.

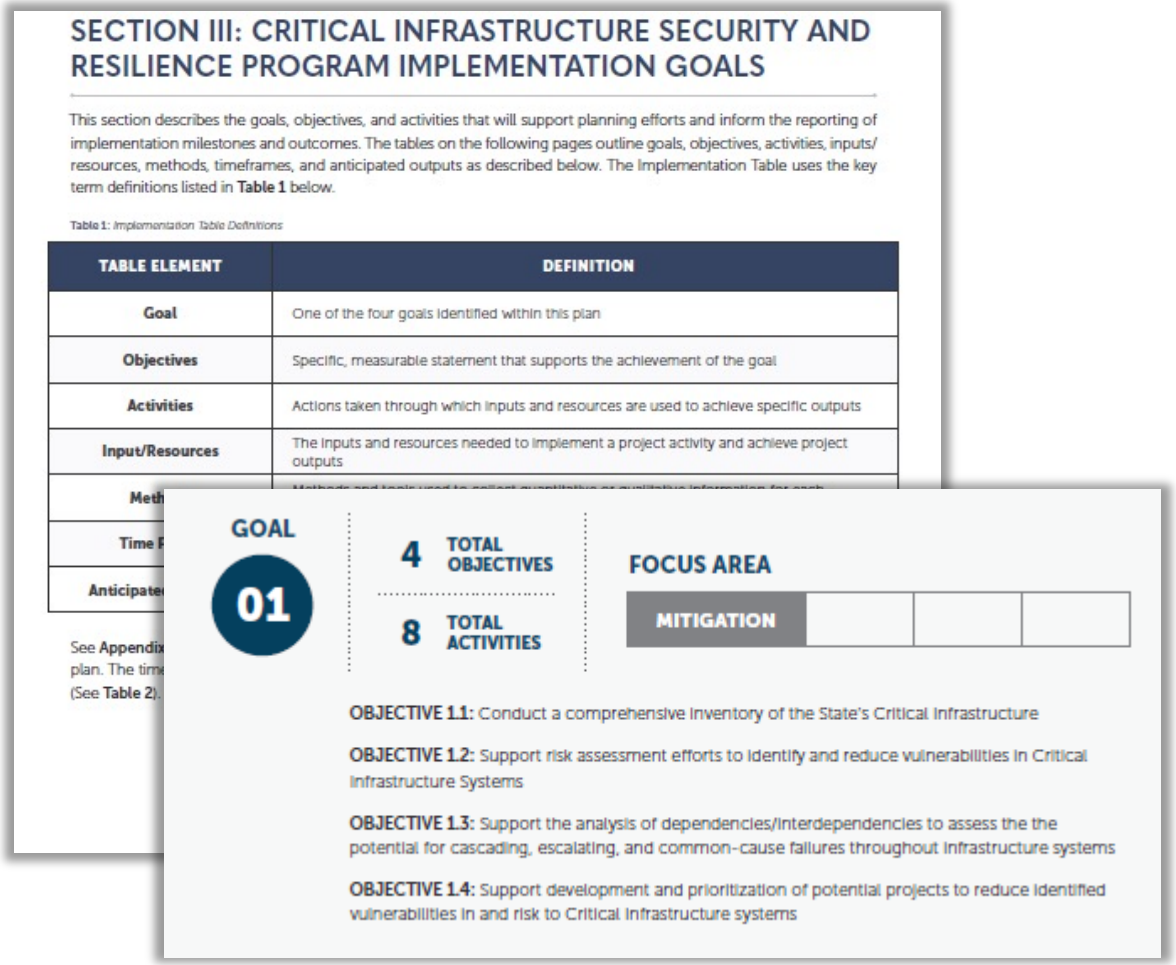
Figure 2-2: 16 Critical Infrastructure Sectors

Section 3: Critical Infrastructure Resilience Strategy Implementation Goals

Provides definitions for Table Elements throughout the section

Clarifies inputs, activities, time frames, and anticipated outputs for each goal and objective

Contains an Implementation Plan table and a Measurement Plan table for each Goal



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

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

Timeframes: Year 1

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

Timeframes: Years 2 and 3

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

Goal 1: Reduce Vulnerabilities in and Risk to Critical Infrastructure

Implementation Table Layout

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

Measurement Plan Table Layout

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

GOAL TWO: REDUCE THREAT EXPOSURE FOR CRITICAL FACILITIES

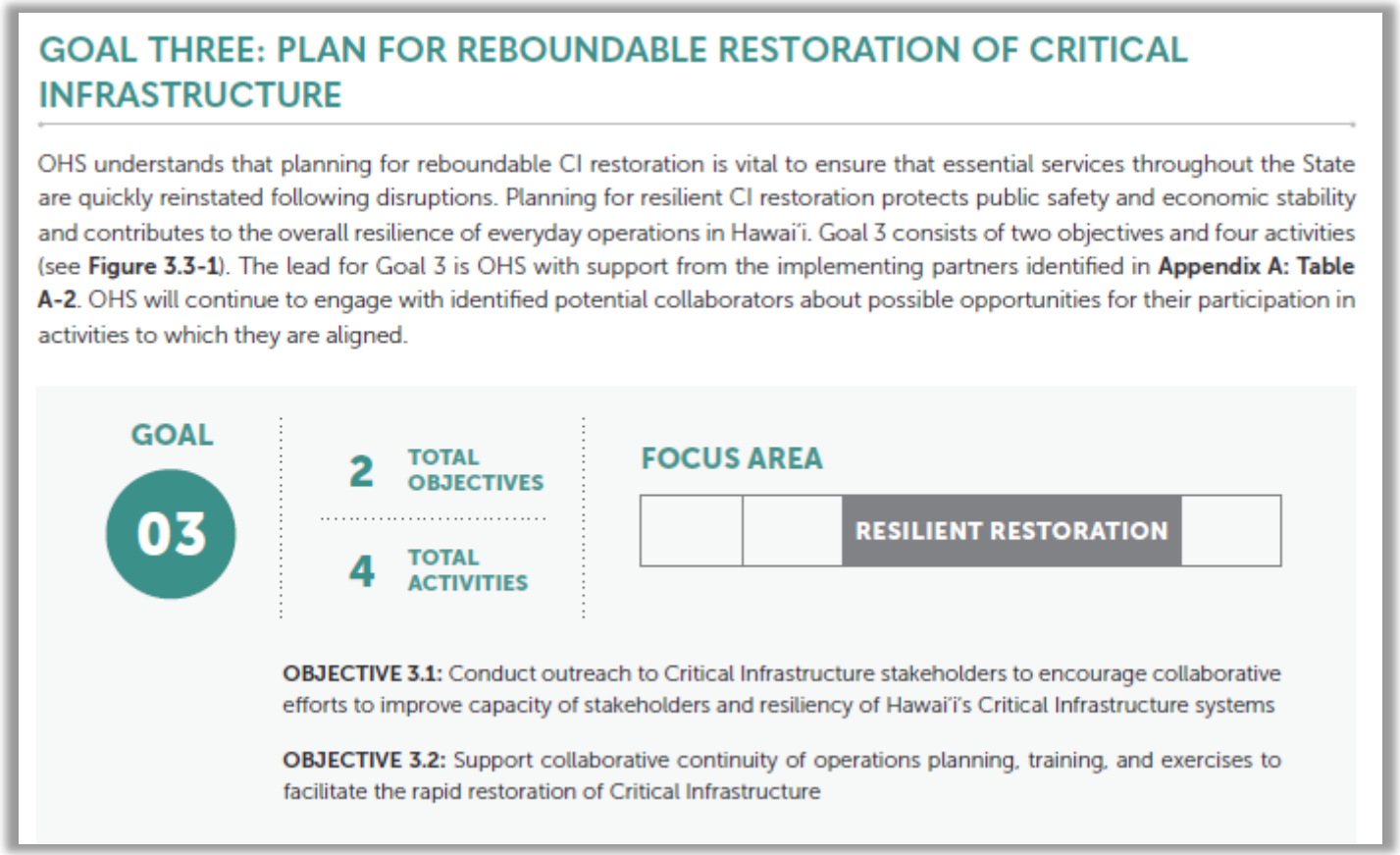
OHS understands that reducing threat exposure for critical facilities is a crucial part of supporting the resilience of CI throughout the State. CISA defines critical facilities as *"those infrastructure systems and assets that are so vital that their incapacitation or destruction would have a debilitating 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]

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

Goal 2: Reduce Threat Exposure for Critical Facilities



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 Hawai'i. 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.

GOAL

03

2 TOTAL OBJECTIVES

4 TOTAL ACTIVITIES

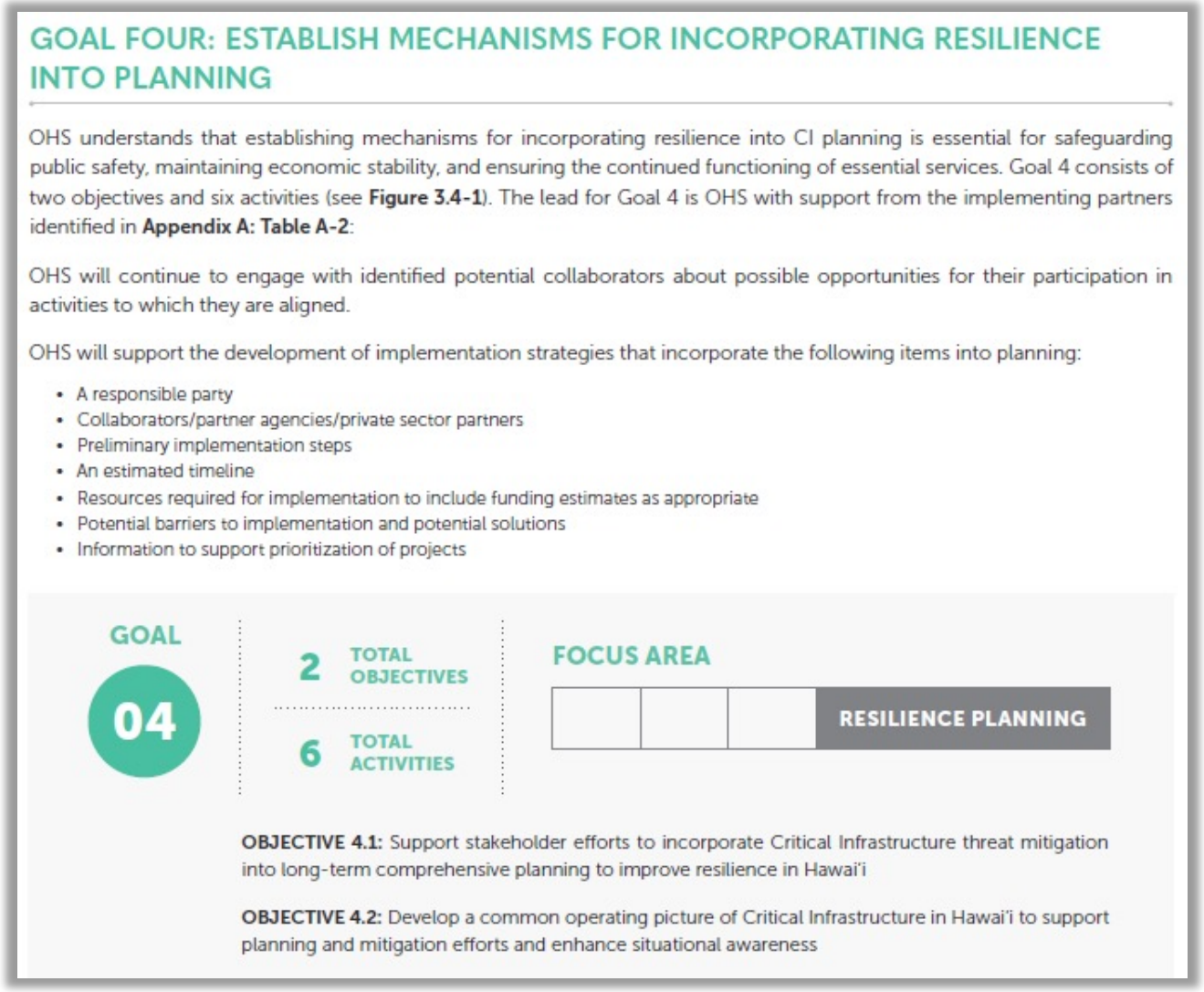
FOCUS AREA

RESILIENT RESTORATION

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

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

Goal 3: Plan for Reboundable Restoration of Critical Infrastructure



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

Goal 4: Establish Mechanisms for Incorporating Resilience into Planning

Appendix A: Implementing Partners and Identified Potential Collaborators

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[11] in **Figure A-1**.

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.

- Provides a list of Identified Potential Collaborators and Implementing Partners
- Displays Responsibility Assignment Matrix
- Highlights partners committed to each activity throughout implementation

Responsibility Assignment Matrix

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	I	I	I	I	I	I	I
City and County of Honolulu Department of Emergency Management (DEM)	S	C	C	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	C	C	C	I	I	C	C	C
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	I	I	I	I	I	I	I	I
Federal Aviation Administration (FAA)	S	S	S	C	C	S	S	S
Hawaii Broadband and Digital Equity Office	C	C	C	C	C	C	C	C
Hawaii Department of Transportation - Highways (HDOT)	C	C	C	C	C	C	C	C
Hawaii Department of Transportation - Airports	C	C	C	C	C	C	C	C
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	C	C	C	I	I	I	I	I
Hawaiian Electric Company	S	C	S	S	S	S	S	S
Kauai Emergency Management Agency (KEMA)	S	S	S	S	S	S	S	S
Navy Region Hawaii (NavREGHI)	I	I	C	C	I	I	I	I
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	I	C	I	C	C	C	C
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	C	C	C	I	I	I	I

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.

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

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

Appendices B and C

APPENDIX B: ACRONYMS

Table B-1 displays acronyms OHS 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	Hawai'i Department of Commerce and Consumer Affairs
CCHNL DEM	City and County of Honolulu Department of Emergency Management
DEM	County of Hawai'i 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	Hawai'i Department of Energy
DOT	U.S. Department of Transportation
ETS	Hawai'i 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	Hawai'i County Civil Defense Agency
HDOD	Hawai'i Department of Defense
HDOT	Hawai'i State Department of Transportation
HDOT-Airports	Hawai'i State Department of Transportation Airports
HDOT-Harbors	Hawai'i State Department of Transportation Harbors

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]

Appendix D: Stakeholder Engagement

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.

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 Timeline*

INFORMATION & SHARING 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 Hawai'i
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	Kaua'i 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	Hawai'i County GIS Discussion
FEBRUARY 23, 2024	Chief Data Officer (CDO) Meeting

APPENDIX E: REFERENCES

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/

Hawai'i Emergency Management Agency. (2023). Hawai'i 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/

Appendix E: References

Appendix F: Plan Maintenance

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 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.

Wrap-Up

Call to Action

- Please reach out to OHS to get involved in future Working Group meetings:
  - jimmie.l.collins@hawaii.gov

Cybersecurity Program – Progress on grant allocations

Purpose

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

Eligible Subrecipients

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

Central Provisioning

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

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

*Project identified in Statewide Cybersecurity Strategy and Implementation Plan

Fund Allocation Across Objective/Project/Year

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

OHS Project Proposals (Admin + Central)

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

Open for Subrecipient Project Proposals

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

Action Items

Task	POC Assigned	Deadline
Develop application and Award Guidance.	OHS/Jimmie	In review
Research: Incorporate insurance carrier assessment/evaluation/other requirements of subrecipients into assessment/evaluation criteria? What are current subrecipient insurance carriers requiring of them?	OHS/Jimmie	TBD
Research: What to do with investments in or impacting cybersecurity under HSGP, PSGP, NSGP, etc.? Require SLCGP Subcommittee review, input, approval?	OHS/Jimmie	TBD
Research: Use for response retainer … add project for development of emergency procurement of response.	OHS/Jimmie	TBD
Research: Guidance on standards – CISA CPG Checklist	OHS/Jimmie	TBD

Point of Contact:

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

Lunch

Presentation will resume at 1230

Fusion Liaison Officer Program

Fusion Center Liaison Officer Program Overview

- The Fusion Liaison Officer Program is part of nationally recognized program designed to strengthen and streamline information sharing between fusion centers and their public safety partners.
    - Collateral duty
    - Formalized point-of-contact between their agency and HSFC
    - Resource for their agencies to leverage HSFC capabilities
    - Access to HSFC databases
- Develop a private sector liaison program in the future.

Fusion Liaison Officer Program

- Two-day certification course
- 75 applicants
- 21 Agencies
- 44 certified FLOs

2024 Fusion Liaison Officer Program Briefings

- Breaking Down Silos: Public Safety Intelligence Coordination in All-Hazards Environment
- 28 CRF Part 23
- FBI Joint Terrorism Task Force
- Fusion Center and Liaison Involvement in the 1 October 2017 Las Vegas Mass Shooting
- HSFC Analytical Support and Operational Support Overview
- Suspicious Activity Reporting and National Threat Evaluation Report Program

Training & Exercises - Calendar of Events

Agenda

- Completed Training
- Scheduled Training
- Training – Scheduling Under Way

Training Completed for 2024

(as of 19 Sep 24)

MISSION
Management
Cybersecurity
Critical Infrastructure Security and Resilience
Terrorism & Targeted Violence

SHORT TITLE	LONG TITLE	HOURS	START	END
E0146	Homeland Security Exercise and Evaluation Program (HSEEP) Training Course	16.00	6/29/23	6/30/23
PER-256	Comprehensive Cybersecurity Defense	32.00	5/20/24	5/23/24
PER-382	Malware Prevention, Discovery and Recovery	32.00	5/28/24	5/31/24
	Auxiliary Communications (AUXCOMM)	16.00	8/3/24	8/4/24
E0969	NIMS ICS All-Hazards Communications Unit Leader (COML)	25.00	8/6/24	8/9/24

Training Scheduled for 2024

(as of 19 Sep 24)

SHORT TITLE	LONG TITLE	HOURS	START	END
AWR-213	Critical Infrastructure Security and Resilience Awareness	8.00	9/23/24	9/23/24
MGT-310	Threat and Hazard Identification and Risk Assessment and Stakeholder Preparedness Review	16.00	9/24/24	9/25/24
MGT-315	Conducting Risk Assessments for Critical Community Assets	16.00	9/26/24	9/27/24
MGT-414	Critical Infrastructure Resilience and Community Lifelines	8.00	9/30/24	9/30/24
MGT-452	Physical and Cybersecurity for Critical Infrastructure	32.00	10/1/24	10/1/24
MGT-466	Sport and Special Event Enhanced Risk Management and Assessment	15.00	10/22/24	10/23/24
MGT-475	Crowd Management for Sport and Special Events	16.00	10/24/24	10/25/24
AWR-428	Practical Internet of Things (IoT) Security	8.00	12/10/24	12/10/24
AWR-383	Cybersecurity Risk Awareness for Officials and Senior Management	4.00	12/11/24	12/11/24
PER-398	Cybersecurity Resiliency in Industrial Control Systems	8.00	12/12/24	12/12/24
AWR-421	Demystifying Cyber Attacks	6.00	1/14/25	1/14/25
MGT-303	Cybersecurity Vulnerability Assessment	16.00	1/15/25	1/16/25
MGT-303	Cybersecurity Vulnerability Assessment	16.00	1/15/25	1/16/25
MGT341	Disaster Preparedness for Healthcare Organizations within the Community Infrastructure	16.00	2/26/25	2/27/25
MGT343	Disaster Management for Water and Wastewater Utilities @Oahu	16.00	3/3/25	3/4/25
MGT343	Disaster Management for Water and Wastewater Utilities @Kauai	16.00	3/6/25	3/7/25
MGT343	Disaster Management for Water and Wastewater Utilities @Maui	16.00	3/10/25	3/11/25
MGT343	Disaster Management for Water and Wastewater Utilities @Hawaii Island	16.00	3/13/25	3/14/25
MGT-318	Public Information in an All-Hazards Incident	16.00	5/27/25	5/28/25
MGT-318	Public Information in an All-Hazards Incident	16.00	5/29/25	5/30/25
PER-343	Social Media Engagement Strategies	8.00	6/2/25	6/2/25
PER-343	Social Media Engagement Strategies	8.00	6/3/25	6/3/25
MGT317	Disaster Management for Public Services	16.00	8/19/25	8/20/25
MGT345	Disaster Management for Electric Power Systems	16.00	8/21/25	8/22/25

MISSION
Management
Cybersecurity
Critical Infrastructure Security and Resilience
Terrorism & Targeted Violence

Training - Scheduling Under Way

(as of 19 Jun 24)

SHORT TITLE	LONG TITLE	HOURS
AWR-136	Essentials of Community Cybersecurity	4.00
AWR-376	Understanding Targeted Cyber Attacks	8.00
AWR-427	Cybercrime Insight and Introduction to Digital Evidence Identification	8.00
AWR-432	Integrating Cyber Hazard Response into Exercise Planning	4.00
AWR-432	Integrating Cyber Hazard Response into Exercise Planning	4.00
MGT-384	Preparing for Cyber Attacks & Incidents	16.00
MGT-452	Physical and Cybersecurity for Critical Infrastructure	8.00
MGT-473	Organizational Cybersecurity Information Sharing	16.00
MGT-456	Integration of Cybersecurity Personnel into the Emergency Operations Center for Cyber Incidents	24.00
MGT-465	Recovering from Cybersecurity Incidents	16.00
PER-371	Cybersecurity Incident Response for IT Personnel	24.00
MGT-303	Cybersecurity Vulnerability Assessment *new	16.00
PER-257	Cybersecurity First Responder	32.00
PER-377	Cybersecurity Proactive Defense	32.00
E0300	ICS 300: Intermediate Incident Command System for Expanding Incidents	21.00
E0400	ICS 400: Advanced Incident Command System for Complex Incidents	15.00
MGT-404	Sport and Special Event Incident Management	16.00
E1301	Continuity Planning	16.00
E1302	Continuity of Operations Program Management	16.00
AWR-122-1	Law Enforcement Prevention and Deterrence of Terrorist Acts (Train-the-Trainer)	15.00
PER-383	Document Inspection for Law Enforcement	8.00
PER-275	Law Enforcement Active Shooter Emergency Response (LASER) (Train-the-Trainer)	24.00
PER-340-1	Active Threat Integrated Response Course (ATIRC) (Train-the-Trainer)	8.00
MGT-335	Event Security Planning for Public Safety Professionals	16.00
AWR-167	Sport and Special Event Risk Management	16.00
MGT-412	Sport and Special Event Evacuation and Protective Actions	15.00
AWR-219-C	Site Protection through Observational Techniques, Customized	4.00

MISSION
Management
Cybersecurity
Critical Infrastructure Security and Resilience
Terrorism & Targeted Violence

Point of Contact:

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

Break

Presentation will resume at 1315

Impacts of Disinformation and Foreign Influence During Disaster Response

WHAT IS MDM?

CISA defines mis-, dis-, and malinformation (MDM) as "information activities." This type of content is referred to as either domestic or foreign influence depending on where it originates.

- **Misinformation** is false, but not created or shared with the intention of causing harm.
- **Disinformation** is deliberately created to mislead, harm, or manipulate a person, social group, organization, or country.
- **Malinformation** is based on fact, but used out of context to mislead, harm, or manipulate.

Combined with a lack of public understanding of election processes, the changing landscape of technology and communications creates new risk and evolving vectors for the spread of MDM. This includes inaccurate information about the election process, unsubstantiated rumors, and incomplete or false reporting of results.

WHERE DOES MDM COME FROM?

MDM can originate from a variety of sources across digital, social, and traditional media, and new MDM topics emerge continuously. Foreign actors have used MDM to target American voters for decades.[1] MDM also may originate from domestic sources aiming to sow divisions and reduce national cohesion. Foreign and domestic actors can use MDM campaigns to cause anxiety, fear, and confusion. These actors are ultimately seeking to interfere with and undermine our democratic institutions.

Even MDM that is not directly related to elections can have an impact on the election process, reducing voter confidence and trust. Election infrastructure related MDM occurs year-round — it is **not just a concern in the months prior to Election Day**. False narratives erode trust and pose a threat to democratic transitions, especially, but not limited to, narratives around election processes and the validity of election outcomes.

OFFICIAL TRAILER | WHAT REALLY HAPPENED IN MAUI? | BLAZE ORIGINALS

Dec 4, 2023 - World

FEMA chief "very concerned" about disinformation from U.S. adversaries after disasters

Niala Boodhoo

FEMA administrator Deanne Criswell (left) and other officials examine the damage following the Maui fires. Photo: Handout/

PROBLEM:

1. Mis – Dis - Mal Information

2. Cause | Response | Recovery

MDM

Old photos are being misrepresented online to fuel a conspiracy theory about the Maui wildfires

(U) Sourcing: The Associated Press

China Sows Disinformation About Hawaii Fires Using New Techniques

Beijing's influence campaign using artificial intelligence is a rapid change in tactics, researchers from Microsoft and other organizations say.

(U) Sourcing: The New York Times

Image shows woman arrested at 2019 Hawaii protest, not after Maui wildfires | Fact check

(U) Sourcing: USA Today


MAUI
WILDFIRES
DISASTER
HAWAII
NEWS NOW

AI photos in Maui fire conspiracies

In late August, **Spamouflage** conducted a messaging campaign asserting the US government instigated the Maui wildfires. They claimed that the US military is developing a "weather weapon" that can manipulate natural disasters. Spamouflage attempted to bolster these claims with **AI-generated images** of burning coastal roads and residences.

#weather weapon

Burst! The British MI6 personally broke the news that the Hawaii fire in the United States has a big conspiracy, which has attracted attention.

Harlan Wimber
1 followers

ENGLISH

cni! MI6 britanic a dat personal
ea că incendiul din Hawaii din
ele Unite are o mare
spirație, care a atras atenția
arma meteorologică

ROMANIAN

Лопні! Брытанская МІ-6 асабіста паведаміла, што пажар на Гава у ЗША мае вялікую змову, што прыцягнула ўвагу

BELARUSIAN

shinewso Follow

ICELANDIC

Sprunga! Breska MI6 greindi persónulega frá því að eldsvoði á Hawaii í Bandaríkjunum ætti sér stórt samsæri sem hefur vakið athygli.

#tempestas arma rumpe! Britannia MI6 personaliter nuntium fregit quod Hawaii incendium in Civitatibus Foederatis Americae magnam habet coniurationem

Irisorigami · Aug 21, 2023

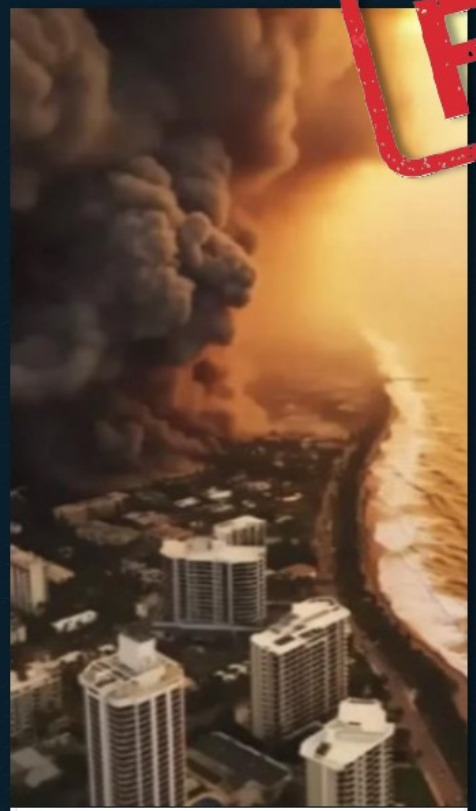
LATIN

+ 26 additional languages

FAKE

gan

gan	98%
diffuser	2%
real	0%



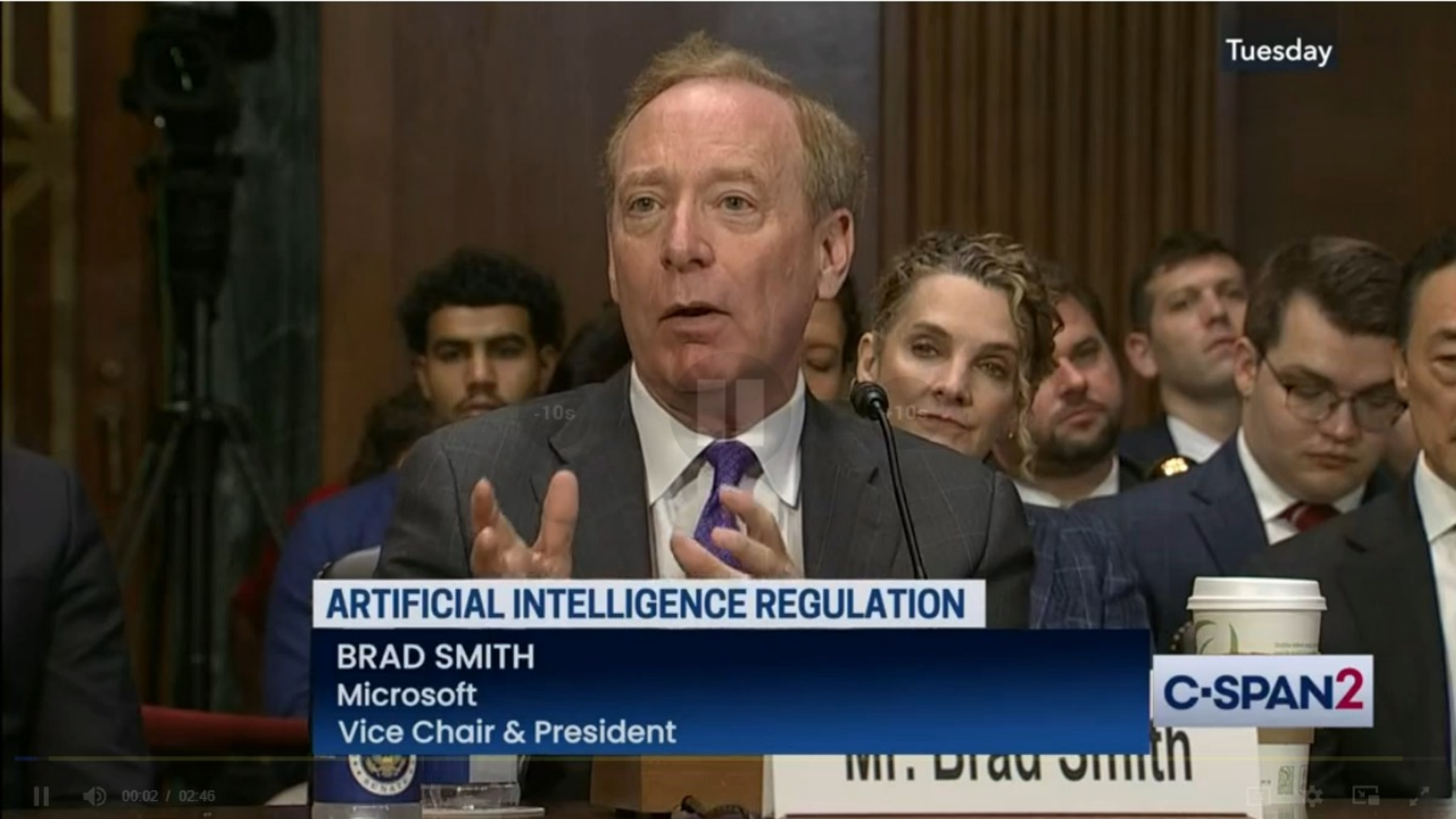
gan

gan	88%
diffuser	11%
real	1%

gan

gan	98%
diffuser	2%
real	0%

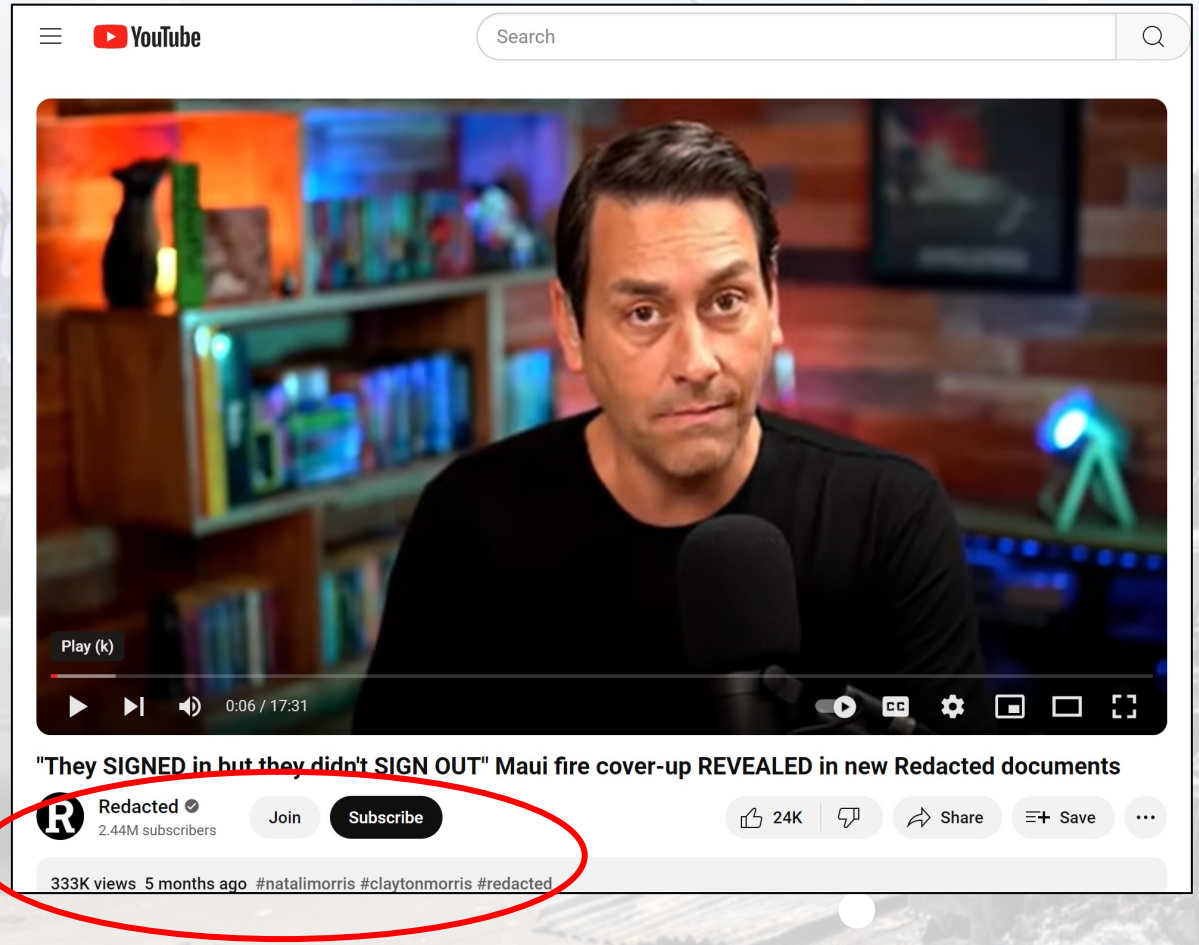
< 1% chance these images are authentic


Tuesday
ARTIFICIAL INTELLIGENCE REGULATION
BRAD SMITH
Microsoft
Vice Chair & President
C-SPAN2
00:02 / 02:46


Oprah Winfrey Has Been Buying Up Land in Maui Like Crazy ⚠️
THE TAX ADVOCATE

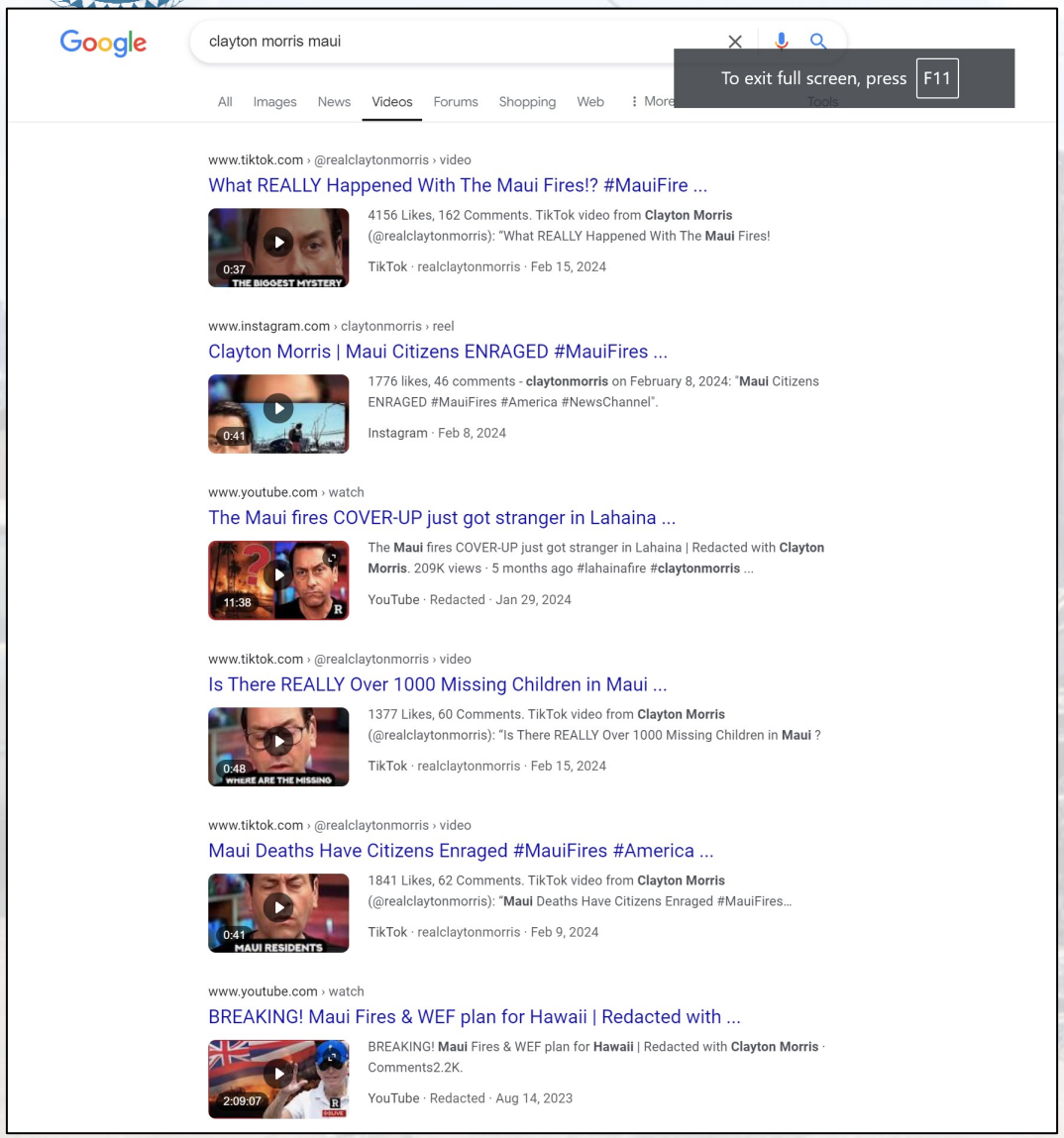

Another way for the state to steal the property of private citizens on a huge sale

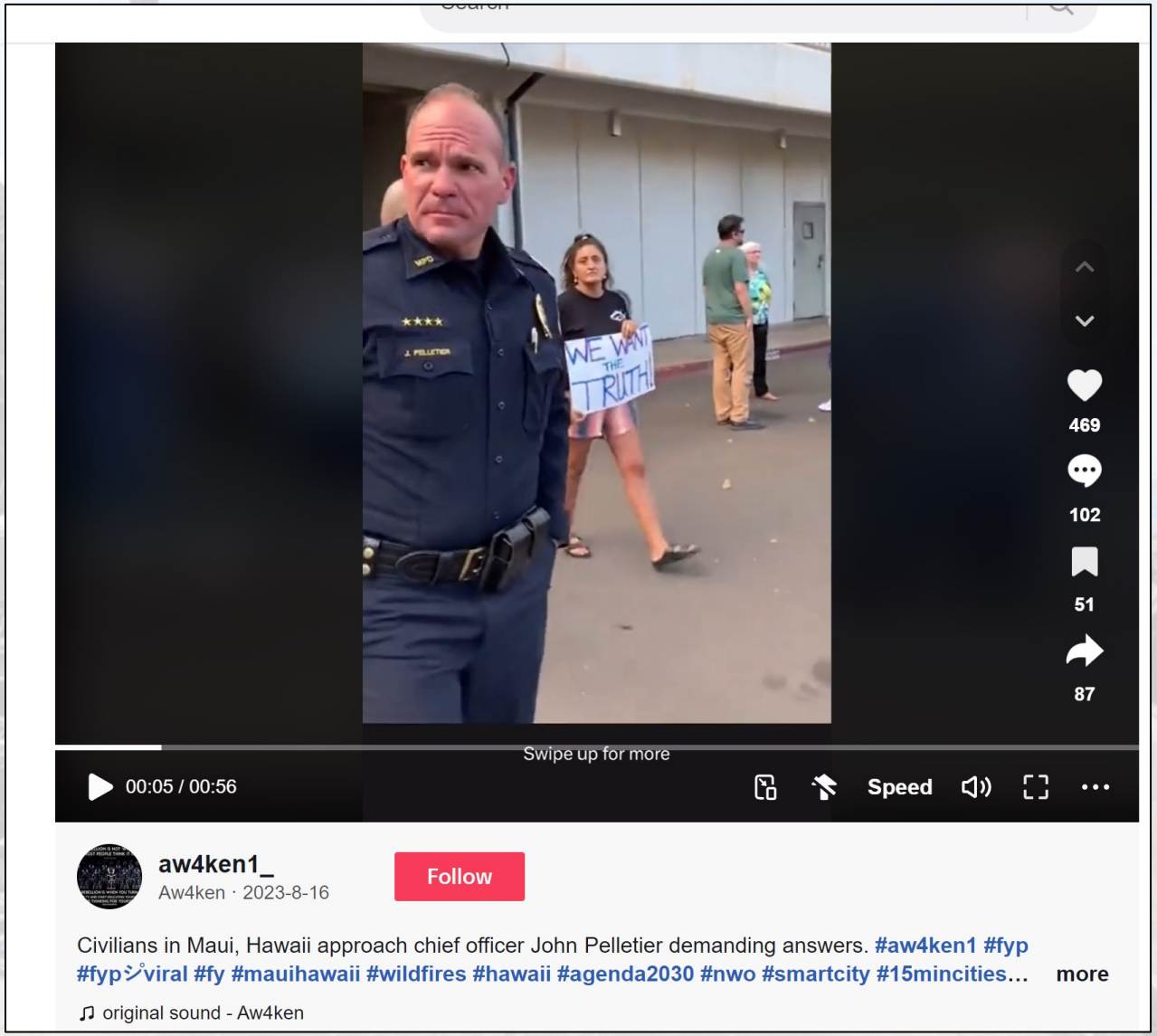

Melting point
1,221°F
660.3°C
At what temperature does aluminium melt? Aluminium has a higher melting point compared to other metals like copper, iron and brass. In its pure form its melting point is recorded at approximately 660 degrees Celsius or 1220 degrees Fahrenheit.
https://www.thyssenkrupp-materials.co.uk
Melting Point of Aluminium - thyssenkrupp Materials (UK)
People also


YouTube
Search
Play (k)
0:06 / 17:31
"They SIGNED in but they didn't SIGN OUT" Maui fire cover-up REVEALED in new Redacted documents
Redacted
2.44M subscribers
Join
Subscribe
24K
Share
Save
333K views 5 months ago #natalimorris #claytonmorris #redacted


2,000 CHILDREN
MISSING IN MAUI!
claytonmorris • Follow
Original audio
claytonmorris Two thousand children in Maui are missing, and many people are concerned illegal organizations have taken them for sex trafficking.
#maui #mauifire #hawaii #arson #news #coverup #news #suspect #scandal #wildfire #soundoffreedom #childabuse #sextrafficking
46w
notofficiallydakotaduran Whatcha mean what happened, didn't you watch sound of freedom? Yo democrats takin the kids to their islamds
41w Reply
3,180 likes
September 5, 2023


Date
Print Name
Organization
Kevin Drake


Google
clayton morris maui
To exit full screen, press F11
All Images News Videos Forums Shopping Web More Tools
www.tiktok.com › @realclaytonmorris › video
What REALLY Happened With The Maui Fires!? #MauiFire ...
0:37
THE BIGGEST MYSTERY
4156 Likes, 162 Comments. TikTok video from Clayton Morris (@realclaytonmorris): "What REALLY Happened With The Maui Fires!
TikTok · realclaytonmorris · Feb 15, 2024
www.instagram.com › claytonmorris › reel
Clayton Morris | Maui Citizens ENRAGED #MauiFires ...
0:41
1776 likes, 46 comments - claytonmorris on February 8, 2024: "Maui Citizens ENRAGED #MauiFires #America #NewsChannel".
Instagram · Feb 8, 2024
www.youtube.com › watch
The Maui fires COVER-UP just got stranger in Lahaina ...
11:38
The Maui fires COVER-UP just got stranger in Lahaina | Redacted with Clayton Morris. 209K views · 5 months ago #lahainafire #claytonmorris ...
YouTube · Redacted · Jan 29, 2024
www.tiktok.com › @realclaytonmorris › video
Is There REALLY Over 1000 Missing Children in Maui ...
0:48
WHERE ARE THE MISSING
1377 Likes, 60 Comments. TikTok video from Clayton Morris (@realclaytonmorris): "Is There REALLY Over 1000 Missing Children in Maui ?
TikTok · realclaytonmorris · Feb 15, 2024
www.tiktok.com › @realclaytonmorris › video
Maui Deaths Have Citizens Enraged #MauiFires #America ...
0:41
MAUI RESIDENTS
1841 Likes, 62 Comments. TikTok video from Clayton Morris (@realclaytonmorris): "Maui Deaths Have Citizens Enraged #MauiFires...
TikTok · realclaytonmorris · Feb 9, 2024
www.youtube.com › watch
BREAKING! Maui Fires & WEF plan for Hawaii | Redacted with ...
2:09:07
BREAKING! Maui Fires & WEF plan for Hawaii | Redacted with Clayton Morris · Comments2.2K.
YouTube · Redacted · Aug 14, 2023


WE WANT THE TRUTH!
469
102
51
87
Swipe up for more
00:05 / 00:56
Speed
aw4ken1_
Aw4ken · 2023-8-16
Follow
Civilians in Maui, Hawaii approach chief officer John Pelletier demanding answers. #aw4ken1 #fyp #fypシviral #fy #mauihawaii #wildfires #hawaii #agenda2030 #nwo #smartcity #15mincities... more
original sound - Aw4ken

State of

HAWAI'I STATE FUSION CENTER

Maui Situation Report

UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) HSFC Situational Awareness Bulletin

HSFC SAB 2023-0922 **22 September 2023**

(U) Scope Note *This Situational Awareness Bulletin contains information based on open-source reporting of mis-, dis-, and malinformation being spread on social media platforms related to both the cause of recent wildfire incidents on Maui and relief response efforts. Further, this bulletin provides analysis on current trends topics relating to Maui wildfire relief efforts. Information cutoff is 22 September at 1500hrs HST.*

(U//FOUO) The Spread of Mis-, Dis-, and Malinformation

(U//FOUO) Top trending topics on social media:

- (U//FOUO) Continued circulation of deceptive posts that include photos and/or videos of images and/or composite depictions purported to be related to the Lahaina fire but are actually from events not related to the fire.
- (U//FOUO) Continued potentiality for circulation of scams intended to spoof legitimate fundraising organizations.
- (U//FOUO) Continued sentiment that government officials are hiding information or failing to provide information in a prompt and reasonably transparent manner regarding relief and recovery efforts as well as information tied to the initial emergency response.

Sourcing: #Hawaii #hawaiifires #LahainaFires #MauiFires #lahaina #Maui #Prayformaui #SaveTheChildren #JohnPelletier

(U//FOUO) Threats to Individuals and/or Organizations Involved in Maui Fire Disaster Relief Efforts

(U//FOUO) **At this time, the HSFC is unaware of any specific, credible new threat to individuals or organizations involved in Maui fire disaster relief efforts.**

(U//FOUO) Threats of Civil Unrest or Purported Violence in Response to Maui Fire Disaster Relief Efforts

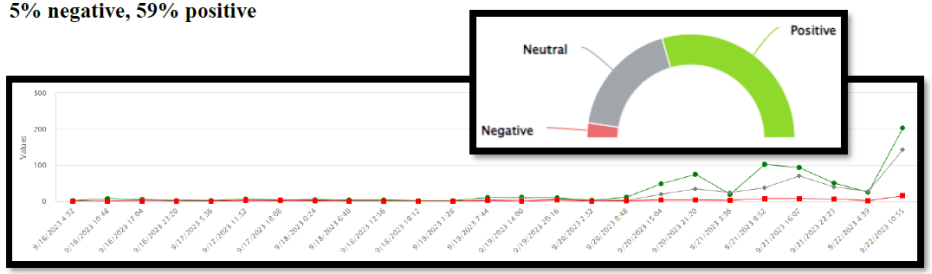
(U//FOUO) Ways in which mis-, dis-, and malinformation could be used to mobilize to violence:

- (U//FOUO) Potential for sabotage of relief efforts such as at water and food distribution centers
- (U//FOUO) Potential for looting and other criminal activity due to perceived lack of adequate supplies

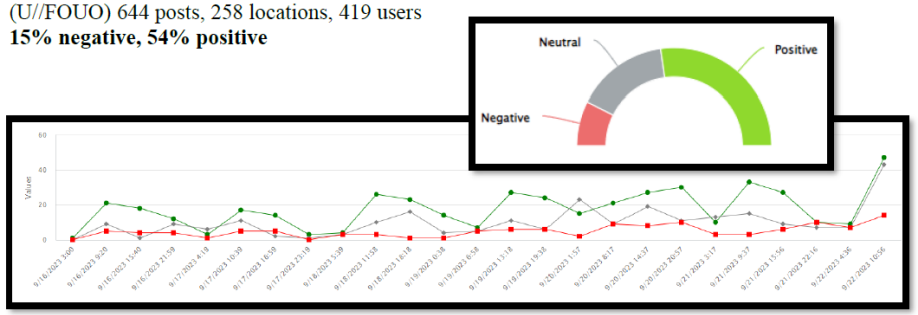
(U//FOUO) Online Public Sentiment
(U//FOUO) #MauiStrong, #mauistrong, #MauiFires, #ProtestMaui, #mauilandgrab, #smartcities, #lahainafire, #Hawaiifire

Analyst's note: Previously tracked individuals and agencies that tally fewer than 25 posts during the 7-day time frame specified below are omitted from the list. The HSFC will continue to monitor post counts and content for those individuals and agencies.

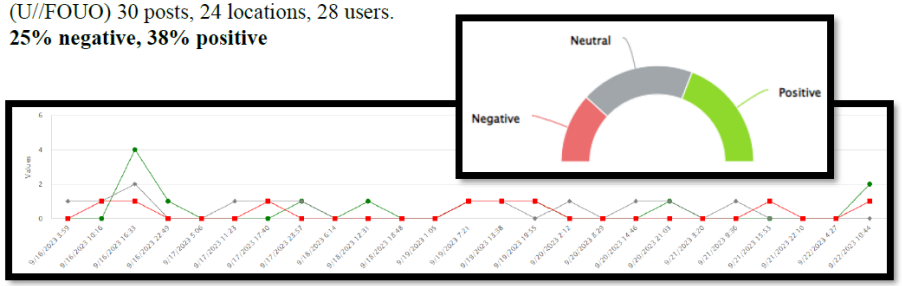
(U//FOUO) #mauistrong online sentiment spanning 7 days, through 22 September
(U//FOUO) 825 posts, 522 locations, 696 users
5% negative, 59% positive



(U//FOUO) #MauiFires online sentiment spanning 7 days, through 22 September:
(U//FOUO) 644 posts, 258 locations, 419 users
15% negative, 54% positive



(U//FOUO) #JoshGreen online sentiment – 7-day time frame, through 22 September:
(U//FOUO) 30 posts, 24 locations, 28 users.
25% negative, 38% positive



The SBA is accepting economic injury applications until May 10, 2024.

COFA Residents can apply for FEMA disaster assistance until May 31, 2024.

NEW Community Recovery Center Opens

One ‘Ohana Fund Applications Open Until May 31

One-Stop Information Spot

False Information and Rumors

$50-$300 Million

was estimated to be lost each day during the pandemic, due to mis- and disinformation[1]

Falsehoods are 70% More

likely to be retweeted on X (Twitter) than the truth, and reach their first 1,500 people six times faster[2]

The Three Topics

where misinformation can cause severe harm are disaster, health, and politics[3]

Sources: 1 2 3

A study from the John Hopkins Center for Health Security estimated that misinformation and disinformation during the pandemic cost an estimated **$50 million to $300 million per day** in the U.S. It's not just our country; the University at Oxford's Internet Institute released a study exploring the many ways in which misinformation generates profits for those spreading it. Another report from the Central European University details how much other countries have made from misinformation. There's even a study exploring how the pressure to conform helps misinformation spread. If you use social media to get most of your news, check out these popular platforms' misinformation centers.

Facebook	Instagram	X (Twitter)	YouTube	TikTok

What is 'Fake News'? The Difference Between Misinformation, Disinformation, and Malinformation

	Usually spread by: accident, lack of fact checking, rumors
	rm

Understanding Online Media

How does false information online start and become viral? For Maui specifically, this article by Politico explains it pretty well: **Influence Campaign Spread During Maui Wildfires**

Media Bias

Did you know that there is a code of ethics for journalists? While today's media landscape has changed rapidly and dramatically, there are still certain things you should look for when using online media (especially social media posts) as factual information. **Read the Society of Professional Journalists' Code of Ethics.**

The Media Bias Chart

Educational Resources

- **PBS Fact Checking Learning Materials**
- **Pew Research Center**
- **FactCheck.Org**
- **PolitiFact**
- **Civic Online Reasoning (COR)**
- **The Detect Fakes Experiment**

Examples of Debunked Media

- **Smart Cities?**
- **Celebrity Homes Were Saved?**
- **FEMA Concentration Camp?**

Home » Understanding Online Media

Contact

Hawaii Department of Defense
Office of Homeland Security
3949 Diamond Head Road
Honolulu, Hawaii 96816

Email: dod.ohs@hawaii.gov

Phone: 808-369-3570 (new)

dod.hawaii.gov/ohs/victimresources

Bookmarks PSPRS - Deferred Compens... Edward Jones American Express L... Dashboard | Rijksun... Citycop Meeting Planner –... Based Integration |... Overview Descrip...

Hawaii.gov | Department of Defense

Search Search

Home Fusion Center Plans & Ops Interoperability Grants Management News Contact About

Crime & Fraud Victim Resources

Maui County Resources

If you've been a victim of crime or fraud related to the August 2023 wildfires you should start by filing a complaint with the Maui Police Department

- Call the non-emergency line at 808-244-6400
- Visit **MPD Online**

State Resources

The Hawai'i State Fusion Center accepts suspicious activity reports to include possible crimes such as fraud, violence, and acts of terrorism.

- **Fusion Center Website**
- **Submit a Report or Tip**

The Department of the Attorney General

The Department of Commerce & Consumer Affairs

Federal Resources

United States Department of Justice

- **Report a Crime or Submit a Complaint**
- **Help and Information for Crime Victims**

Homeland Security Investigations (Immigrations & Customs Enforcement)

- **Honolulu Field Office**
- **Report a Crime**

Federal Bureau of Investigation (FBI)

- **Honolulu Field Office** (services the entire state)
- **Report a Crime**

United States Secret Service

- **Website**
- **Office Locator**
- **Investigations**

Internet Crime Complaint Center (IC3)

If you believe you have fallen victim to cyber crime, **file a complaint or report with the IC3**, which is a division under the FBI. Your information is invaluable to helping the FBI and its partners bring cybercriminals to justice.

Home » Crime & Fraud Victim Resources

Adobe Connect

Dora Wildfires Hawaiian Islands ...

ATTENDEE LIST (1)

Hosts (1)

Dale Clites, HSFC You

Presenters (0)

Participants (0)

EDIT YOUR NAME TO REFLECT YOUR AGENCY

The information shared on this platform is considered U//FOUO up to LES. Please hover on your name and Edit your information to include your agency so that all participants are aware of who has access to the information being shared. Mahalo.

PLACE CONTACT INFORMATION HERE

Clarence. D. Clites, HSFC, hsfc@hawaii.gov, c. (808) 475-5077

Gen Tamura, DHS CISA, gen.tamura@cisa.dhs.gov, (808) 445-2161

Kevin Baggs HSFC kevin.l.baggs@hawaii.gov

20230923DR4724HISITREP209A#9.PDF Stop Sharing

1 / 12 53%

MAUI COUNTY CHAT

U//FOUO HSFC MAUI SITREPS

1. Maui SIB 08212023 PK (2).pdf
2. Maui SIB 08222023 PK.pdf
3. Maui SIB 08242023.pdf
4. UFOUO 2023-0815 SAB Maui Daily Situation Report (1).pdf

20230923DR4724HIPLNTRIFOLD22.P... Stop Sharing

GENERAL CHAT

Everyone

Sun, 13 Aug 2023

You: Updated SitReps for 8-13-2023 uploaded to Share File pods. 12:43 PM

Mon, 14 Aug 2023

You: U//FOUO NOC SWO Update 7 uploaded to FEDERAL AGENCY REPORTS pod 10:06 AM

You: 1814 hours, 8-14-2023: All sites back online from previous power outage in downtown Honolulu. Electrical outage disrupted the circuits connecting the DEM EOC, all Warning Points on Oahu including the JTMC, and HSFC at HPD. 11:18 PM

Tue, 15 Aug 2023

You: Updated USCG Notice for Lahaina Harbor and Surrounding Waters uploaded to FEDERAL AGENCY File Share pod. 03:30 PM

Wed, 16 Aug 2023

You: Maui Disaster Update #8 provided by Retail Merchants Hawaii uploaded to SHARE FILE pod. 12:18 PM

Type here

U//FOUO INCIDENT ACTION PLANS

1. 001 Joint IAP Counties Brushfires.pdf
2. 002 Joint IAP Counties Brushfires.pdf
3. 003 Joint IAP Counties IAP Counties Brushfires.pdf
4. DR4724-HI_IAP_004_2023-08-13.pdf
5. DR4724-HI_IAP_005_2023-08-14.pdf
6. DR4724-HI_IAP_006_2023-08-15.pdf
7. DR4724-HI_IAP_006_2023-08-15_751130041.pdf

HAWAII COUNTY CHAT

Everyone

You: 10:02 AM HST: Advisory: Queen Kaahumanu Hwy from Kawaihae Rd to the Westin Hapuna entrance is now OPEN. 03:28 PM

You: 4:20 PM HST: Per Hawaii County PD - Akoni Pule Hwy is no OPEN. 09:21 PM

You: Edit: Akoni Pule Hwy is now OPEN. 09:22 PM

Type here

STATE OF HAWAII CHAT

Everyone Romel Jacob

Wed, 09 Aug 2023

You: Aloha Nancy, please use this area for the State Warning Point communications. 09:32 AM

Nancy HI-EMA: Thank you Dale! 09:34 AM

Type here

FEDERAL AGENCY REPORTS

1. Central Pacific Hurricane Center NWS TWO_briefing_081023.pdf
2. FOUO FEMA Statewide 08.10.23 COP Hawaii Wildfire 1300.pdf
3. MSIB23-006 - Lahaina Harbor and area waters.PDF
4. U--FOUO NOC SWO Sitrep 8-12-2023.pdf
5. U--FOUO NOC SWO Update 11 AUG 2023.pdf
6. FOUO 08.12.23 COP Counties Brushfires 1300.pdf
7. FEMA_Region_IX_DSAR_Aug_13.pdf

FEDERAL AGENCY CHAT

Everyone

Wed, 16 Aug 2023

You: FEMA Region IX Daily Situation Awareness Report 16 August 2023 uploaded to FEDERAL AGENCY REPORTS pod. 12:37 PM

Type here

SHARE FILES HERE (SITUATION REPORTS, ETC.)

1. U--FOUO NOC Situation Report.pdf
2. August-2023-fires-emergency-proclamation.pdf
3. 2023 08 09 1130 PDT - FEMA RIX SPOTREP Hawaiian Wildfires....
4. U--FOUO NOC SWO Multiple Fires Update 2 Hawaiian Islands A...
5. Lahaina Image 1.jpg
6. Lahaina Image 2.jpg
7. Lahaina Image 3.jpg

SHARE WEB LINKS HERE

1. National News: Hawaii Residents Forced to Jump Into Water as Fire Engu...
2. HSIN Connect COP LINK
3. https://www.msn.com/en-us/weather/topstories/evacuation-orders-in-...
4. https://www.cnn.com/us/live-news/maui-wildfires-08-09-23/h_e218c23...
5. https://www.civilbeat.org/2023/08/live-maui-fire-evacuations-closures-...

Type Here

UNCLASSIFIED//FOR OFFICIAL USE ONLY

ENG US 4:45 PM 9/25/2023

nnect

Dora Wildfires Hawaiian Islands ...

LIST (7)

es, HSFC You

ggs, HSFC Guest

ers (5)

ura - DHS CISA Guest

moto HI-EMA Guest

I-EMA Guest

oronel - HIEMA Guest

4 Guest

ants (0)

NAME TO REFLECT YOUR AGENCY

nation shared on this platform is
I U//FOUO up to LES. Please hover
me and Edit your information to
ur agency so that all participants are
ho has access to the information
ed. Mahalo.

TACT INFORMATION HERE

. Clites, HSFC, hsfc@hawaii.gov, c.
5077

ra, DHS CISA,
isa.dhs.gov, (808) 445-2161

DORA2023 MAUI EMA OPEN SHELTERS.JPG Stop Sharing

MAUI COUNTY CHAT

Everyone +

GENERAL CHAT

Everyone +

Today

You: Aloha Everyone, Mahalo for joining this HSIN Connect room to share official information. Please invite your trusted partners involved in response and mitigation of the wildfires in Hawaii and Maui counties. Mainstream media and Social Media platforms are sharing information related to these events. Some of the info is factual, and there is info being spread that is not completely factual. Please share Official Information from

HAWAII COUNTY CHAT

Everyone +

Today

You: Per Hawaii Police Department 06:39 AM HST: Queen Kaahumanu Hwy remains CLOSED from the Kawaihae Road junction to the Westin Hapuna entrance due to a fire. Use alternate routes. 11:41 AM

Type here

STATE OF HAWAII CHAT

Everyone +

Today

You: Aloha Nancy, please use this area for the State Warning Point communications. 09:32 AM

Nancy HI-EMA: Thank you Dale! 09:34 AM

Type here

HONOLULU COUNTY CHAT

Everyone +

Start a conversation with everyone or
chat privately with the Hosts, Presenters or any Attendee

FEDERAL AGENCY CHAT

Everyone +

Start a conversation with everyone or
chat privately with the Hosts, Presenters or any Atte

Type here

KAUAI COUNTY CHAT

Everyone +

Start a conversation with everyone or
chat privately with the Hosts, Presenters or any Atte

Type here

SHARE FILES HERE (SITUATION REPORTS, ETC.)

1. U--FOUO NOC Situation Report.pdf

2. August-2023-fires-emergency-proclamation.pdf

SHARE WEB LINKS HERE

1. National News: Hawaii Residents Forced to Jump Into Water as Fir

2. HSIN Connect COP LINK

3. https://www.msn.com/en-us/weather/topstories/evacuation-orde

4. https://www.cnn.com/us/live-news/maui-wildfires-08-09-23/h_e

SOLUTION SETS

1. Visible & Unified Effort of Information Transparency
2. Counter Narrative
3. One-Stop-Shop for Resources and Answers (FAQ)

Open Discussion

Closing Comments

Office of Homeland Security

dod.ohs@hawaii.gov
https://law.hawaii.gov/ohs/

Backup Slides