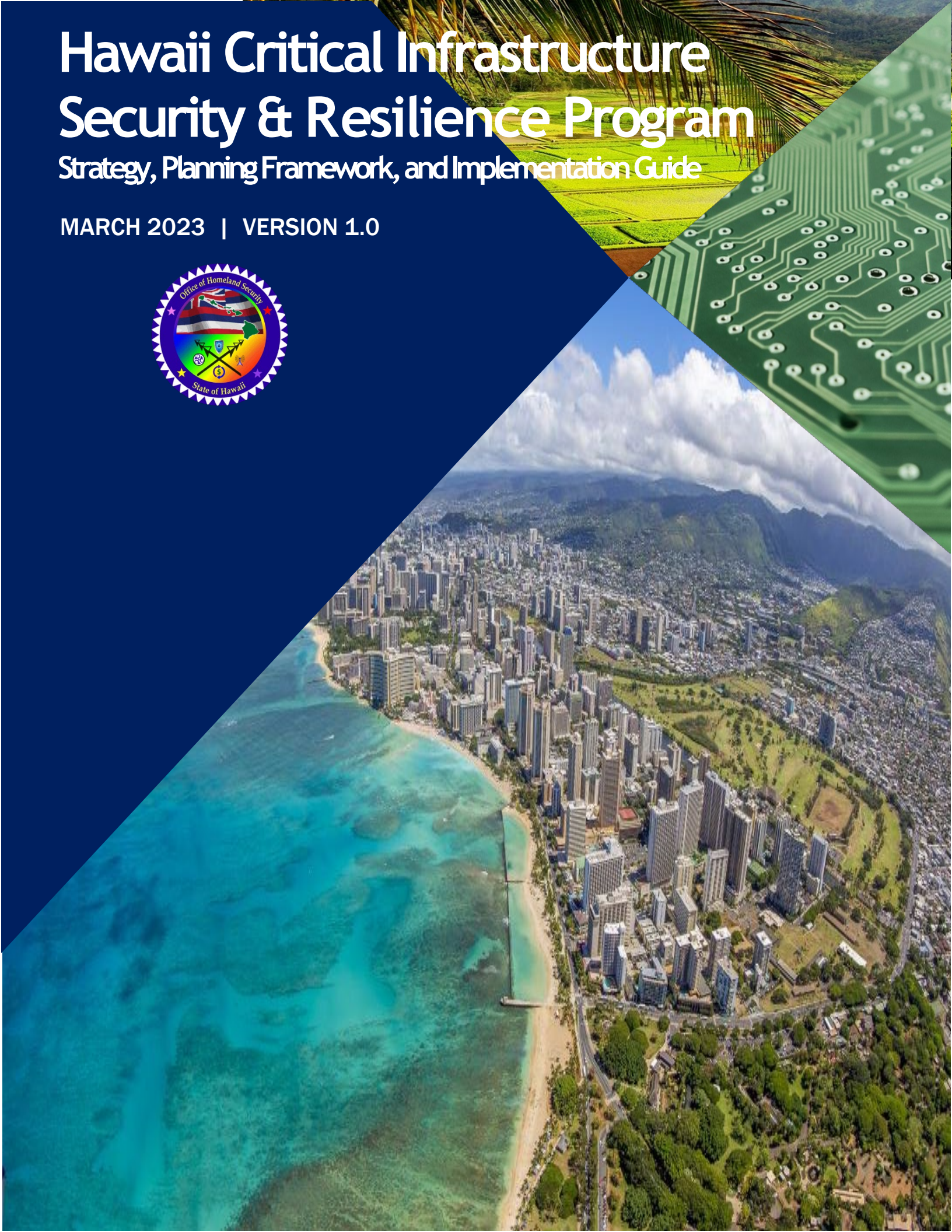
Hawaii Critical Infrastructure Security & Resilience Program

Strategy, Planning Framework, and Implementation Guide

MARCH 2023 | VERSION 1.0



THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

Table of Figures

STRATEGY

The Hawaii Office of Homeland Security (OHS) has developed the Hawaii Critical Infrastructure Security & Resilience Program (CISRP) to enable the incorporation of security and resilience considerations in critical infrastructure planning activities statewide. This framework is based on the groundbreaking work the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) undertook in its development of the Infrastructure Resilience Planning Framework (IRPF). The CISRP relies heavily on efforts undertaken through the Interdependent Critical Energy Infrastructure Memorandum of Agreement (ICEI) Memorandum of Understanding (MOU) (February 2018), to include the Hawaii Critical Infrastructure Interdependency Analysis Guide (January 2020), developed under the auspices of that MOU. Additionally, the shaping and execution of cybersecurity-related efforts, in keeping with the construct of the federal State and Local Cybersecurity Grant Program, will be informed predominantly through the development of the statewide Cybersecurity Program Strategy and Implementation Plan. As such, the cybersecurity elements included below are intended to cover entities and activities that are anticipated to fall outside the purview of the to-be-developed statewide Cybersecurity Program Strategy and Implementation Plan, which is slated to begin in early 2023.

Context

In today's interconnected world, our critical infrastructure and way of life face a wide array of serious risks. Nation-state adversaries and competitors seek to advance their objectives through a variety of hybrid tactics, including subtle actions that significantly weaken the foundations of U.S. power, degrade society's functions, and increase adversaries' ability to hold our critical infrastructure at risk. Extreme weather events and other natural hazards are becoming ever-present. The heightened threat from terrorism and violent crime remains, is increasingly local, and often aimed at soft targets like malls, theaters, stadiums, and schools.

The critical functions within our state are "systems of systems" with complex interdependencies and systemic risks that can have cascading effects during all types of incidents. As networked devices further weave into our lives and businesses, their vulnerabilities provide additional attack vectors for nation states and criminals. Global supply chains introduce the risks of malicious activity in software and hardware, disruptions from physical attacks or natural events, and manipulation for political and economic purposes. Aging, outdated, and under-resourced infrastructures are a challenge across the state. During any emergency, communication between first responders and between decisionmakers is at risk from disruption or lack of interoperability.

Many of these risks are complex, dispersed both geographically and across a variety of stakeholders, and challenging to understand and address. As articulated in the Hawai'i Homeland Security Strategy (March 2022), one of the key objectives under the Strategy's stated goal to "Develop functional core programs to cultivate a state of readiness for homeland security threats" is to "Develop a critical infrastructure program."

Approach

Borrowing from the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) own work in establishing its Strategic Intent (August 2019), OHS has adopted the "Defend Today, Secure Tomorrow" approach for our Hawaii Critical Infrastructure Security & Resilience Program.

A key element of OHS' purpose is to mobilize a collective defense of our state's critical infrastructure. We lead the Hawaii's risk management efforts by bringing together diverse stakeholders to collaboratively identify risks, prioritize them, develop solutions, and drive those solutions to ensure the stability of our state's critical functions. As the state's risk advisor, OHS is unique in its position to partner with private industry, researchers, governmental organizations, emergency responders, intelligence, defense, and other communities.

OHS seeks to achieve two strategic goals across all of our mission space:

First, OHS defends today by addressing the imminent risks facing our state's critical functions. For example, we coordinate collective governmental response to relevant information technology infrastructure during entity-level response to cybersecurity incidents and disruptions that threaten resident and visitor safety and security and state-based critical infrastructure.

Second, OHS secures tomorrow by helping organizations manage their own risk during steady-state conditions. For example, we help soft targets and crowded places plan and secure themselves in advance of an attack or in preparation of large-scale events.

We achieve these ends through a variety of ways that are common across our goals and mission domains through risk analysis, risk management planning, information sharing, capacity building, and incident response. These ways are all reliant on successful partnerships with other stakeholders.

ENDS OVERALL GOALS	GOAL 1			GOAL 2		
	DEFEND TODAY Defend against urgent threats and hazards			SECURE TOMORROW Strengthen critical infrastructure and address long-term risks		
	Seconds	Days	Weeks	Months	Years	Decades

WAYS GENERAL METHODS	**MEANS** SPECIFIC RESOURCES
Risk management planning, governance, and execution	Analysts, risk models, and technical alerts
Risk visibility and analysis	Collaborative planning teams and task forces
Information sharing	Policy and governance actions
Stakeholder engagement	Technical assistance teams and security advisors
Capacity building and technical services	Grants and operational contracts
Incident management and response coordination	Exercises and training

Figure 1 - Strategic Approach: Ways, Means, Ends

Goal 1: Defend Today | Defend Against Urgent Threats

With the right preparations and partnerships, OHS can ensure:

- **Prevention or mitigation of most of the significant threats to state-based critical infrastructure;**
- **Mitigation of impacts of all-hazards events to the greatest extent possible;**

- **Seamless flow of voice, video, and data communications during incident response; and**
- **Appropriate mitigation of significant hybrid, supply chain, and emerging threats.**

A statewide, coordinated effort is necessary to meet these ends. This requires proactive, collaborative, and creative planning of the best ways to respond. Through data and information sharing, we have a unique state position to gain risk visibility. We prevent, mitigate, and respond through alerts and risk reporting, technical assistance, deployed technologies, and collaboration with operational partners. We stand shoulder-to-shoulder with our partners in defending the state and each other.

Desired end-state: Incidents with a potentially significant impact on national security, public health and safety, and economic security are prevented or mitigated.

1.1 Cyber Defense	Significant cyber threats are unable to achieve their objectives in Hawaii.
1.1.1 Visibility	OHS knows current threat activity and strategic interests of all major threat group and has timely access to available data on the risk posture of key infrastructure.
1.1.2 Analysis and Event Management	OHS prioritizes the most urgent risks and coordinates response actions within OHS and with its partners.
1.1.3 Prevention and Response Activities	Prevention and response actions from OHS and its partners prevent or mitigate significant threat activity and vulnerabilities.
1.2 Physical Hazards	Impacts from physical hazards are minimized through coordinated incident preparation and response.
1.2.1 Visibility and Analysis	OHS is aware of imminent threats to critical infrastructure with accuracy and fidelity commensurate with risk to homeland security, public health and safety, and economic security of the State.
1.2.2 Planning and Preparedness Activities	Stakeholders are prepared in advance for specific threats and special events and mass gatherings.
1.2.3 Event Management and Recovery	Impacts are minimized to the greatest extent possible through coordination with partners during an incident.
1.3 Incident Communications	Voice, video, and data communications are available and interoperable during daily operations and incident response.
1.3.1 Emergency Support Function #2	During times of emergency and declared disasters, communications are protected, restored, and reconstituted effectively.
1.3.2 Priority Telecommunications Services	Homeland security and emergency preparedness communications are available and prioritized on commercial networks under all circumstances when network congestion or damage renders conventional communications ineffective.
1.3.3 Incident Communications Support	Emergency communications are operable, interoperable, and resilient during incidents.
1.4 Hybrid, Supply Chain, and Emerging Threats	Hybrid, supply chain, and emerging threats are unable to achieve their objectives in Hawaii.
1.4.1 Visibility and Analysis	OHS has awareness of imminent hybrid, supply chain, and emerging threats and their potential impacts on Hawaii.
1.4.2 Response Planning and Preparedness	Through collaborative planning, stakeholders are prepared in advance of incidents.

1.4.3 Response Actions and Management	Impacts are minimized to the greatest extent possible through response actions and coordination with partners during an incident.

Figure 2 - Goal 1 Objectives

Goal 2: Secure Tomorrow | Strengthen Critical Infrastructure and Address Long-Term Risks

Medium-term risks: OHS will assess and prioritize strategic risk, drive planning and policy efforts, and build the capacity of our stakeholders. As the State's risk advisor, OHS must ensure that growing risks to critical infrastructure and other entities are managed at an acceptable level. That means identifying the serious risks to critical infrastructure and evaluating whether they are being managed appropriately. If there is a gap, OHS must act as the backstop and bring options for technical assistance, help to drive policy changes, or find other creative solutions for mitigation. OHS must support critical infrastructure and other stakeholders so that they have the capabilities to manage state- and national-level risks.

Long-term risks: we need to sow the seeds of change today to make a difference in the years to come. OHS will make a concerted effort to anticipate and address long-term risks, including building systems secure by design and ensuring a national workforce supply to support critical infrastructure.

Desired end-state: The community successfully manages medium- and long-term risks with a significant impact on national security, public health and safety, and economic security.

2.1 Critical Infrastructure Resilience and Capacity Building	The community maintains an appropriate level of security and resilience through risk management and capacity building.
2.1.1 Strategic Risk Posture Awareness	OHS knows the risk postures of critical infrastructure and other entities with accuracy and fidelity commensurate with risk to the homeland security, public health and safety, and economic security of the State.
2.1.2 Planning, Policy, and Governance	OHS effectively uses all available levers, including statutorily required regulatory programs, to drive risk management and ensure appropriate security at critical infrastructure and other entities.
2.1.3 Capacity Building and Mitigation Services	OHS provides tools and services that fill key gaps in the security of critical infrastructure and other entities, establishes relationships to help with defense operations, and increases visibility into the risk posture of the state.
2.2 State Cybersecurity Governance and Capacity Building	Cybersecurity risk in state executive branch agencies is managed at an acceptable level, commensurate with each agency's own risk and that of the broader state enterprise.
2.2.1 Strategic Risk Posture Awareness	OHS knows the risk postures of agencies with accuracy and fidelity commensurate with risk to the critical functions of the state enterprise.
2.2.2 Planning, Policy, and Governance	OHS effectively uses all available governance levers to drive appropriate security within the state enterprise.
2.2.3 Capacity Building Tools and Services	OHS provides tools and services that fill critical gaps in the cybersecurity of state entities, establishes relationships to help with

	cyber defense operations, and increases visibility into the risk posture of the state enterprise.
2.3 Emergency Communications Governance and Capacity Building	Responders at all levels of government can seamlessly share voice, video, and data communications during daily operations and major incidents and events.
2.3.1 Capacity Building Services and Grants	OHS provides grants guidance, technical assistance, training, standard operating procedures, and services to ensure all levels of government can manage their communications resources, strengthen their response, and prepare for emerging technologies.
2.3.2 Governance	OHS effectively facilitates state governance bodies and partners with standards development organizations to share best practices, develop tools and resources, and drive policies and standards to improve interoperability.
2.3.3 Analysis, Planning and Policy	OHS knows the effectiveness of emergency communications across the country and uses the National Emergency Communications Plan and other policy and planning sources to ensure that public safety agencies are effectively managing current and future communications resources.
2.4 Long-Term Risk Management	Long-term risks are addressed through collaborative risk management across the community.
2.4.1 Analysis, Planning, and Innovation	OHS anticipates, understands, and responds to long-term risks.
2.4.2 Secure by Design	Systems, assets, and services are designed with the security and resilience of national critical functions in mind.
2.4.3 State Workforce	There is an appropriate supply of security professionals for the state demand.

Figure 3 - Goal 2 Objectives

INTRODUCTION

Hawaii's well-being relies upon secure and resilient critical infrastructure—those assets, systems and networks that underpin our society. The purpose of the **Hawaii Critical Infrastructure Security & Resilience Program (CISRP)** is to guide the statewide effort to manage risks to the State's critical infrastructure. State of Hawaii (SOH) Critical Infrastructure (CI) is defined 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]

To achieve the desired risk management of critical infrastructure, critical infrastructure partners must collectively identify priorities; articulate clear goals; mitigate risk; measure progress; and adapt based on feedback and the changing environment. Success in this complex endeavor leverages the full spectrum of capabilities, expertise, and experience from across a robust partnership.

This CISRP Strategy and Implementation Plan builds on the framework of the National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience (hereafter referred to as the National Plan).

The audience for this plan includes a wide-ranging critical infrastructure community comprised of public and private critical infrastructure owners and operators; Federal departments and agencies, including Sector-Specific Agencies (SSAs); Hawaii state and county governments; regional entities; and other private and non-profit organizations charged with securing and strengthening the resilience of critical infrastructure in Hawaii.

Managing risks to critical infrastructure requires an integrated approach across this broad community to:

- **Identify, deter, detect, disrupt, and prepare for threats to the State's critical infrastructure;**
- **Reduce vulnerabilities of critical assets, systems, and networks; and**
- **Mitigate the potential consequences to critical infrastructure of incidents or adverse events that do occur.**

This section addresses the following:

- **Key Concepts**
- **Planning for Resilient Infrastructure**
- **Benefits of the Hawaii Critical Infrastructure Security & Resilience Program**
- **The Planning Framework**
- **Alignment to Other Processes**
- **Resources for Funding and Technical Assistance**

[1] Hawaii Critical Infrastructure Interdependency Analysis Guide (January 2020).

Key Concepts[2]

The key concepts described below provide context for this critical infrastructure environment. An understanding of these key concepts influences the state of critical infrastructure and shapes the community's approach to ensuring security and resilience.

- Critical infrastructure represents "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." The National Plan acknowledges that the Nation's critical infrastructure is largely owned and operated by the private sector; however, Federal and SLTT governments also own and operate critical infrastructure, as do foreign entities and companies.
- PPD-21 defines security as "reducing the risk to critical infrastructure by physical means or defens[ive] cyber measures to intrusions, attacks, or the effects of natural or manmade disasters." There are several elements of securing critical infrastructure systems, including addressing threats and vulnerabilities and sharing accurate information and analysis on current and future risks. Prevention and protection activities contribute to strengthening critical infrastructure security.
- Resilience, as defined in PPD-21, is "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions...[it] includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents." Having accurate information and analysis about risk is essential to achieving resilience. Resilient infrastructure assets, systems, and networks must also be robust, agile, and adaptable. Mitigation, response, and recovery activities contribute to strengthening critical infrastructure resilience.
- Security and resilience are strengthened through risk management. Risk refers to the "potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood [a function of threats and vulnerabilities] and the associated consequences;" risk management is the "process of identifying, analyzing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level at an acceptable cost."
- Partnerships enable more effective and efficient risk management. Within the context of this National Plan, a partnership is defined as close cooperation between parties having common interests in achieving a shared vision. For the critical infrastructure community, leadership involvement, open communication, and trusted relationships are essential elements to partnership.

Planning for Resilient Infrastructure

Infrastructure is the backbone of our communities, providing not only critical services (such as water, transportation, electricity, and communications), but also the means for health, safety, and economic growth. These systems often extend beyond our communities, providing service to entire regions and contributing to the delivery of National Critical Functions.

Given the vital importance of infrastructure to our social and economic well-being, it is imperative we ensure our critical infrastructure systems are strong, secure, and resilient. For communities to thrive in

[2] National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience

the face of uncontrollable circumstances and adapt to changing conditions (e.g., evolving security threats, impacts from extreme weather, technological development, and socio-economic shifts), we must work to make our infrastructure more resilient.

Benefits of the Hawaii Critical Infrastructure Security & Resilience Program

The Hawaii Critical Infrastructure Security & Resilience Program (CISRP) and its Planning Framework provide an approach for the state, its counties, and the private sector to work together to plan for the security and resilience of critical infrastructure services in the face of multiple threats and changes.

In many ways, the CISRP complements and supplements other planning activities such as National Institute of Standards and Technology's (NIST) Community Resilience Planning Guide (CRPG).

CISRP provides tools and resources for integrating critical infrastructure into planning as well as a framework for working regionally and across systems and jurisdictions by helping communities and regions:

- Understand and communicate how infrastructure resilience contributes to community resilience;
- Identify how threats and hazards might impact the normal functioning of community infrastructure and delivery of services;
- Prepare governments, and owners and operators to withstand and adapt to evolving threats and hazards;
- Integrate infrastructure security and resilience considerations, including the impacts of dependencies and cascading disruptions, into planning and investment decisions; and
- Recover quickly from disruptions to the normal functioning of community and regional infrastructure.

The CISRP is not a definitive roadmap, but rather a flexible set of guidance documents, tools, and resources to kickstart infrastructure security and resilience planning and incorporate it into existing planning mechanisms. Throughout this guide, we provide links to tools and resources developed by partners other than the Federal or Hawaii State Government. This information is provided "as is" for informational purposes only. OHS does not provide any warranties of any kind regarding this information. OHS does not endorse any entity, product, or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by OHS.

The CISRP helps explore dependency relationships between infrastructure systems to better understand infrastructure risk, develop projects and strategies to address it, and identify funding and implementation resources to act.

Ultimately infrastructure resilience contributes to a more resilient community, and can help develop and maintain a strong, safe, and economically vibrant place to live and work.

The CISRP concerns itself with all 16 sectors of critical infrastructure identified by Presidential Policy Directive 21 (PPD-21) – Critical Infrastructure Security and Resilience, which establishes a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure against

physical and cyber threats. PPD-21 identifies 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

CRITICAL INFRASTRUCTURE SECTOR	TYPICAL COMPOMENTS
1. Chemical	Facilities that manufacture basic chemicals, specialty chemicals, agricultural chemicals, pharmaceuticals, and consumer products
2. Commercial Facilities	Publicly- and privately-owned facilities that draw large crowds of people for entertainment and/or media; gaming; lodging; outdoor events; public assembly; real estate; retail; and sports purposes.
3. Communications	Voice and data services and/or terrestrial, satellite, and wireless communication networks.
4. Critical Manufacturing	Facilities supporting the manufacture of primary metals; machinery; electrical equipment, appliances, and components; and transportation equipment.
5. Dams	Assets in the sector include dam projects, hydropower plants, navigation locks, levees, dikes, hurricane barriers, mine tailings, and other industrial waste impoundments. The National Inventory of Dams lists more than 100,000 dams throughout the United States. A large and diverse set of public and private entities own and operate these facilities under highly distributed regulatory oversight from federal, state, and local entities.
6. Defense Industrial Base	Laboratories, special purpose manufacturing facilities, organizations, and supply chains that perform research and development, design, manufacturing, systems integration, maintenance and servicing of military weapon systems, subsystems, components, subcomponents, or parts that support military operations.
7. Emergency Services	Facilities, communications structures; other specialized equipment supporting/housing law enforcement, fire and rescue services, emergency medical services, emergency management, and public works.
8. Energy	Facilities and systems for electricity generation, transmission, and distribution, and for oil and natural gas extraction, refining, and distribution.
9. Financial Services	Depository institutions, providers of investment products, insurance companies, other credit and financing organizations, and the providers of the critical financial utilities and services that support these functions.
10. Food and Agriculture	Areas or facilities associated with the production, processing, and delivery of consumable products (e.g., restaurants, food outlets, food facilities, and farms).
11. Government Facilities	Facilities owned or leased by federal, state, local, territorial, and tribal governments, as well as government and private sector-owned education facilities and national monuments and icons. Election infrastructure was designated as part of the nation's critical infrastructure as a subsector here in January 2017.
12. Healthcare & Public Health	Public and private healthcare facilities, research centers, suppliers, manufacturers, and other physical assets.
13. Information Technology	Physical assets and virtual systems and networks involved in creating information technology products and services, such as research and development, manufacturing, distribution, upgrades, and maintenance.
14. Nuclear Reactors, Materials, and Waste	Nuclear power reactors and/or their facilities, research and test reactors, cooling ponds, and fuel cycle facilities.
15. Transportation Systems	Aviation, terrestrial or maritime transportation systems (e.g., mass transit, ships, railroad, roadways, and pipeline systems).
16. Water and Wastewater	Potable water systems, wells and wastewater treatment systems.

Figure 4 - Critical Infrastructure Sectors

Importantly, nearly all sectors are reliant on energy, water and wastewater, communications, and transportation systems to function. The CISRP examines these infrastructure systems to identify key dependencies within and between them and incorporate that knowledge into planning.

Alignment to Other Processes

The CISRP and its Planning Framework were based on the DHS Infrastructure Resilience Planning Framework (IRPF) (Version 1.0, October 2021). The IRPF was developed to align with and inform other federal, state, local, tribal, and territorial planning efforts a community may be responsible for executing. (See Figure 5.)

EXISTING FEDERAL, STATE, LOCAL, TRIBAL & TERRITORIAL PLANS	
Capital Improvement Plans	Land Use Plans
Comprehensive/General Plans	Long-Term Recovery Plans
Economic Development Plans	Pre-Disaster Recovery Plans
Emergency Operations Plans	Specific/Area Development Plans
FEMA Logistics Capability Assistance Tool (LCAT)	Threat and Hazard Identification and Risk Assessment (THIRA)
Growth Management Plans	Transportation Plans
Hazard Mitigation Plans	Watershed Management Plans
Housing Plans	Other local and regional plans

Figure 5 - Existing Planning Efforts the CISRP Can Inform

The CISRP steps and the associated tools can be easily integrated into other planning processes, such as comprehensive, hazard mitigation, environmental, capital improvement programming, and regional transportation. Outputs from the CISRP planning framework can inform Step 3 of the Community Resilience Planning Guide (CRPG), Characterizing the Built Environment, and can support nearly every phase of the hazard mitigation planning process by supporting a deeper dive into critical infrastructure and dependencies, getting infrastructure owners to the table, and analyzing risks and hazards, which can in turn be used by the community to apply for Federal grant funding.

Format: Matrix
Type: PDF
Pages: 2
Summary: This matrix illustrates how the planning framework is in alignment with and complimentary to the various other existing federal risk and/or resilience planning processes and guidelines.

*Figure 6 - **LINKED RESOURCE:** Alignment of CISRP to Planning and Risk Management Processes*

Resources for Funding and Technical Assistance

Finally, a key feature of planning is determining resource availability to develop and carry out planning and implementation, so the CISRP provides a compendium of such resources outlining funding opportunities and technical assistance

The CISRP and its Planning Framework can help identify resilience projects that can be incorporated into these plans, allowing for resilience building over the long-term and providing a prioritized list of potential projects that can be implemented with Federal funding following a disaster.

The CISRP aligns with and supports the Federal Emergency Management Agency (FEMA) National Mitigation Investment Strategy and the U.S. Government Accountability Office (GAO) Disaster Resilience Framework.

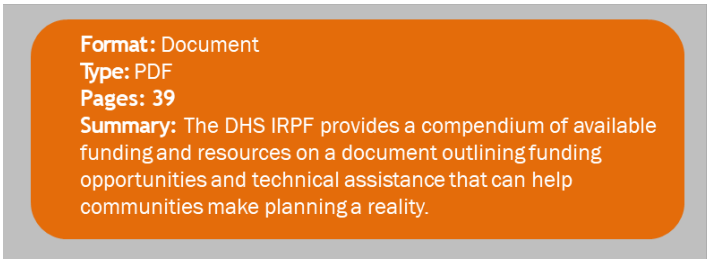


*Figure 7 - **LINKED TOOL:** Compendium of Programs and Mechanisms for Funding Infrastructure Resilience*

THE PLANNING FRAMEWORK

Figure 8 - Hawaii CISRP Planning Framework

The CISRP's Planning Framework is designed to be an easy-to-use framework for incorporating critical infrastructure resilience into state and local plans. It is intended to help improve understanding of critical infrastructure risk, identify opportunities to enhance resilience, and inform policy and investment decisions.

- **In Step 1**, Lay the Foundation, communities define and scope the planning effort, form a planning team to execute the effort, and review existing data, plans, studies, maps, and other resources.
- **Step 2**, Critical Infrastructure Identification, provides guidance to communities on how to identify and prioritize infrastructure and evaluate dependencies among infrastructure systems.
- **Step 3**, Risk Assessment, walks through the process of conducting a risk assessment of critical infrastructure to include evaluating vulnerabilities to threats and hazards, and consequences that may result.
- **Step 4**, Develop Actions, provides guidance on the development of a strategic action plan for addressing risk and enhancing infrastructure resilience by identifying and prioritizing potential solutions.

The CISRP takes a functional, system-based approach and considers the critical functions provided by infrastructure systems as well as the dependencies that exist within and between those systems.

- Individual infrastructure assets are only as important as the ultimate function they help provide; it may not matter that a water treatment plant or pumping station is disrupted during an incident, for example, if there are adequate alternatives for providing potable water to the community until that system can be restored.
- Alternately, infrastructure systems are highly interconnected, and disruption in one may have cascading impacts that affect a range of other infrastructure systems.

A strong understanding of these two factors can help planners identify strategies and projects to reduce their risk and make better investments in resilience.

Step 1. Lay the Foundation

Figure 9 - Process to Lay the Foundation

Step 1 of the CISRP planning framework lays the foundation for success by providing guidance on how to develop initial buy-in, form a collaborative planning group, and collect and review existing data, plans, studies, maps, or other technical resources that may be relevant in informing the planning effort. While this section is structured as a sequential process, many of these "steps" occur simultaneously and iteratively. For example, as a champion and planning team are identified, users may wish to revisit their scope and re-evaluate what past assessments and planning activities are relevant to their current effort. Planners should consider how the CISRP planning framework can best supplement their current planning process, and which steps will add the most value. Ultimately, the framework is intended to be flexible--users are encouraged to adapt the IRPF process as best meets their needs.

This section addresses the following:

- Define and Scope the Effort
- Collect and Review Existing Information
- Form Collaborative Planning Group
- Establish Goals and Objectives

Define and Scope the Effort

OHS, as program manager for CISRP, will serve as both project champion and will provide a Planning Team Lead and Project Manager to actively support the planning process and implementation efforts.

Time and Resources

It is important to adequately staff and fund planning efforts such that resources are dedicated commensurate with resilience goals and the complexity of the work entailed in meeting them. In recognition of time and resource constraints that may exist, the IRPF is designed to support and complement existing or ongoing local and regional planning activities. Thus, it is anticipated that nominal additional resources and time will be required to incorporate the infrastructure resilience concepts outlined in the Hawaii CISRP.

Conduct Preliminary Activities

Once the planning team lead has been identified, they should conduct preliminary activities to lay the foundation for a successful effort. These activities include:

- Defining the purpose of the effort and identifying its relationship to other community planning efforts;
- Defining the scope of the effort (including the planning area);
- Articulating goals and objectives and outlining a strategy for the effort;
- Developing a preliminary schedule;
- Securing a meeting facility;
- Identifying a facilitator to facilitate discussions during planning group meetings (if applicable); and
- Identifying stakeholders that have an interest or information critical to the effort.

Defining Resilience Goals

Defining the resilience goals creates boundaries for the identification of CI. Draft goals can be identified by an executive group, such as the ICEI Working Group and then socialized and refined by the stakeholder community.

Resilience goals are defined in terms of operational restoration time and function. Goals can be state-wide or sector specific. Establishing resilience goals supports the analysis of dependencies/interdependencies across the CI, the prioritization of CI, and the development of mitigation strategies. Examples of resilience goals include:

- SOH emergency response facilities can operate for 7 days without fuel resupply
- Medical facilities can operate for 7 days without fuel resupply
- Indo-Pacific Command facilities can operate critical missions for 10 days without fuel resupply
- Water supplies and wastewater treatment facilities can operate for 10 days without fuel resupply
- Electric grid has repair materials, personnel, and generation resources to restore power to 75% of SOH within 7 days of a catastrophic event
- Non-residents can be evacuated from SOH within 5 days of a catastrophic event
- Major ports can operate within 7 days of a catastrophic event

- Communications industry has repair materials and personnel to restore service for 75% of SOH within 7 days of a catastrophic event
- 14-day food supply available for residents and non-residents
- SOH Department of Transportation can enable movement for 75% of SOH within 7 days of a catastrophic event

Collect and Review Existing Information

To establish a solid foundation for participants, it is important to identify previous planning efforts, studies, mapping, and other data that can inform the effort. These data resources can come from state, county, regional, or federal sources.

Prior to the first planning meeting, the planning team lead should identify and review data and information pertinent to the community's infrastructure assets, systems, and networks, as well as data and information on threats, hazards, and disaster events in the community.

Other existing community plans should also be reviewed to identify information pertinent to the current planning effort. See Figure 5 for a list of community plans to review. During the review, the strategies in these existing plans should be compared to identify any inconsistencies or conflicts that might be resolved through the current planning effort.

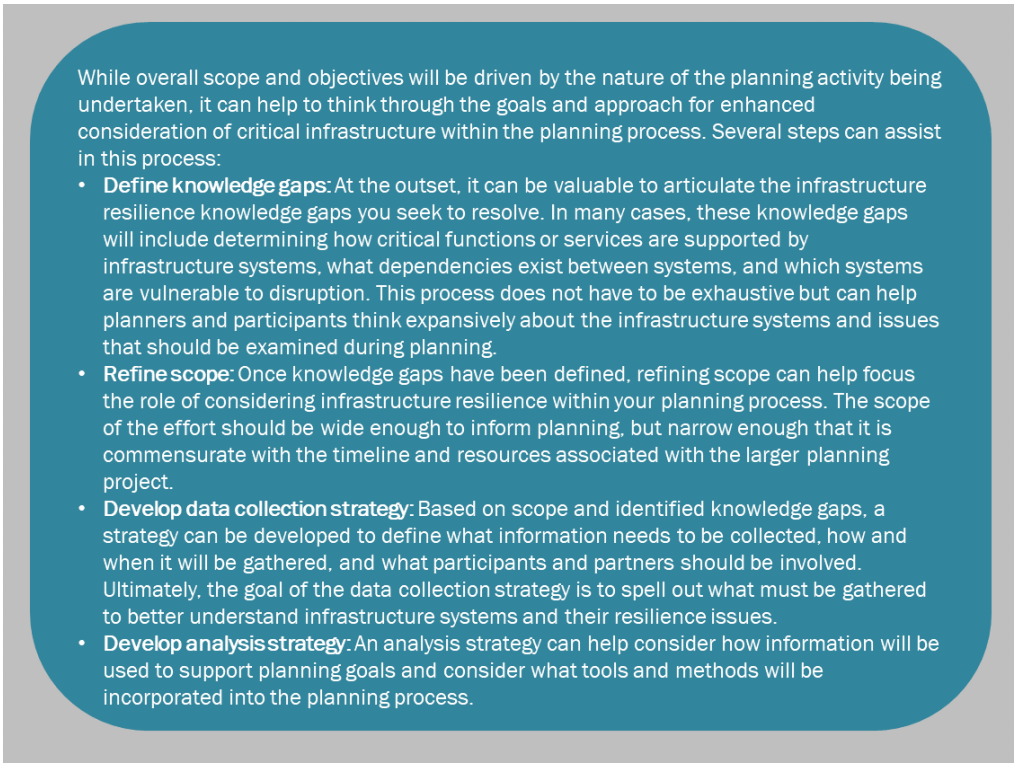


*Figure 10 - **QUICK TIP:** Enhanced Consideration for Critical Infrastructure*

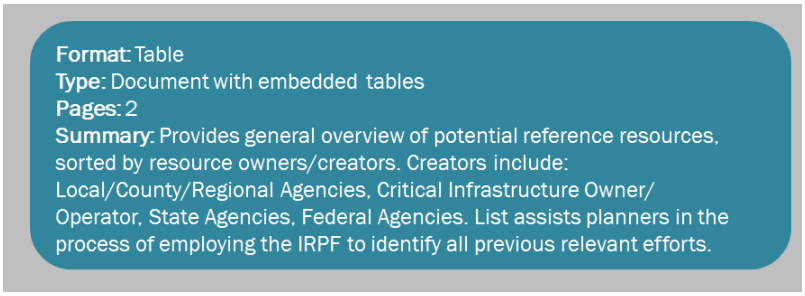


*Figure 11 - **LINKED RESOURCE:** Data Collection Sample List of Resources*

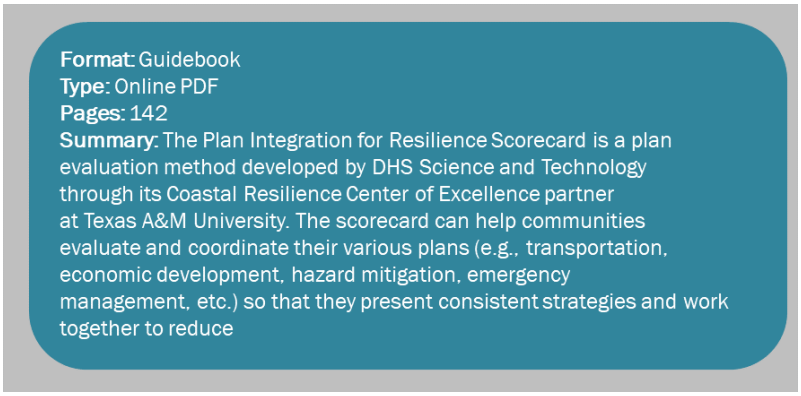


*Figure 12 - **LINKED RESOURCE:** Plan Integration for Resilience Scorecard Guidebook*

Form Collaborative Planning Group

Identify Participants

Establish a group of external partners that can inform the broader planning effort. Inviting participation from representatives of the groups identified in Figure 14 can provide vital insights and perspectives that inform planning efforts and improve resilience. Collaboration is key and can yield the benefits identified in Figure 13.

For the purposes of the CISRP, critical infrastructure stakeholders include community and private sector partners responsible for the planning, design, development, investment in, and operations and management of critical infrastructure assets and systems. This includes elected officials, community leaders, planners, engineers, public works staff, emergency management personnel, business owners and infrastructure operators.

Partners from key sectors can provide operational information about their infrastructure systems that can lead to the identification of resilience challenges and options for improving resilience strategies.

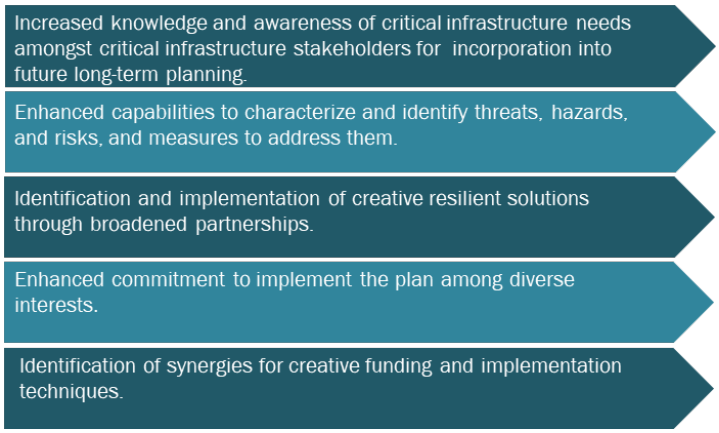


Figure 13 - Results of Effective Collaboration

Engagement should include representatives from service providers, including:

- **Energy**
- **Communications**
- **Transportation**
- **Water and Wastewater**

Additionally, including representatives from the wider community who can provide input about critical infrastructure considered essential to the regular functioning of the community.

Federal, state, and county government agency representatives can provide valuable data and information that will be useful in the collection and review of existing data, plans, studies, and mapping resources; the identification of applicable best practices; and the identification of technical assistance and implementation support. Additionally, their participation can provide political support. If these representatives are not able to actively participate, communities can reach out to these representatives as needed and provide periodic updates throughout the planning process.

Cybersecurity should be considered during the planning process and information technology/security officers or experts that understand the interconnectivity of the cyber infrastructure with the physical infrastructure should be invited to participate. Infrastructure systems and assets increasingly rely on industrial control systems and automated systems that will require cybersecurity expertise to inform planning and investment decisions.

Business risk should be considered in the planning process, so that dependency on critical skills, imports, and other supply chains that are essential to the long-term resilience of the community can be accounted for. This can include discussion with critical infrastructure operators and key businesses. Finding ways to diversify sources proactively will enable the community to be more adaptive as global, national, or local economic conditions change. In November 2020, the Homeland Security Advisory Committee released a report documenting how business risks could impact resilience.

POTENTIAL PARTICIPANTS		
KEY SECTORS		
Communications	Information technology/security officers for each communications sector entity IP-based network services Satellite service providers	State and Local Department of Public Safety/Emergency Management Statewide Interoperability Coordinators (SWICs) Telecommunications service providers
Energy	Electric power engineer & cooperatives Energy distribution system provider Energy generation representatives	Information technology/security officers for each energy sector entity Liquid fuel distributor
Transportation	Bridge engineers Information technology/security officers for each transportation sector entity Port/airport authorities Public transit authorities/providers	Railroad representatives Regional Transportation Authorities/Planners State & county Departments of Transportation Traffic engineers
Water and Wastewater	Information technology/security officers for each water/wastewater sector entity Potable water providers Special Utility Districts	Storm water utilities Wastewater treatment plant/systems operators Water Board
GOVERNMENT AND OTHER		
Buildings and Critical Facilities	Building owners Construction firms Critical facility managers	Developers Hospital & healthcare facility representatives Local industry facility managers
City/County Agencies	Building department staff City managers Community planners Economic development agency staff Elected officials	Emergency Management Health department Law enforcement Legal or general council Public works department staff
Region/State Agencies	State/Tribal/Territorial Emergency Management Environmental quality agencies Health departments	Public Utilities Commission Regional/metropolitan planning agency
Federal Agencies	CISA Department of Energy (DOE) Department of Health and Human Services (HHS) Department of Housing and Urban Development (HUD)	Department of Transportation (DOT) Environmental Protection Agency (EPA) FEMA US Army Corps of Engineers

Figure 14 - Potential Planning Group Participants

It is important to note that not all participants will be involved in all phases of the planning process. Users should consider when participation will be most valuable to avoid placing undue burden on external partners and ensure efficient collection of relevant information. In addition to active planning team participants, there may be other stakeholders that should be involved in the process. Stakeholders are individuals or groups that are affected by, depend on, and interact with a community's infrastructure. These stakeholders should be engaged to get buy-in and support for the planning process and the final outcomes. However, unlike participants, stakeholders may not be involved in all stages of the planning process, but they provide valuable information on a specific topic or input from different points of view in the community. Stakeholders may include:

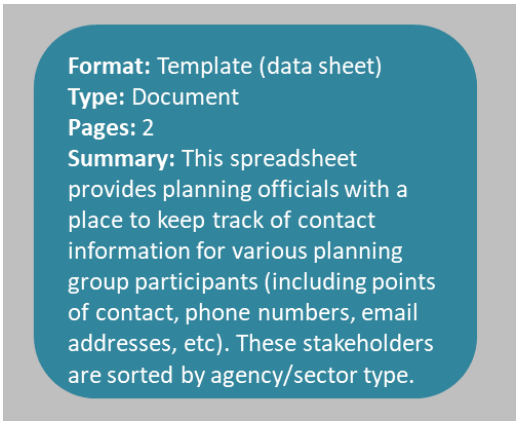


*Figure 15 - **LINKED TOOL:** Planning Participant Contact Information Sheet*

- Local businesses and industry representatives, including critical infrastructure system owners and operators;
- Representatives of the community's social institutions (e.g., community organizations, non-governmental organizations, business/industry groups, health, education, environmental, etc.); and
- Interested citizens of the community.

The planning team lead can develop a distribution list for these other interested stakeholders to provide them with periodic updates of the progress and outcomes of the planning process and opportunities to provide feedback. The planning team lead may also hold interviews with specific stakeholders or groups of stakeholders to garner input during the critical infrastructure identification, risk assessment, and action development steps of the process.

In September 2018 the ICEI identified the following potential stakeholders:

- Hawaii (HI) State Fusion Center
- Emergency responders (e.g., HPD, Red Cross)
- Water/Wastewater/Waste transfer & management
- City Council
- Transportation/Roads (HI Transportation Association, HI DOT)
- Retail/Merchants Association
- Health Care Association
- Hawai'i Harbor Users Group (HHUG)
- Airlines/Maritime – Airports/Ports
- Community Associations/ Mayors/ Neighborhood Boards
- Federal agencies
- Coast Guard
- Volunteer Organization Active in Disaster
- INDO-PACOM/OSD
- FEMA/Pacific Area Office/FEMA Recovery Officer
- Hawai'i Hotel Visitor Industry Security Association (HHVISA) Tourism
- Sierra Club
- HI culture (as it relates to construction)
- Commerce
- City/County governments
- Power/Energy/Fuel Companies
- Blue Planet
- Geographic Information System (GIS) specialists
- Military Installations/DSCA
- Telecommunications
- State & County Emergency Management

Invite Participation and Secure Commitments

After identifying prospective participants and gathering relevant contact information, the planning team lead should invite them to participate. Stakeholders, especially many in private industry may be initially reluctant to participate in planning activities. This can stem from a few causes, including:

- Concerns about potential regulation
- Business sensitivities and concern about sharing proprietary information
- Competing viewpoints of competitors or other key partners

In communication with private sector partners, it is often valuable to highlight the benefits of improved planning for participants. These include quicker, more effective response and recovery for both their businesses and their customer base, potential insurance savings and reduced costs associated with disaster recovery, improved mitigation activities that can improve the resilience of their upstream and downstream dependencies, and an opportunity to better understand community priorities through planning.

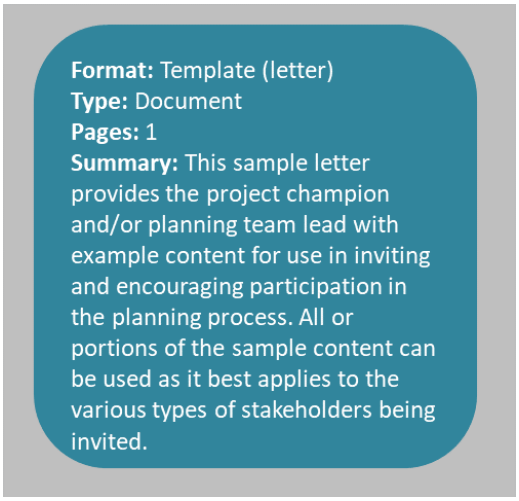


*Figure 16 - **LINKED TOOL:** Stakeholder Invitation Letter*

Establish Goals and Objectives

Setting clear goals and objectives is an essential foundation for any successful planning effort as it defines and supports a community's vision of "where it wants to go" or "what it wants to do" with respect to critical infrastructure security and resilience. It is recommended that the planning team lead establish initial goals and objectives based on the high-level goals identified by the project champion and a review of other community plans.

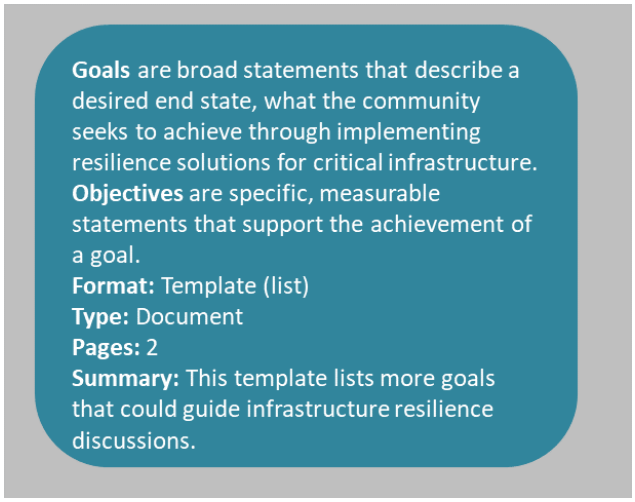


*Figure 17 - **LINKED RESOURCE:** Sample Goals and Objectives*

Goals and objectives development should include the full range of planning factors that address critical infrastructure systems as well as other community outcomes, such as livability, sustainability, the economy, the environment, and equity. It is important to consider community goals for economic security and resilience, as well. Sustainable employment and a productive local economy are fundamental resources for supporting the local government and sustaining viable infrastructure resources.

The initial goals and objectives can be high level. After performing Step 2 Critical Infrastructure Identification, adjustments can be made to these goals and objectives to make them more specific to the critical infrastructure that the group has identified. Be sure to revalidate these updated goals with the project champion. These goals and objectives can also be further refined at later stages of the IRPF planning process (e.g., alongside the development of an action plan in Step 4).

As the community moves through the iterative planning process, new data, facts, and information may become available, at which time the goals and objectives can be adjusted accordingly. Participants/stakeholders will have an opportunity to validate and refine the goals and objectives based on the findings and determinations from the Critical Infrastructure Identification and Risk Assessment steps of the CISRP.

Step 2. Critical Infrastructure Identification

Figure 18 - Process for Identifying Critical Infrastructure

This section addresses the following:

- Identify Infrastructure
- Prioritize Infrastructure
- Identify Dependencies

Identify Infrastructure

It is important to identify infrastructure systems and assets critical to the regular functioning of the community or region. This should include fundamental systems such as energy, water and wastewater, communications, and transportation as well as infrastructure that is critical to the safety, health, and economic vitality of the community. In addition to these sectors, the NIST CRPG also identifies several social functions that contribute to a prospering community, including:

- Community Service
- Economy
- Education
- Family
- Government
- Health
- Media
- Religious & Cultural Beliefs

Each of these functions comprises its own set of critical infrastructure systems from hospitals and nursing homes to schools and churches, to businesses and community centers. As you work to identify critical infrastructure systems in your community, you should consider what facilities and systems support these societal functions.

Additional considerations for identifying infrastructure include:

- Future critical infrastructure systems and assets that are planned or anticipated to support potential future development in the community;
- Infrastructure located across and outside the relevant geographical areas but provide critical services to the community (e.g., transmission lines and pipelines.); and
- Critical infrastructure assets, systems, or networks located within the community that may not provide direct services to the community but are critical to the region or Nation at large.

Planning groups should consider creating a database/matrix listing of the community's critical infrastructure to help catalog and analyze infrastructure assets. Beyond serving as an input for establishing dependencies among community infrastructure, the baseline inventory of infrastructure can be used:

- To describe characteristics of existing infrastructure
- To form the basis for a more comprehensive infrastructure identification effort
- To develop mapping products and other visualizations

As you collect information about critical infrastructure systems and assets in your community, it can be entered into local and regional geospatial platforms, enabling visualization and additional analysis.

The CI list will likely change over time given the identification of dependencies and interdependencies and prioritization. An initial CI list is prepared to start the discussion with stakeholders. Each stakeholder will likely have their own formal (or informal) CI list. The initial list can be created reviewing an existing list of all CI against a set of criteria. Or if a list does not exist, a new CI list can be created based on the same criteria. The review criteria may need to be adapted based on the SOH resilience goals. When

reviewing an infrastructure list, if the answer is "yes" to any of the following questions (adapted from DHS 2012), the asset could be considered CI:

- Would an infrastructure disruption result in significant loss of life?
- Could an incident cause an immediate evacuation of people at the asset and/or the surrounding area?
- Does the asset support a critical state function?
- Does the asset support a critical community function?
- Is the asset necessary for the regional supply chain?
- Does the asset support a national security mission?
- Is the asset essential to the continuity of government (city, county, state or federal)?
- Is the asset critical to response to an incident?
- Is the asset part of DHS's "community lifeline" system?
- Is the asset part of DHS's CI Sectors?
- Does the asset provide an essential product or service?
- Would an incident at the asset result in an adverse environmental impact?
- Is the asset significant to the state's economic stability?
- Is the asset significant to the region's economic stability?
- Is the asset significant to the nation's economic stability?

Once a compiled CI list has been collated from stakeholder input, maps can be developed identifying CI locations. This map may assist with the dependency and interdependency discussion.

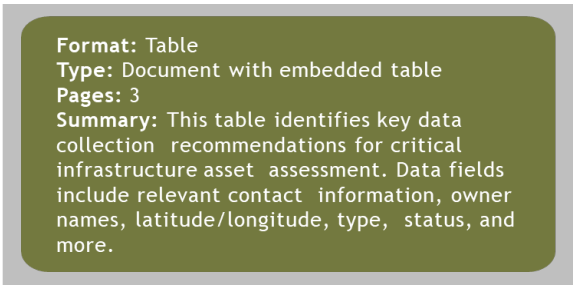


*Figure 19 - **LINKED TOOL:** Recommended Data Fields for Infrastructure Assets Matrix*

Defining Cyber Infrastructure

Communities should understand their reliance on information technology and communications systems required to operate and monitor critical infrastructure and to support key social and economic functions, such as the provision of essential public services and continuity of operations.

Cyber infrastructure is essential for the operations and maintenance of critical infrastructure such as power plants, water and wastewater facilities, hospitals, telecommunications systems, oil and gas refineries, and transportation networks. Due to the interconnectedness of physical and cyber infrastructure, community planners and stakeholders who participate in the planning process should have an understanding of the cyber infrastructure assets, systems, and cybersecurity networks that support and ensure the continued operations of infrastructure systems.

Cyber infrastructure includes a wide array of systems that should be considered, such as:

- Computer systems;
- Control systems used to monitor and control a plant or equipment (e.g., Supervisory Control and Data Acquisition (SCADA));
- Networks, such as the Internet;

- Cyber services (e.g., managed security services);
- Data storage and processing systems, including mainframes, cloud providers, server farms, data centers;
- Hardware and software that process, store, and communicate information, or any combination of these elements within electronic information and communications systems; and
- Data and information within electronic information and communications systems.

In considering cyber infrastructure, it is important for planners to consider factors such as the age, origins, upkeep, and locations of remote service providers, so that the full range of challenges to community resilience can be determined.

Prioritize Infrastructure

Having generated a list of critical infrastructure in the community, the planning team lead or a designated facilitator should lead the planning group in prioritizing the identified infrastructure assets. It is recommended that the planning group focus on the impacts each critical infrastructure system/asset has on the community as a means of determining their criticality and priority. **Figure 20** outlines key impacts to consider. These can be used as criteria with which to prioritize identified critical infrastructure.

Communities can decide to use all of the key considerations listed in **Figure 20** as criteria or simply choose the ones most applicable for their communities. Additionally, communities can modify the key considerations or add their own criteria to best meet their needs.

KEY CONSIDERATIONS	DESCRIPTION
Safety Impact	Effect of the system/asset on loss of life, well-being of individuals in the community, the environment, and the physical condition of other infrastructure systems/assets
Context	Value of the system/asset to the identity of the community, region, or Nation; importance of the system/asset as a priority attribute of the community, region, or nation (e.g., primary industry, identifying feature, cultural symbol, etc.)
Operational Impact	Effect of the system/asset on the overall network's ability to operate; the functional impact of the system/asset associated with dependencies that exist within and among systems/assets
Economic Impact	The potential effect on the economic security of the locality, region, or Nation if this infrastructure had a long-term disruption or degradation
Service Impact	Impact of a disruption of the system/asset on the community, region, or a larger critical infrastructure system based on the service it provides to these entities

Figure 20 - Key Considerations for Prioritizing Infrastructure Systems/Assets

Identify Dependencies and Interdependencies

The National Infrastructure Protection Plan (NIPP)[3] affirms that "effective risk management requires an understanding of the criticality of assets, systems, and networks, as well as the associated dependencies of critical infrastructure that is essential to enhancing critical infrastructure security and

[3] National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience

resilience." Dependencies are relationships of reliance within and among infrastructure systems that must be maintained for those systems to function or provide services.[4] Dependencies have a multiplicative effect, as a threat or hazard can result in the loss of services (such as electric outage) which can impact other critical infrastructure using these resources, further impacting other critical infrastructure that depend on them. An impact to a single node or link can result in significant economic and physical damage on a city-wide, regional, and national scale.[5] An improved understanding of dependencies, especially for key infrastructure systems, can inform risk assessment activities and lead to the identification of new priorities for enhancing resilience.

In order to identify dependencies among infrastructure systems, participants should consider:

- **Primary and secondary sources/providers of resources and services required or used by an infrastructure asset to operate.** For example, when considering energy dependency for an infrastructure asset, a community should identify who the electrical power distribution provider is and where the primary and secondary substations for the infrastructure asset are located.
- **Backup sources of resources to sustain operations of the infrastructure asset in the event of a damaging event.** For example, when considering energy and water dependency for an infrastructure asset, a community should identify on-site backup generators and on-site water storage capacity in the event of a significant incident or change to supply chains.
- **Impacts on downstream infrastructure assets and essential services upon disruption or degradation.** For example, an electric outage could halt operations at a water/wastewater facility as the pumps will not be able to operate and the cyber and information systems will not be able to monitor operations.

The process of identifying the dependencies and interdependencies will likely increase the number of assets on the SOH CI list, and it will provide useful information for the CI prioritization efforts. For the purposes of CI, an asset is considered dependent if it is reliant on another asset or capability of that asset to function, and an asset is considered interdependent if it and another asset are mutually reliant on each other. Discussing the three primary types of asset failure with stakeholders will assist in the identification of CI and identify dependencies and interdependencies (Figure 21). Stakeholder engagement, via a workshop or a series of meetings, is necessary to identify and assess dependencies and interdependencies for an asset's potential for cascading, escalating or common cause failures.

Asset Failure Types	Examples
Cascading failure: A disruption in one asset causes a disruption in at least one other asset.	*The disruption of a distribution network within the natural gas infrastructure can result in failure of an electric utility's generating unit in the service territory of the gas system.*
Escalating failure: A disruption in one asset exacerbates an independent disruption of at least one other asset.	*The time for recovery or restoration of an infrastructure increases because another asset is not available.*

[4] Adapted from the NIST CRPG. While there are multiple dimensions of dependency—including internal, external, time, space, and source dependencies—the assessment process outlined considers physical and functional relationships between different systems (e.g., drinking water systems require electricity to operate pumps).
[5] Argonne National Laboratory; Analysis of Critical Infrastructure Dependencies and Interdependencies (June 2015).

Common-cause failure: A disruption of two or more assets at the same time is the result of a common cause.	*Effects of a natural disaster over a geographical area.*

Figure 21 - Asset Failures that Identify Dependencies and Interdependencies

Figure 22 illustrates the concept of interdependencies using a gas station as an example. While the presence of an operating gas station is essential to ensure movement of emergency vehicles, fuel delivery relies on multiple upstream infrastructures (e.g., power transmission, transportation, etc.). Any operating failure of one of these infrastructures could lead to cascading effects.

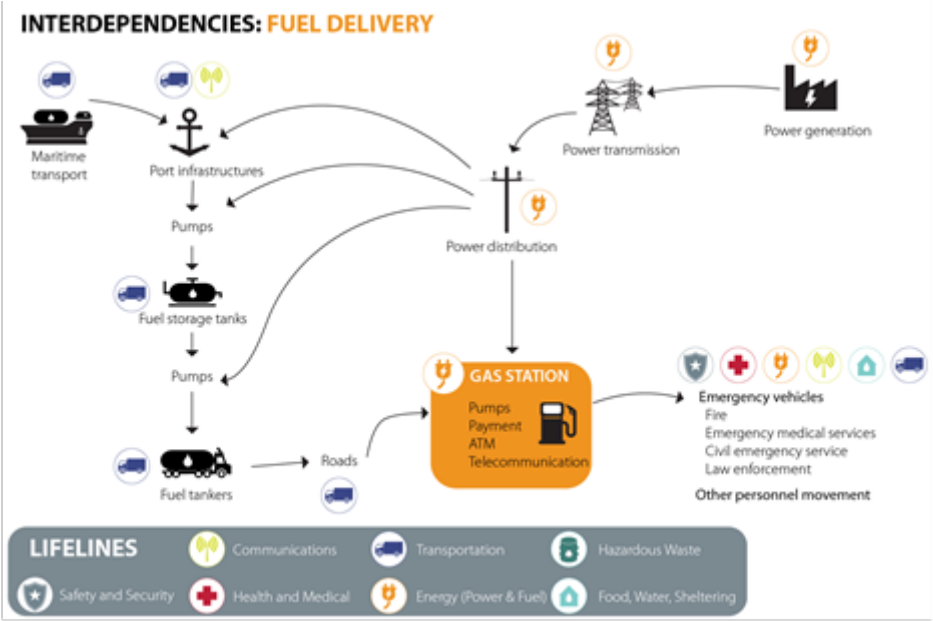


Figure 22 - Dependencies and Interdependencies Example

Dependency and interdependency evaluations include examining:

- Physical relationships—where the material output of one infrastructure is used by another asset, such as in a supply chain, or where electrical controls may be required for pipeline operations.
- Cyber and communications relationships—where an infrastructure uses electronic information and control systems, or a system that relies upon communications systems for control.
- Geographic relationships—such as when infrastructure assets or systems share a common corridor or control the access to another asset.
- Data to characterize and evaluate the energy demand and energy load requirements for each of the priority assets on the CI list.

DEPENDENCY EXAMPLES
Drinking water systems require electricity to operate pumps
Financial services rely on communications to facilitate transactions and communications systems need power to operate
Crews needed to repair electrical distribution systems need access via roads

Delivery of emergency services depend on communications and roads
Cyber and information technology infrastructure is used to operate and monitor power systems, water/wastewater systems, transportation networks, etc.
Need for a resilient supply of commodities, goods, and services, and manpower to operate businesses and infrastructure

Figure 23 - Examples of Typical Dependencies

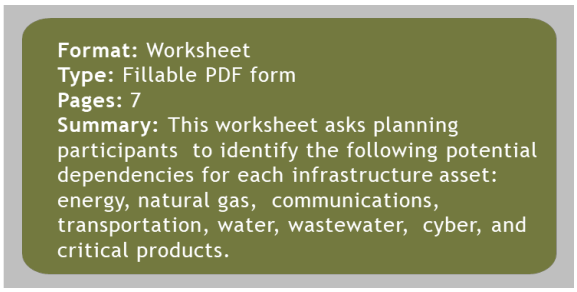


*Figure 24 - **LINKED TOOL:** Dependency Identification Worksheet*

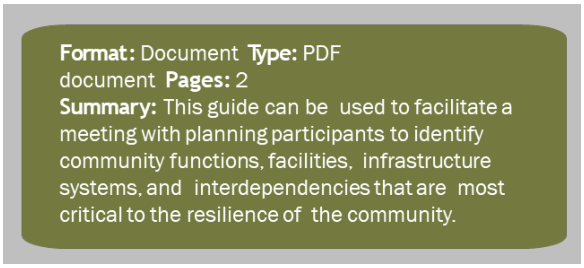


*Figure 25 - **LINKED TOOL:** Meeting Facilitation Guide*

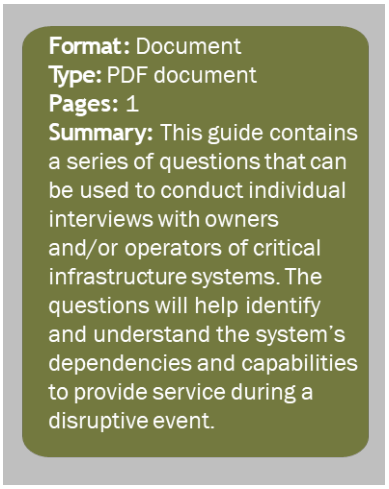


*Figure 26 - **LINKED TOOL:** System Owner/Operator Dependency*

Please Note: Some service providers (e.g., energy and communications) may be hesitant to provide system dependency information in a group setting due to information sharing security and liability concerns. Several approaches for identifying lifeline interdependencies are provided in the dependency identification discussion, interview, and worksheet tools to help account for this.

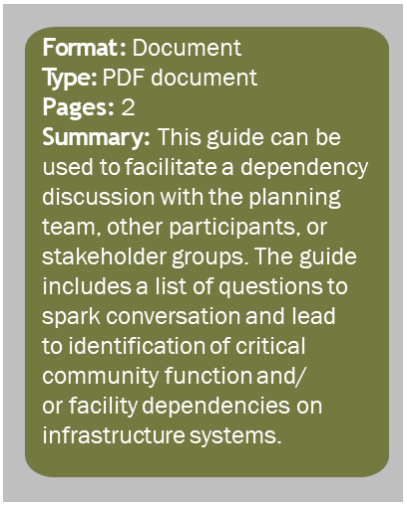


*Figure 27 - **LINKED TOOL:** Community Systems Dependency Discussion Guide*

Step 3. Risk Assessment

Figure 28 - Process for Assessing Risk

Risk Assessment is a process during which information is collected and values are assigned to risk in order to inform priorities, develop and compare courses of action, and inform decision making. A broad range of risk assessment methodologies are utilized by critical infrastructure stakeholders to understand the most likely and severe incidents that could affect infrastructure assets, systems, and networks. Information resulting from assessment is utilized to support planning activities and resource allocation.

The Risk Assessment Methodology utilized for the CISRP planning framework entails:

- identifying the threats and hazards to infrastructure,
- assessing vulnerabilities of prioritized infrastructure,
- assessing consequences and interactions among infrastructure systems, and
- prioritizing risk to infrastructure systems.

Once complete, the risk assessment will guide action development and implementation activities.

Critical infrastructure risk assessments often use hypothetical situations or scenarios to divide identified risks into components that can be individually assessed and analyzed. These situations or scenarios consist of an identified threat, an entity impacted by that threat, and associated conditions including vulnerabilities and consequences.

Critical infrastructure risks can be assessed in terms of the following:[6]

- **Threat:** Natural, man-made or technological occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.
- **Vulnerability:** Characteristic of design, location, security posture, operation, or any combination thereof, that renders an entity, asset, system, network, or geographic area susceptible to disruption, destruction, or exploitation.
- **Consequence/Impact:** Effect of an incident, event, or occurrence, whether direct or indirect.

This section addresses the following:

- Identify Threats and Hazards
- Assess Vulnerability
- Assess Consequences and Interactions
- Prioritizing Risk to Infrastructure System

[6] National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience

Identify Threats and Hazards

There are myriad threats and hazards to which infrastructure systems/assets may be exposed. **Figure 27** identifies potential natural, deliberate, and accidental threats and hazards that should be considered for current and future applicability to priority critical infrastructure. Note: Accidental hazards can be standalone incidents or may be the result of a Deliberate threat or Natural hazard event.

NATURAL	ACCIDENTAL	DELIBERATE
Avalanche	Airplane crash	Armed attack
Drought	Cyber incident	Arson/incendiary attack
Earthquake	Dam failure	Biological agent
Extreme cold	HAZMAT release	Chemical agent
Extreme heat	Industrial accident	Civil unrest
Flood	Levee failure	Conventional bomb/improvised explosive device
Hurricane	Mine accident	Cyber incident
Insect infestation	Power failure	Radio spectrum interference
Landslide	Radiological release	Radiological agent
Pandemics	SCADA system failure	Sabotage
Tornado	Train derailment	Theft
Tsunami	Urban conflagration	
Volcanic eruption		
Wildfire		
Winter storm		

Figure 29 - Example Threats & Hazards by Category

While all hazards and threats can be considered, communities may want to evaluate the likelihood that each one will occur to identify those that should be further assessed for risk. Hazard likelihood can be determined from defined hazard recurrence rates, the frequency of recorded historic events, or good-faith estimations. Sources of information for determining threat/hazard likelihood are identified in Section 3.1.1 and include federal, state, local, tribal, or territorial agencies, as well as colleges and universities. Another valuable source of hazard information is the experience and historical knowledge of planning participants and stakeholders. While it is prudent to prioritize threats/hazards that are most plausible and likely to occur, all hazards can be assessed as time and resources permit.

It is important to recognize that threat/hazard exposure will change over time, and the type, frequency, or magnitude of impacts may vary from experience. Factors such as climate, social and economic conditions, the built environment, and technology are dynamic and should be considered when developing threat and hazard context descriptions. Taking future conditions into consideration will yield sound and resilient infrastructure solutions that may change the risk landscape.

Sources of Threat and Hazard Information

Sources of threat and hazard information include:

- Online national weather-related resources, such as the National Climatic Data Center and the Spatial Hazard Events and Losses Database for the United States (SHELDUS)

Format: Table with external links
Type: Document with embedded table
Pages: 4
Summary: Provides external links to hazard information and analysis resources, including single- and multi-hazard data as well as modeling and analytic tools. Includes links from federal programs such as NOAA, USGS, NIFC, and others.

*Figure 30 - **LINKED RESOURCE:** Hazard Information and Analysis Resources*

- Local or regional National Weather Service offices
- Local resources such as the newspaper, chamber of commerce, local historical society, or other resources with records of past occurrences
- Federal and state disaster declaration history
- FEMA Regional Offices
- Emergency management/homeland security agencies
- CISA Regional Protective Security Advisors
- CISA Regional Cybersecurity Advisors
- CISA Interagency Security Committee Regional Advisors
- CISA Chemical Inspectors
- CISA Emergency Communications Coordinators
- United States Computer Emergency Readiness Team (US-CERT)
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
- SLTT hazard mitigation offices
- State and major urban area fusion centers
- Tribal governments
- Colleges/universities and other research organizations that have threat and hazard-related programs or extension services

Accounting for Cyber Threats

The cyberspace domain and its underlying infrastructure are vulnerable to a wide range of risk stemming from both physical and cyber threats and hazards. In addition, physical infrastructure systems increasingly include automated control systems, which are at risk to these same cyber threats. Malicious actions seek to exploit vulnerabilities to steal information or money or disrupt, destroy, or threaten the delivery of essential services.

Cyber threat Actors can include:

- Hackers
- Organized Crime
- Terrorist Groups
- State Sponsored / Foreign Intelligence Services

Types of Cyber Attacks can include:

- Web Application Attack
- SQL Injection
- Cross-site Scripting
- Phishing
- Spamming
- Application Specific Attacks
- Advanced Persistent Threats
- Malware
- Distributed Denial of Service (DDoS) & Denial of Service (DoS)
- Adware
- Bot
- Ransomware
- Rootkit
- Spyware
- Trojan Horse
- Virus
- Worm

Assess Vulnerability

Participants/stakeholders should assess the vulnerability of the prioritized community infrastructure to the identified threats/hazards. A vulnerability assessment involves the evaluation of specific threats and hazards to infrastructure, with the goal of identifying areas of weakness that could result in consequences of concern.

Vulnerability assessments can inform resilience solutions by identifying internal and external factors that may be exploited by adversaries or impacted by hazards and potential points of failure. The identification of problem statements helps in the development of actions for enhancing security and resilience. Key elements of vulnerability to consider during the assessment are:

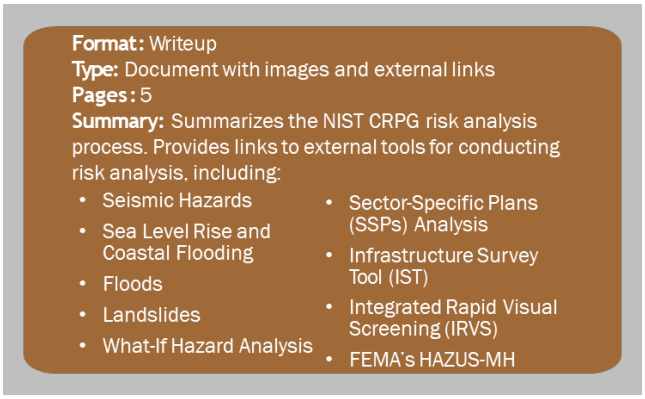


*Figure 31 - **LINKED RESOURCE:** Risk Assessment Methodologies*

- **Accessibility:** vulnerability of an infrastructure asset based upon its general accessibility to the public.
- **Recognizability:** vulnerability of an infrastructure asset based upon how easily recognizable the asset may be to the public.
- **Recoverability:** ability of an infrastructure asset to easily recover from a disruptive event; a qualitative assessment of the asset's ability to return to normal operations considering its dependence on outside services, the capacity at which it is operating, and its own robustness.
- **Susceptibility:** overall vulnerability based on security measures and procedures in place at the infrastructure asset.
- **Proximity:** vulnerability based on an asset's nearness to other susceptible assets.
- **Redundancy:** vulnerability based on whether an asset represents a single point of failure within its overall system.

Assess Consequences/Impacts

Once the threats and hazards have been identified, participants/stakeholders should consider the likely consequences of those hazards to prioritize critical infrastructure. Consequence is the effect of an event, incident, or occurrence and is commonly measured in four ways:

- **Human** (injury, illness, or loss of life)
- **Economic** (costs associated with loss of infrastructure business continuity, and replacement costs)
- **Mission** (ability of an organization or group to meet a strategic objective or perform a function)
- **Psychological** (mental or emotional state of individuals or groups resulting in a change in perception and/or behavior)

Consequence factors to consider when assessing risks to the community's infrastructure include security concerns (costs associated with the loss of infrastructure supporting security or defense mission) and additional variables that can cause localized events to turn into broader disruptions

(dependencies). Historical events can be used to estimate the resulting disruptions to critical infrastructure.

Infrastructure System Risks

Once the threats have been identified and vulnerabilities and consequences have been assessed, they can be combined to determine the risk to prioritized infrastructure. The planning team should work together to compare each threat/hazard, vulnerability, and consequence scenario in order to prioritize them based on which pose the highest risk.

One starting point for prioritization criteria is the list of questions used to identify the SOH CI list. In addition to those questions, whether an asset has dependencies or interdependencies, and whether an asset has the potential of a cascading, escalating or common-cause failure (Figure 32). Additional criteria specific to the SOH resilience goals can be added to further tailor the prioritization effort. For example, a criterion could be specifically focused on the availability of diabetes services within each community that could become isolated during a natural disaster.

#	Prioritization Criteria
1	Would an infrastructure disruption result in significant loss of life?
2	Could an incident cause an immediate evacuation of people at the asset and/or surrounding area?
3	Does the asset support a critical state function?
4	Does the asset support a critical community function?
5	Is the asset necessary for the regional supply chain?
6	Does the asset support a national security mission?
7	Is the asset essential to the continuity of government (city, county, state or federal)?
8	Is the asset critical to response to an incident?
9	Is the asset part of DHS's "community lifeline" system?
10	Is the asset part of DHS's CI Sectors?
11	Does the asset provide an essential product or service?
12	Would an incident at the asset result in an adverse environmental impact?
13	Is the asset significant to the state's economic stability?
14	Is the asset significant to the region's economic stability?
15	Is the asset significant to the nation's economic stability?
16	Is there a dependency on other infrastructure?
17	Are there interdependencies between this asset and other assets?
18	Is there potential for a cascading failure?
19	Is there potential for an escalating failure?
20	Is there potential for a common-cause failure?

Figure 32 - Example Prioritization Criteria

Scoring each of the assets will be somewhat subjective. There are multiple ways this can be managed including having each member of the resilience assessment team score the assets on the CI list and then meeting to reconcile the major differences.

Once the resilience assessment team has developed a prioritized CI list, it will share those results with the broader group of stakeholders to review and address recommended changes as needed. Categorizing the prioritized CI into groupings from highest priority to lower priorities can help with the

validation of the prioritized list. For example, the prioritized list could be parsed into the top 10%, top 25%, bottom 10%, and then provide that information for a separate prioritization of assets by owners/stakeholders. Agreeing to the highest priority assets will help focus the near-term efforts toward addressing the SOH resilience goals. Sharing how a stakeholder's assets ranked will offer them an opportunity to see if their assets are similarly prioritized by the SOH as they are within their own organization.

Step 4. Develop Actions

Figure 33 - Process for Developing Actions

This step of the CISRP planning framework guides communities through the process of identifying and selecting projects and solutions for enhancing critical infrastructure resilience and developing implementation strategies.

This section addresses the following:

- Refine Goals and Objectives
- Identify Resilience Solutions
- Assess Existing Resources and Capabilities
- Select Resilience Solutions
- Develop Implementation Strategies

Refine Goals and Objectives

Prior to identifying and implementing resilience solutions, communities should revalidate their vision and refine their initial goals and objectives for critical infrastructure resilience in more granularity based on the Critical Infrastructure Identification and Risk Assessment findings from steps 2 and 3 of the CISRP planning framework.

In preparation for the development of mitigation strategies, it is useful to review each CI asset for resilience gaps, as it relates to the potential threats for that asset. Documenting this gap analysis helps identify actions that can be taken to resolve any resilience gaps. Questions to ask to identify resilience gaps include:

- Is sufficient backup power available for key equipment, systems, or assets during an emergency?
- Is there redundancy for key equipment, systems, or assets?
- Have emergency operations procedures been developed and tested?
- Is the CI asset or associated systems designed to minimize exposure to the most likely hazards/threats?
- Does the condition of the system reduce the potential for performance degradation or failure?
- Using the collected energy data, what are the potential gaps between the likely energy supply and expected energy demand?

Identify Resilience Solutions to Mitigate Risk

The core result of the IRPF is risk mitigation solutions for community infrastructure. Resilience solutions can be policies, strategies, plans, codes and ordinances, programs to increase resilience, and/or actual infrastructure projects. The following is a list of resilience-enhancing activities. It is not exhaustive, but rather offers possible points of departure.

Format: Table with external links
Type: Document with embedded table
Pages: 9
Summary: Provides a list of sources with external links for resilience solution ideas sorted by disaster type. Provides short description for each link.

*Figure 34 - **LINKED RESOURCE:** Sources for Resilience Solution Ideas*

Potential mitigation activities are highlighted in the following FEMA resources linked here.

- **Mitigation Ideas: A Resource for Reducing Risk to Natural Hazards** provides examples of mitigation actions that would enhance the resilience of the community's infrastructure to various and specific natural hazards.
- **Mitigation Best Practices Portfolio** provides best practice stories and case studies which offer insight into how other communities have taken action to mitigate against disasters.
- **HazardMitigation Planning: Practices for Land Use Planning and Development near Pipelines** provides an overview of risks associated with transmission and distribution pipeline systems and mitigation strategies that can be implemented to reduce these risks.
- **Building Science Branch publications** provide multi-hazard mitigation implementation guidance and ideas for mitigation activities.
- Another resource is **FEMA's Mitigation Action Portfolio** available for download from the Building Resilient Infrastructure and Communities (BRIC) website.

*Figure 35 - **LINKED RESOURCE:** FEMA Mitigation Action Resources*

- **Utilize Land Use Planning Tools.** Communities can incorporate overlays or new zoning ordinances to restrict infrastructure development/ construction in high hazard areas.
- **Update codes and standards.** Based on the threats, hazards, and vulnerabilities identified through the risk assessment process, communities can update codes and standards to mitigate the greatest risks to community infrastructure. All regulatory updates should include accompanying provisions for enforcement.
- **Invest in robust infrastructure.** Communities can use information generated through the risk assessment

process to identify measures that will reduce the vulnerability of key infrastructure to threats and hazards. Potential options include building in spare service capacity, diversifying service networks, diversifying supply chains, designing flexible systems, and reducing service demand through the judicious use of resources.

- **Update infrastructure maintenance and capital improvement programs.** Communities can use the list of prioritized community infrastructure and list of associated dependencies to inform maintenance and renewal priorities for service providers. Existing inspection programs can be augmented to identify infrastructure systems that need improvements that can be prioritized for maintenance.
- **Develop continuity and contingency plans.** Critical infrastructure owners and operators can use information about dependencies to create resourceful, reflective, and flexible continuity plans that help maintain utility services to critical infrastructure during emergency situations. Communities can also use this information to develop effective contingency plans.
- **Incorporate Green Infrastructure.** Consideration of green infrastructure can address climate risk, improve energy efficiency, and reduce resource requirements resulting in not only environmental benefits but also social and economic benefits.
- **Develop an Infrastructure Council.** Consisting of both local government agencies and public and private infrastructure owners and operators, an Infrastructure Council provides a forum for key stakeholders to meet and discuss current activities and issues, dependencies, future development, and opportunities for partnerships and creative funding.

Considering Cybersecurity in Resilience Solutions Identification

Because so much of a community's physical infrastructure is now controlled, in whole or in part, by computers and connected through the internet, planning should consider sound policies and procedures for incorporating cybersecurity improvements into the infrastructure development lifecycle. The following provides some resources to help communities consider cyber threats and take appropriate actions to protect their critical infrastructure.

*Figure 36 - **LINKED RESOURCE:** DHS Cybersecurity Resources*

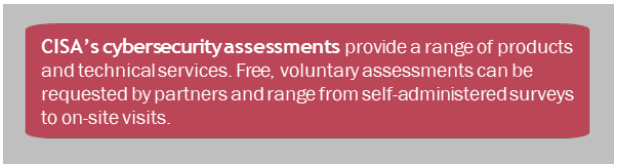


*Figure 37 - **LINKED RESOURCE:** DHS Cybersecurity Assessments*

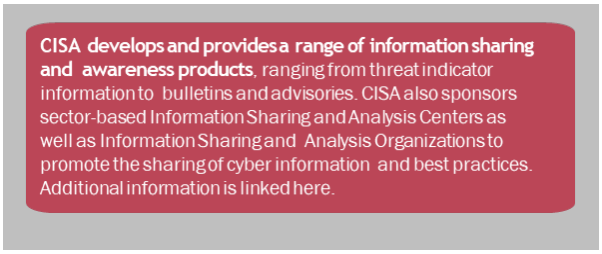


*Figure 38 - **LINKED RESOURCE:** DHS Cybersecurity Information Sharing*

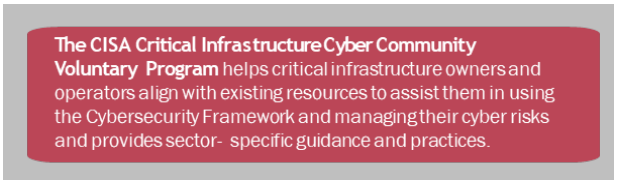


*Figure 39 - **LINKED RESOURCE:** DHS Critical Infrastructure Cyber Community Voluntary Program*

The NIST Cybersecurity Framework provides voluntary guidance, based on existing standards, guidelines, and practices, for organizations to better manage cybersecurity issues, reduce cybersecurity risk, and mitigate vulnerabilities.

*Figure 40 - **LINKED RESOURCE:** NIST Cybersecurity Framework*

Identifying Existing Resources and Capabilities

The action plan can include asking other public and private entities to support implementation to address mutual benefits of resilient infrastructure systems. Identifying and assessing the resources and capabilities of both the community and critical infrastructure owners and operators will help the community prioritize the list of resilience solutions for implementation.

Figure 38 illustrates some of the most common types of existing resources and capabilities that should be considered when prioritizing identification solutions.

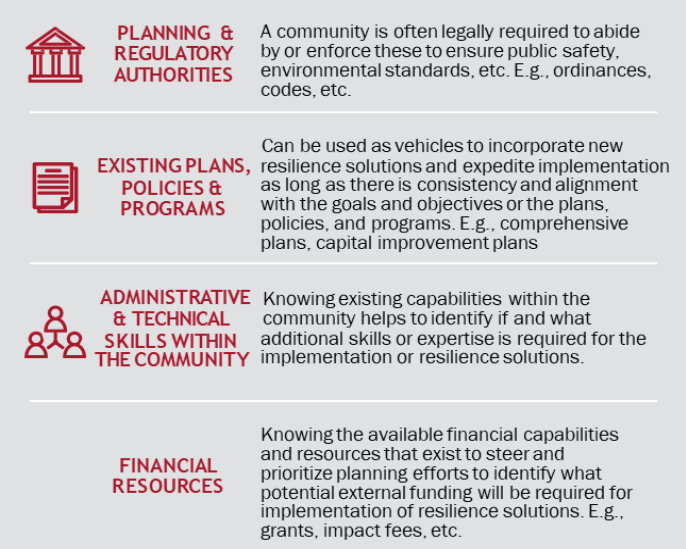


Figure 42 - Common Types of Community Capabilities

Format: Worksheet
Type: Fillable PDF form
Pages: 6
Summary: This worksheet asks planning participants to identify all relevant programs and policies in place to assist in the process of resilience oversight. These capabilities are sorted into the following categories: Regulatory, Administrative/Technical, Fiscal, and Utilities. The final pages of the worksheet ask planning participants to self-assess their degree of capability based on the previous worksheets, and poses a series of additional questions to assist with the self-assessment process.

*Figure 41 - **LINKED TOOL:** Sample Capability Assessment Worksheet*

Format: Guide
Type: Document
Pages: 1
Summary: Questions that can be used to support facilitated discussions and qualitatively analyze alternatives for enhancing resilience.

*Figure 43 - **LINKED RESOURCE:** Mitigation Alternatives Evaluation Guide*

Select Resilience Solutions for Implementation

After producing a list of resilience solutions and identifying capacity, communities should focus their efforts on identifying which public and private entities will need to act for the goals to be achieved.

An evaluation and prioritization process can help weigh the pros and cons of the different identified resilience solutions. The first step is to develop evaluation criteria for assessing the list of resilience solutions. Criteria consideration should include infrastructure criticality, vulnerabilities, and threat/hazard likelihood, in addition the ability to meet the community goals, objectives, and performance measures.

Additional considerations in evaluating resilience solutions may include:

- Planning and operational requirements of the community and the critical infrastructure owners and operators (e.g., comprehensive/ general plans, emergency operations plans, continuity of operations plans, inspection and maintenance plans, etc.)

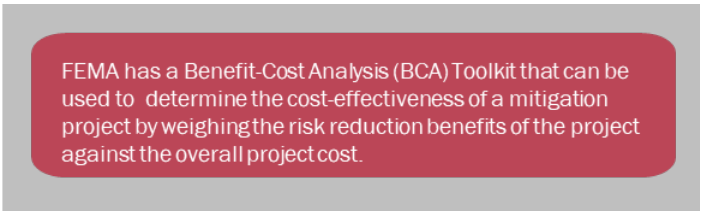


*Figure 44 - **LINKED TOOL:** FEMA Benefit-Cost Analysis (BCA) Toolkit*

- Funding limitations, including operations and maintenance
- Partnership opportunities
- Relevant political priorities
- Community concerns
- Economic impacts

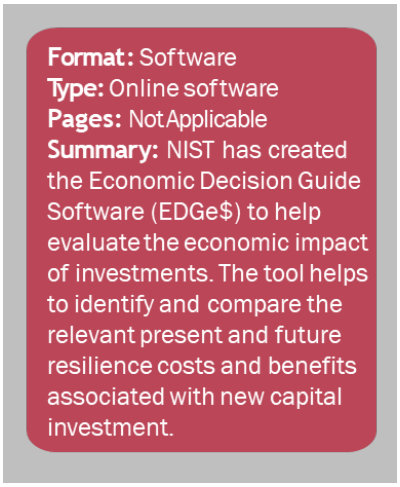


*Figure 45 - **LINKED TOOL:** NIST Economic Decision Guide Software (EDGE$)*

Other evaluation criteria is described in FEMA's Local Hazard Mitigation Planning Handbook (March 2013). It suggests the below evaluation criteria when analyzing potential solutions. Whatever evaluation criteria are used, they should be agreed upon by planning participants/stakeholders.

- **Benefit-Cost:** Are the estimated costs reasonable compared to the probable benefits?
- **Social:** Will the proposed action adversely affect one segment of the population? Will the action disrupt established neighborhoods, break up voting districts, or cause the relocation of lower income people?
- **Life safety:** How effectively will the action protect lives and prevent injuries?
- **Property protection:** How significant will the action be at eliminating or reducing damage to structures and infrastructure?
- **Technical:** Is the resilience solution technically feasible? Is it a long- term solution?
- **Administrative:** Does the community have the personnel and administrative capabilities to implement the resilience solution and maintain it, or will outside assistance be necessary?
- **Political:** Does the public support the resilience solution? Is there political will to support it?
- **Legal:** Does the community have the authority to implement the resilience solution?

- Environmental: What are the potential environmental impacts of the resilience solution? Will it comply with environmental regulations?
- **Local champion:** Is there a strong advocate for the action or project among local departments and agencies who will support the action's implementation?
- **Other community objectives:** Does the action advance other community objectives, such as capital improvements, economic development, environmental quality, or open space preservation? Does it support the policies of the comprehensive plan?

Develop Implementation Strategies

After the resilience solutions are evaluated and prioritized, the community can begin to develop implementation strategies. The implementation strategies describe how each prioritized resilience solution will be implemented and administered by the community. Elements that should be included in the implementation plan are briefly described below:

- **Responsible Party:** A specific agency, department, or position/person should be assigned to carry out the resilience solution.
- **Collaborators/partner agencies/private sector partners:** Other partner agencies or collaborators to assist in the implementation of the resilience solution.
- **Preliminary implementation steps:** Description of the preliminary steps for the implementation of the resilience solution. The responsible person/agency/department and any collaborators/partner agencies can provide input on the preliminary steps for implementation. These steps can be revised over time, as necessary, based on changing conditions, situations, resources, etc.
- **Estimated timeline:** Timeframe for implementation of the resilience solution. The timeframe can detail when the resilience solution will be started and when it should be fully implemented.
- **Resources required for implementation:** Resources include funding, technical assistance, personnel, and materials.
- **Potential barriers to implementation and potential solutions:** Description of potential barriers to implementation and potential solutions to overcome those barriers.

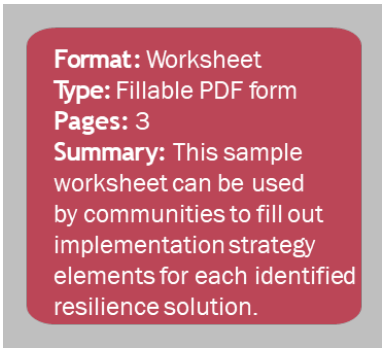


*Figure 46 - **LINKED TOOL:** Resilient Solution Strategy Worksheet*

IMPLEMENTATION AND EVALUATION

Figure 47 - Implementation and Evaluation Process

This section provides information on how communities can implement the prioritized resilience solutions through existing community planning mechanisms, and potential funding and technical assistance sources.

This section addresses the following:

- Implement Through Existing Planning Mechanisms
- Monitor and Evaluate Effectiveness
- Update Plans

Implement Through Existing Planning Mechanisms

One of the best ways for communities to succeed in reducing risks from threats and hazards in the long term is to integrate the prioritized resilience solutions in existing community plans, policies, and programs. Planning participants and other community stakeholders should review the community's operations, priorities, and existing planning mechanisms to see how and where resilience projects and strategies can be integrated. Some examples of existing plans and programs in which resilience solutions can be integrated include:

Format: Table
Type: Document with embedded table
Pages: 3
Summary: Provides an overview of possible integrations with other community planning efforts/ processes. General recommendations.

*Figure 48 - **LINKED RESOURCE:** Planning Framework Plan Integration*

- Capital Improvement Plans
- Comprehensive/General Plans
- Economic Development Plans
- Emergency Communications Plans
- Emergency Operations Plans
- FEMA Hazard Mitigation Plans
- FEMA Threat and Hazard Identification and Risk Assessment (THIRA)
- Growth Management Plans
- Housing Plans
- Land Use Plans
- Long-Term Recovery Plans
- Other community-specific plans
- Pre-Disaster Recovery Plans
- Specific/Area Development Plans
- Transportation Plans
- Watershed Management Plans

Potential Funding and Technical Assistance Sources for Implementation

Format: Document
Type: PDF document
Pages: 39
Summary: The IRPF provides a compendium of available funding and resources on a document outlining funding opportunities and technical assistance that can help communities make planning a reality.

*Figure 49 - **LINKED TOOL:** Compendium of Programs and Mechanisms for Funding Infrastructure Resilience*

There are several ways a community can fund the implementation of its identified resilient solutions. Sources can include traditional infrastructure mechanisms such as taxes, fees, and bonds, as well as grants from federal and state government agencies and philanthropic organizations.

In a time of limited resources at all levels of government, communities should also consider public-private partnerships to develop innovative financing mechanisms. These mechanisms bring additional resources to bear for infrastructure development and can create efficiencies by distributing risks across many parties.

In addition to the compendium linked at **Figure 46**, the FEMA Hazard Mitigation Assistance Grants page provides additional detail and information about FEMA grants.

Various departments and agencies at the Federal, State, and County level, as well as non-profit and professional organizations may also provide technical assistance. Technical assistance is the provision of

technical expertise to assist a community in the design and development of community infrastructure projects incorporating best practices with respect to resilience enhancements.

Monitor, Evaluate, and Assess Effectiveness

All plans should have maintenance procedures developed by the community to monitor, evaluate, and assess the effectiveness of the resilience solutions in meeting the community goals and objectives. Measuring performance provides a foundation for subsequent solution and plan modification in the future.

Exercises may be one way to evaluate the effectiveness of operational plans and resilience solutions. The CISA Tabletop Exercise Package (CTEP) is a resource that can be used by communities and critical infrastructure stakeholders to develop and conduct exercises of plans and procedures.

Key considerations for evaluating plans include the following:

- Have the nature or magnitude of the threats or hazards changed?
- Are there new threats or hazards affecting the community?
- Do the identified goals, objectives, and solutions address current and expected risk conditions?
- Have the resilience solutions been implemented and completed?
- Has the implementation of solutions resulted in expected outcomes?
- Are current resources adequate to implement solutions?
- What other resources are needed to implement the solutions?
- What factors have resulted in successful implementation of solutions?
- What obstacles to implementation have you encountered? What can be done to overcome these obstacles?

Develop Framework to Monitor, Evaluate, and Assess Effectiveness of Resilience Solutions

Communities should develop a framework for monitoring, evaluation, and assessment of the effectiveness of planning efforts. At a minimum, planners should identify:

- **Responsible party:** Who or what agency will be responsible for monitoring implementation? Who or what agency will coordinate the monitoring and evaluation process?
- **Schedule:** When will resilience planning and implementation efforts be evaluated?
- **Process:** What is the process or method in which plans will be monitored and evaluated? What criteria will be used to evaluate the effectiveness of resilience solutions?

Update Plans

Communities should include a process for updating their plans. As a community monitors, evaluates, and assesses the effectiveness of its planning activities, there will be feedback based on successes, obstacles encountered, and lessons learned that can be incorporated into future efforts. The community should consider who or what agency will lead and coordinate a plan update, as well as how and when an update process should be initiated.

The update schedule may be accelerated following a disaster event or concurrent with the development of a recovery or post-disaster redevelopment plan. This allows the community to address subsequent changes in vulnerabilities and priorities, goals, and objectives following a disaster event. Additional funding sources will be available after a disaster event that communities will be able to

leverage for implementation of resilience solutions. Communities should also leverage the greater public awareness and interest in resilience after a disaster event and incorporate infrastructure resilience into additional community planning efforts and strategies.

Key reasons for updating plans include:

- Changes in community development, such as new, recent, or potential development or demographic changes that would impact infrastructure requirements.
- The occurrence of a major incident/disaster.
- Changes in operational resources (policy, personnel, facilities, equipment, or organizational structure) that would impact development or maintenance/operations of infrastructure systems.
- Changes in guidance or standards for the development or maintenance and operations of infrastructure systems.
- Changes in political priorities that would impact buy-in or support for the implementation of resilient solutions to enhance the community's infrastructure systems.
- Changes in the acceptability of various risks and major disruptions to infrastructure systems.

APPENDICES

This section addresses the following:

- Key Terms
- Abbreviations and Acronyms
- Critical Infrastructure Sector Risk Management Agencies (SRMAs)
- References

Key Terms

Community	One or more local jurisdictions or special districts representing a region or shared infrastructure corridor.
Consequence	The effect of an event, incident, or occurrence and is commonly measured in four ways: Human, Economic, Mission, and Psychological.
Critical Infrastructure	Assets, systems, and networks, both physical and virtual, so regionally or nationally vital that their incapacitation or destruction would have a debilitating effect on security, the economy, public health or safety, or any combination thereof.
Criticality	A measure of the importance associated with the loss or degradation of infrastructure.
Cyber Infrastructure	Electronic information and communications systems and services.
Dependency	Relationship of reliance within and among infrastructure systems that must be maintained for those systems to function or provide services. Dependencies can be bi-directional in nature.
Evaluation	Assessing the effectiveness of planning at achieving its stated goals, objectives, and performance measures.
Facilitator	Individual or entity responsible for convening stakeholders and managing dialogue to result in plans and commitments to action. May also serve as the planning team lead.
Goal	Broad statement that describes a desired end state, what the community seeks to achieve through implementing resilience solutions for critical infrastructure.
Man-made Hazard	Criminal or terrorist attack such as an explosive, biological, cyber, or chemical agent that have the potential to disrupt or exploit the community's infrastructure.
Mitigation	The capabilities necessary to reduce loss of life and property by lessening the impact of disasters.
Monitoring	Tracking the implementation of the prioritized resilient solutions.
Natural Hazard	Weather and geological events, such as flood, hurricane, tornado, or earthquake that have the potential to disrupt or incapacitate the community's infrastructure.
Objective	Specific, measurable statement that supports the achievement of a goal.
Physical Infrastructure	Tangible structures or facilities and components that provide infrastructure sector services to communities or regions providing services.
Planning Framework	Steps communities can follow to develop a strategy or list of prioritized actions that enhance the security and resilience of critical infrastructure.
Planning group	Group of individuals within the community from various sectors, agencies, and organizations who add value to the resilience planning process and remain committed throughout the effort.
Planning Team Lead	The key personnel that is involved in and drives the infrastructure resilience planning process throughout and has a working knowledge and understanding of local threats, hazards, and infrastructure. May be dual-hatted as the "facilitator".

Resilience	The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions; includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.
Risk	The potential for an adverse outcome assessed as a function of threats, vulnerabilities, and consequences associated with an incident, event, or occurrence, often measured and used to compare different future situations.
Risk Assessment	An evaluation that considers the types of threats and hazards that threaten community infrastructure systems and weighs vulnerable community infrastructure.
Stakeholder	A stakeholder is a party or entity that delivers, depends on, or is affected by infrastructure service or facility operations, plans or decisions under consideration.
Technological Hazard	Accidental human activities, such as dam and levee construction or the manufacture, transportation, storage, and use of hazardous materials that have the potential to disrupt or incapacitate the community's infrastructure.
Threat	Any entity, action, or occurrence, whether natural or man-made, that has or indicates the potential to pose danger to life, information, operations, and/or property.
Vulnerability	Characteristic of design, location, security posture, operation, or any combination thereof, that renders an entity, asset, system, network, or geographic area susceptible to disruption, destruction, or exploitation.

Abbreviations and Acronyms

ASCE	American Society of Civil Engineers
CIP	Capital Improvement Plan
CISA	Cybersecurity and Infrastructure Security Agency
CRPG	Community Resilience Planning Guide
CTEP	CISA Tabletop Exercise Package
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DOE	Department of Energy
DOT	Department of Transportation
DoS	Denial of Service
EDGe$	Economic Decision Guide Software
EPA	Environmental Protection Agency
FEMA	Federal Emergency Management Agency
FIRM	Flood Insurance Rate Map
HUD	Housing and Urban Development
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IDR	Infrastructure Development and Recovery
IRPF	Infrastructure Resilience Planning Framework
IRVS	Integrated Rapid Visual Screening
IST	Infrastructure Survey Tool
LCAT	Logistics Capability Assessment Tool
NIFC	National Interagency Fire Center
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NOAA	National Oceanic and Atmospheric Administration
PPD	Presidential Policy Directive
PSA	Protective Security Advisor
SCADA	Supervisory Control and Date Acquisition
SHELDUS	Spatial Hazard Events and Losses Database
SLTT	State, Local, Tribal, and Territorial
SME	Subject Matter Expert
SSA	Sector Specific Agency
SSP	Sector Specific Plan
THIRA	Threat and Hazard Identification Risk Assessment
US-CERT	United States Computer Emergency Readiness Team
USGS	United States Geological Survey

Critical Infrastructure Sector Risk Management Agencies (SRMAs)

Chemical	Cybersecurity and Infrastructure Security Agency
Commercial Facilities	Cybersecurity and Infrastructure Security Agency
Communications	Cybersecurity and Infrastructure Security Agency
Critical Manufacturing	Cybersecurity and Infrastructure Security Agency
Dams	Cybersecurity and Infrastructure Security Agency
Defense Industrial Base	Department of Defense
Emergency Services	Cybersecurity and Infrastructure Security Agency
Energy	Department of Energy
Financial Services	Department of Treasury
Food and Agriculture	Department of Agriculture and Department of Health and Human Services
Government Facilities	General Services Administration
Healthcare and Public Health	Department of Health and Human Services
Information Technology	Cybersecurity and Infrastructure Security Agency
Nuclear Reactors, Materials, and Waste	Cybersecurity and Infrastructure Security Agency
Transportation Systems	Department of Transportation
Water and Wastewater Systems	Environmental Protection Agency

References

ANL. 2015. Analysis of Critical Infrastructure Dependencies and Interdependencies. Argonne National Laboratory, Lemont, IL.

DHS. 2008. A Guide to Critical Infrastructure and Key Resources Protection at the State, Regional, Local, Tribal, and Territorial Level. Department of Homeland Security, Office of Infrastructure Protection. Washington, DC.

DHS. 2012. Infrastructure of Concern List Development Process Guide. Official Use Only. Department of Homeland Security, Office of Infrastructure Protection Homeland Infrastructure Threat and Risk Analysis Center. Washington, DC.

DHS. 2013. National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience. Department of Homeland Security, Office of Infrastructure Protection. Washington, DC.

DHS. 2019. National Response Framework Update (Fourth Edition). Department of Homeland Security. Washington, DC.

NIST. 2016. Community Resilience Planning Guide for Buildings and Infrastructure Systems. Department of Commerce, National Institute of Standards and Technology. Washington, DC.

PNNL. 2019. Army Installation Energy and Water Resilience Assessment Guide. Pacific Northwest National Laboratory, Richland, WA.

PNNL. 2020. Hawaii Critical Infrastructure Interdependency Analysis Guide. Pacific Northwest National Laboratory, Richland, WA.