Infrastructure Resilience Planning Framework (IRPF)

NOVEMBER 2022 | VERSION 1.1

Infrastructure Resilience Planning Framework (IRPF)

The **Cybersecurity and Infrastructure Security Agency (CISA)** has developed the **Infrastructure Resilience Planning Framework (IRPF)** to enable the incorporation of security and resilience considerations in critical infrastructure planning and investment decisions.

The IRPF is organized as follows:

0. Overview

This section addresses the following:

0.1 INTRODUCTION

0.2 PLANNING FOR RESILIENT INFRASTRUCTURE

0.3 THE INFRASTRUCTURE RESILIENCE PLANNING FRAMEWORK (IRPF)

0.4 ALIGNMENT TO OTHER PROCESSES

0.5 RESOURCES FOR FUNDING AND TECHNICAL ASSISTANCE

0. Overview

0.1 INTRODUCTION

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 networks are strong, secure, and resilient. In order for communities to thrive in 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.

Presidential Policy Directive 21 (PPD-21) – Critical Infrastructure Security and Resilience defines resilience as the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Infrastructure resilience depends on both physical attributes of engineered infrastructure systems and on the capabilities of organizations affecting the operation and management of those systems (e.g., infrastructure owners and operators, regulatory authorities, and vendors and contractors). Resilience is also influenced by organizational factors such as the existence of business continuity and emergency response plans, the level of workforce training, and the frequency of exercises to test plans. Developing resilience is essential to managing the wide range of risks that communities face, including those presented by dependencies between and among infrastructure systems.[1]

The Cybersecurity and Infrastructure Security Agency (CISA) developed the Infrastructure Resilience Planning Framework (IRPF) to provide an approach for localities, regions, 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. The primary audience for the IRPF is state, local, tribal, and territorial governments and associated regional organizations; however, the IRPF can be flexibly used by any organization seeking to enhance their resilience planning. It provides resources for integrating critical infrastructure into planning as well as a framework for working regionally and across systems and jurisdictions.

This framework provides methods and resources to address critical infrastructure security and resilience through planning, 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, 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

For the purpose of this document, “community” should be understood to include not just individual cities or towns, but also multijurisdictional regional authorities conducting planning and stakeholders with common interests or working on a common corridor to enhance the resilience of related infrastructure systems.

0.2 PLANNING FOR RESILIENT INFRASTRUCTURE

The IRPF is not a definitive roadmap, but rather a flexible set of guidance documents and resources to kickstart infrastructure security and resilience planning and incorporate it into existing planning mechanisms.* While the IRPF is structured as a set of sequential steps, the user can choose which steps and sets of resources to more fully

1 Methodology for Assessing Regional Infrastructure Resilience, CISA, 2021, pg. 8-16 https://www.cisa.gov/sites/default/files/publications/DIS_DHS_Methodology_Report_ISD%20EAD%20Signed_with%20alt-text_0.pdf

* Throughout this guide, we provide links to resources developed by partners other than the Federal Government. This information is provided “as is” for informational purposes only. CISA does not provide any warranties of any kind regarding this information. CISA 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 CISA.

consider infrastructure in any existing or on-going planning process. Communities can review the framework to determine where they are in the planning spectrum and choose the guidance and resources that best serve their needs.

Communities with limited time and resources may want to focus on the infrastructure sectors that support critical functions, such as energy, communications, transportation, and water and wastewater systems initially, with the potential to expand later.

Conversely, communities with more time and resources could consider all other critical infrastructure sectors deemed important and/or vital to the continued performance of key social and economic functions integral to the community or regional prosperity.

The IRPF helps users 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 take action.

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. This can help form a self-reinforcing cycle whereby increased social and economic resilience lead to increased infrastructure resilience and vice versa.

0.3 THE INFRASTRUCTURE RESILIENCE PLANNING FRAMEWORK (IRPF)

The IRPF is designed to be an easy-to-use framework for incorporating critical infrastructure resilience into local, regional, and Tribal plans. It is intended to help communities, regions, and infrastructure owners and operators better understand critical infrastructure risk, identify opportunities to enhance resilience, and inform policy and investment decisions.

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 communities 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.

Step 5, Implement & Evaluate. Focuses on incorporating infrastructure resilience projects and strategies into community and regional plans and processes for measuring success.

To support these efforts, the IRPF also includes an assortment of resources to assist communities as they move through the various steps of the IRPF.

RESOURCES AVAILABLE!

Throughout this guide, the IRPF provides assistance as indicated by the symbols below. The goal of this is to provide a comprehensive list of resilience planning resources available to all jurisdictions. The IRPF identifies resources by entity (federal, state, non-profit, etc.), eligibility, infrastructure sector, etc.

The IRPF encourages planners to take a functional, system-based approach when considering critical infrastructure. 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. Because of these two factors, the IRPF encourages planners to consider the critical functions provided by infrastructure systems as well as the dependencies that exist within and between those 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.

The IRPF can be applied to 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. These critical infrastructure sectors are listed in Table 1, including a brief description of the typical components that comprise each sector. While PPD-21 takes a national perspective on critical infrastructure systems and assets, these sectors are also relevant at the local, state, and regional level and understanding risk to these systems can improve security, health and safety, and economic growth in your community.

Within every community and region, these sectors provide critical functions through infrastructure systems. These systems are composed of assets that are linked to and reliant on one another, and the continued operation of these systems is dependent not only on their own assets, but also other systems in other sectors. Importantly, nearly all sectors are reliant on energy, water and wastewater, communications, and transportation systems to function. The IRPF helps users examine these infrastructure systems, identify key dependencies within and between them, and incorporate that knowledge into planning.

Table 1. Critical Infrastructure Sectors

CRITICAL INFRASTRUCTURE SECTOR	TYPICAL COMPONENTS
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.
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 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/Wastewater Systems	Potable water systems, wells and wastewater treatment systems.

0.4 ALIGNMENT TO PLANNING EFFORTS AND FEDERALLY RECOGNIZED PROCESSES

It is important to note that 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. Table 2 identifies some of the existing planning efforts which the IRPF can inform.

The steps and the associated resources can be easily integrated into other planning processes, such as comprehensive, hazard mitigation, environmental, capital improvement programming, and regional transportation. In fact, a key benefit of the IRPF is that it can help identify resilience projects that can be incorporated into these plans, allowing a community to build its resilience over the long-term and providing a prioritized list of potential projects that can be implemented with Federal funding following a disaster. Additionally, the IRPF 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. While FEMA has established a series of "community lifelines" that, at first, may seem to be at odds with CISA's sector-based approach, these two frameworks are in fact complementary. The community lifelines established by FEMA align with CISA's infrastructure sectors and are intended to support response operations, whereas CISA's 16 sectors can support steady-state activities.

Table 2. Planning Efforts the IRPF Can Inform

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

QUICK TIP

The IRPF can support nearly every phase of the hazard mitigation process by providing a deeper dive into critical infrastructure and dependencies, getting infrastructure owners to the table, and analyzing risk from hazards, which can in turn be used by the community to apply for Federal grant funding. For additional resources, please refer to the **Infrastructure Resilience Planning Resources**.

THERE'S A RESOURCE FOR THAT!

Alignment of IRPF to Federal Planning and Risk Management Processes

This matrix illustrates how the IRPF is in alignment with and complimentary to the various other existing federal risk and/or resilience planning processes and guidelines.

View resource in the Infrastructure Resilience Planning Resources.

Methodology for Assessing Regional Infrastructure Resilience

Based on lessons learned from CISA's Regional Resiliency Assessment Program, this assessment methodology provides a common process for assessing and addressing complex infrastructure resilience issues validated through a decade of RRAP project experience.

View resource in the Infrastructure Resilience Planning Resources.

In many ways, the IRPF complements and supplements other resilience guides and methodologies. For example, outputs from the IRPF can inform Step 3, Risk Assessment, and Characterizing the Built Environment of the National Institute of Standards and Technology (NIST) Community Resilience Planning Guide (CRPG). In addition, the infrastructure resilience assessment process documented in CISA's Methodology for Assessing Regional Infrastructure Resilience closely aligns with the planning steps and guidance outlined in the IRPF.

0.5 RESOURCES FOR FUNDING OPPORTUNITIES AND TECHNICAL ASSISTANCE

A key feature of planning is determining resource availability to develop and carry out planning and implementation. The IRPF provides a compendium of these resources in both a document and a user-friendly matrix, outlining funding opportunities and technical assistance that can help communities make planning a reality.

THERE'S A RESOURCE FOR THAT!

Compendium of Programs and Mechanisms for Funding Infrastructure Resilience

The Compendium of Programs and Mechanisms for Funding Infrastructure Resilience provides a list of potential funding and technical assistance sources with links.

View resource in the Infrastructure Resilience Planning Resources.

1. Lay the Foundation

This section addresses the following:

1.1 IDENTIFY A PROJECT CHAMPION

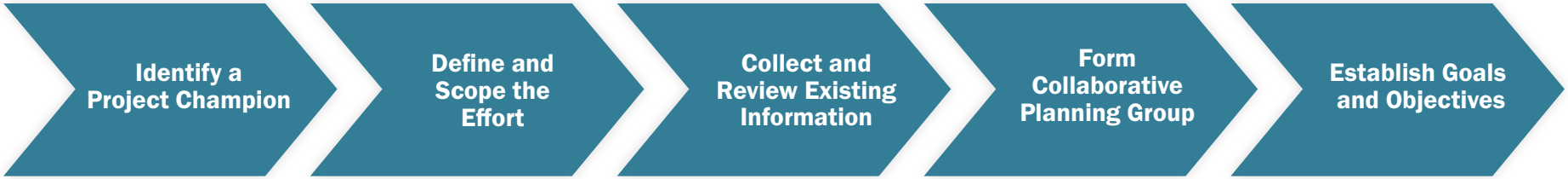
1.2 DEFINE AND SCOPE THE EFFORT

1.3 COLLECT AND REVIEW EXISTING INFORMATION

1.4 FORM COLLABORATIVE PLANNING GROUP

1.5 ESTABLISH GOALS AND OBJECTIVES

1. Lay the Foundation



Step 1 of the IRPF 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 IRPF 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.

1.1 IDENTIFY A PROJECT CHAMPION

To develop buy-in, it is important that an individual entity who champions the importance of resilience provide support in the form of time and resources to the planning effort. This champion can be a state division, tribal council, local jurisdiction, community planning department, regional planning organization, public/private non-profit, or other organization who is leading the development of a plan. What is important, is that this entity is able to actively support the planning process and implementation efforts.

1.2 DEFINE AND SCOPE THE EFFORT

Prior to integrating the IRPF into a planning process, several questions should be considered to define the effort:

- What is driving the desire or need for resilience planning?
- What are the community's resilience goals and objectives?
- Are there specific shortcomings in infrastructure serving the community that need to be addressed?

There are many types of assessments and analysis that can inform planning, from threat, vulnerability, and criticality analysis, system mapping and diagramming, to modeling and simulation analysis. Defining clear goals, objectives, and scope can help planners determine what forms of analysis will best support their efforts. The Methodology for Assessing Regional Infrastructure Resilience provides additional detail on analytic methods that planners can use to improve their understanding of infrastructure systems in their community, drawn from more than 10 years of experience and more than 120 unique assessments. Once the overall direction of the effort has been determined, a community can more effectively allocate time, funds, and personnel to match the scope of the effort.

PLEASE NOTE

One critical component of success for the IRPF planning process is **process documentation**. At all stages of the IRPF, coordinating leadership and documenting all planning efforts is very important. Take care to ensure proper note-taking, and try to keep regular backups (with redundancies, if possible) of all relevant files.

1.2.1 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 IRPF.

QUICK TIP

Communities may be able to save money by incorporating IRPF processes and resources with existing planning practices being funded by grants or technical assistance, such as hazard mitigation, comprehensive, or economic development planning.

1.2.2 Identify a Planning Team Lead

Strong leadership is needed throughout the IRPF integration process, and a planning team lead should serve as a project manager. In most cases, the lead will be an individual from the project champion entity. At a minimum, the lead should report to the project champion, community officials and others as necessary, to provide progress updates and results of the various activities related to the planning process. Table 3 identifies qualifications for a good planning team lead.

Table 3. Planning Team Lead Qualifications

WHAT MAKES A GOOD PLANNING TEAM LEAD?
1. Working knowledge of local and regional infrastructure, such as public works
2. Understanding of threats and hazards, risks, and consequences
3. Ability to engage a broad spectrum of stakeholders to participate in the planning process and provide expertise on critical infrastructure issues
4. Ability to perform administrative, coordination, and event-planning functions and facilitate planning sessions

1.2.3 Conduct Preliminary Activities

Once the planning team lead has been identified, he/she 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)
- Identifying stakeholders that have an interest or information critical to the effort

PLEASE NOTE

It can be challenging to get all the right stakeholders together and ensure a diverse range of opinions and interests are considered. It can be helpful to hold a stakeholder assessment or analysis with the project champion to determine the multiple organizations that should be included. Repeating this process as stakeholders are added can create a snowball effect of increasing the effectiveness of outreach.

PLEASE NOTE

Collaboration and Safeguarding Information

Planners should be aware of information sharing concerns and consider how sensitive material will safeguarded. Use common cyber security methods like password protected documents in conjunction with Non-Disclosure Agreements. There are existing resources such as the Congressionally mandated Protected Critical Infrastructure Information (PCII) which is designed to protect private sector infrastructure information voluntarily shared without exposing sensitive data, as well as the Transportation Security Administration (TSA) SSI Program which protects and redacts Sensitive Security Information (SSI).

1.3 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, local, tribal, and territorial (SLTT), 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 Table 2 in Section 0.2 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.

QUICK TIP

While overall scope and objectives will be driven by the nature of the planning activity being undertaken, it can help to think through the goals and approach for enhanced consideration of critical infrastructure within the planning process. Several steps can assist in this process:

- **Define knowledge gaps:** At the outset, it can be valuable to articulate the infrastructure resilience knowledge gaps you seek to resolve. In many cases, these knowledge gaps will include determining how critical functions or services are supported by infrastructure systems, what dependencies exist between systems, and which systems are vulnerable to disruption. This process does not have to be exhaustive but can help planners and participants think expansively about the infrastructure systems and issues that should be examined during planning.
- **Refine scope:** Once knowledge gaps have been defined, refining scope can help focus the role of considering infrastructure resilience within your planning process. The scope of the effort should be wide enough to inform planning, but narrow enough that it is commensurate with the timeline and resources associated with the larger planning project.
- **Develop data collection strategy:** Based on scope and identified knowledge gaps, a strategy can be developed to define what information needs to be collected, how and when it will be gathered, and what participants and partners should be involved. Ultimately, the goal of the data collection strategy is to spell out what must be gathered to better understand infrastructure systems and their resilience issues.
- **Develop analysis strategy:** An analysis strategy can help consider how information will be used to support planning goals and consider what resources and methods will be incorporated into the planning process.

THERE'S A RESOURCE FOR THAT!

Data Collection – Sample List of Resources

The Sample List of Existing Resources provides a general overview of potential reference resources, sorted by resource owners/creators. Creators include:

- Local/County/Regional Agencies
- Critical Infrastructure Owners/Operators
- State, Tribal, and Territorial Agencies
- Federal Agencies

The goal of this list is to encourage that planners employing the IRPF framework identify all previous relevant efforts.

View resource in the Infrastructure Resilience Planning Resources.

Comparison of Existing Community Plans

The Plan Integration for Resilience Scorecard is a plan evaluation method developed by Department of Homeland Security (DHS) Science and Technology through its Coastal Resilience Center of Excellence partner at Texas A&M University. The scorecard can help communities evaluate and coordinate their various plans (e.g., transportation, economic development, hazard mitigation, emergency management, etc.) so that they present consistent strategies and work together to reduce vulnerabilities to hazards.

View the resource at this link and in the Infrastructure Resilience Planning Resources.

1.4 FORM COLLABORATIVE PLANNING GROUP

1.4.1 Identify Participants

One approach for incorporating critical infrastructure resilience into planning is to establish a group of external partners that can inform the broader planning effort. Inviting participation from representatives of the groups identified in Table 4 can provide vital insights and perspectives that inform planning efforts and improve resilience. Collaboration is key and can yield the benefits identified in Figure 1.

For the purposes of the IRPF, 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.

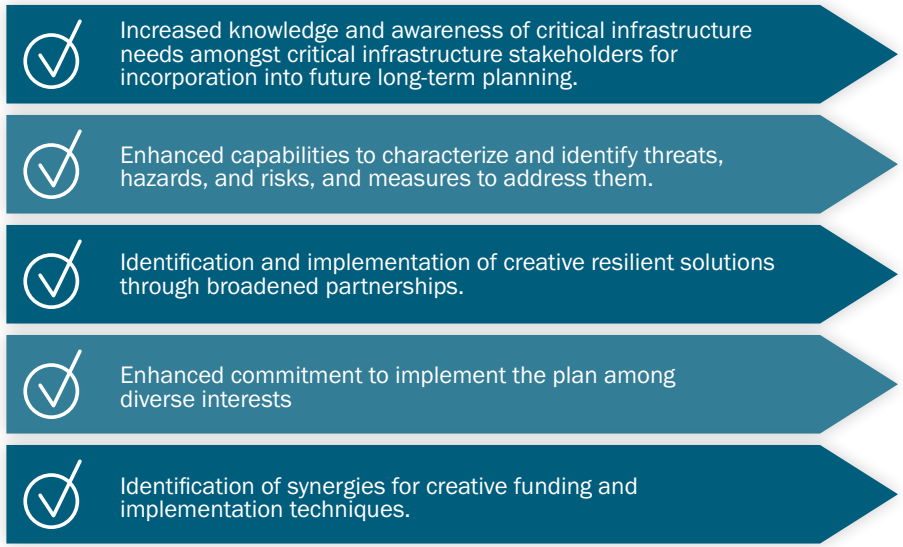


Figure 1. Results of Effective Collaboration

Table 4. Potential Planning Group Participants[2]

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

2 Adapted from the NIST Community Resilience Planning Guide

Engagement should include representatives from service providers, including energy, communications, transportation, and water and wastewater, as well as representatives from the wider community who can provide input about critical infrastructure considered essential to the regular functioning of the community.

Federal, state, tribal, and territorial 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 also 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.

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:

- Local businesses and industry representatives
- 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.)
- Interested citizens of the community

The planning team lead can develop a mailing/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 input/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.

THERE'S A RESOURCE FOR THAT!

Planning Participant Contact Information Sheet

This spreadsheet provides planning officials with a place to keep track of contact information for various stakeholders (including points of contact, phone numbers, email addresses, etc). These stakeholders are sorted by agency/sector type.

View resource in the Infrastructure Resilience Planning Resources.

1.4.2 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 number of 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.

THERE'S A RESOURCE FOR THAT!

Stakeholder Invitation Letter

This sample letter provides the project champion and/or planning team lead with example content for use in inviting and encouraging participation in the planning process. All or portions of the sample content can be used as it best applies to the various types of stakeholders being invited.

View resource in the Infrastructure Resilience Planning Resources.

1.5 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 suggested 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.

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 IRPF.

DEFINITION OF GOALS & OBJECTIVES

Goals are broad statements that describe a desired end state, what the community seeks to achieve through implementing resilience solutions for critical infrastructure.

Objectives are specific, measurable statements that support the achievement of a goal.

THERE'S A RESOURCE FOR THAT!

Sample Goals and Objectives

This list template provides example goals that could guide infrastructure resilience discussions.

View resource in the Infrastructure Resilience Planning Resources.

2. Critical Infrastructure Identification

This section addresses the following:

2.1 IDENTIFY INFRASTRUCTURE

2.2 PRIORITIZE INFRASTRUCTURE

2.3 IDENTIFY DEPENDENCIES

2. Critical Infrastructure Identification

Step 2 includes the identification and prioritization of critical infrastructure in the community and the interdependencies among the infrastructure systems.

2.1 IDENTIFY INFRASTRUCTURE

During planning, 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 a number of social functions that contribute to a prospering community, including: Community Service, Economy, Education, Family, Government, Health, Media, and 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

- 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.)
- Critical infrastructure assets, systems, or networks located within the community that may not provide direct services to the community per se, 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.

THERE'S A RESOURCE FOR THAT!

Infrastructure Assets Matrix: Suggested Data Fields Guide

This Guide provides suggested data fields to include in the database/matrix as well as descriptions and key considerations for collecting information about infrastructure assets.

Completing all suggested data fields will help facilitate Federally-supported analyses that the community might wish to undertake in the future. However, the data fields may be modified to best suit the information collection needs of participants/stakeholders and the community.

View resource in the Infrastructure Resilience Planning Resource.

Datasets for Infrastructure Identification

This document provides various datasets to explore sorted by category (Communication, Energy, Transportation, Water, Other, Hazards).

View resource in the Infrastructure Resilience Planning Resource.

2.1.1 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.

2.2 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 suggested 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. Table 5 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 Table 5 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.

Table 5. Key Considerations for Prioritizing Infrastructure Systems/Assets

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

2.3 IDENTIFY DEPENDENCIES AMONG INFRASTRUCTURE SYSTEMS

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 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.

3 2013 Plan

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, Risk and Infrastructure Science Center, Global Security Sciences Division. "Analysis of Critical Infrastructure Dependencies and Interdependencies, June 2015. ANL/GSS-15/4"

Table 6 provides examples of dependencies that are common among critical infrastructure systems.

Table 6. Examples of Typical Dependencies

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

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 resources to help account for this.

View resources in the Infrastructure Resilience Planning Resources.

THERE'S A RESOURCE FOR THAT!

Infrastructure Dependency Primer

This primer is a web-based, informative resource that provides a foundation for understanding critical infrastructure, identifying dependencies and their impact on communities' risk, and incorporating that knowledge into planning for resilience.

The online primer is publicly accessible at https://www.cisa.gov/idp.

View resource in the Infrastructure Resilience Planning Resources.

Dependency Identification Worksheet

The Dependency Identification Worksheet can assist in documenting the dependencies of the community's infrastructure on other identified critical infrastructure.

The Dependency Identification Worksheet walks communities through a series of questions about an infrastructure asset's dependencies focusing on energy (including electricity and natural gas), communications services, access to key transportation systems, and water and wastewater. Additional questions in the Dependency Identification Worksheet include cyber considerations, such as the data processing systems and services, and consideration of critical products required for functionality/operations, such as chemicals, fuels, raw materials, and removal of byproducts and waste.

View resource in the Infrastructure Resilience Planning Resources.

Community Systems Dependency Discussion Guide

This guide can be used to facilitate a dependency discussion with the planning team, other participants, or stakeholder groups. The guide includes a list of questions to spark conversation and lead to identification of critical community function and/or facility dependencies on infrastructure systems.

View resource in the Infrastructure Resilience Planning Resources.

THERE'S A RESOURCE FOR THAT!

System Owner/Operator Dependency Interview Guide

This guide contains a series of questions that can be used to conduct individual interviews with owners and/or operators of critical infrastructure systems. The questions will help identify and understand the system's dependencies and capabilities to provide service during a disruptive event.

View resource in the Infrastructure Resilience Planning Resources.

Meeting Facilitation Guide

This guide can be used to facilitate a meeting with planning participants to identify community functions, facilities, infrastructure systems, and interdependencies that are most critical to the resilience of the community.

View resource in the Infrastructure Resilience Planning Resources.

3. Risk Assessment

This section addresses the following:

3.1 IDENTIFY THREATS AND HAZARDS

3.2 ASSESS VULNERABILITY

3.3 ASSESS CONSEQUENCES

3.4 INFRASTRUCTURE SYSTEM RISKS

3. Risk Assessment

The Risk Assessment step 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 the assessment is utilized to support planning activities and resource allocation.

The Risk Assessment Methodology utilized for the IRPF entails:

1) identifying the threats and hazards to infrastructure,

2) assessing vulnerabilities of prioritized infrastructure,

3) assessing consequences and interactions among infrastructure systems, and

4) 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 or hazard, an entity impacted by that threat or hazard, and associated conditions including vulnerabilities and consequences.

UNDERSTANDING RISK*

Risk in the homeland security context is defined as 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. Resilience is part of the risk equation in that it can influence an entity's vulnerability (or exposure) to different threats and hazards, as well as the consequences that might arise from an event. Ultimately, the process of analyzing risk is important because it shapes decision making on ways to manage risk by accepting, avoiding, transferring, or controlling it to an acceptable level at an acceptable cost. Thus, resilience is fundamentally part of a community's broader risk management strategy.[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 (or impact): The effect of an incident, event, or occurrence, whether direct or indirect.

**National Infrastructure Protection Plan*

6 Methodology for Assessing Regional Infrastructure Resilience, CISA, 2021, pg. 15 https://www.cisa.gov/sites/default/files/publications/DIS_DHS_Methodology_Report_ISD%20EAD%20Signed_with%20alt-text_0.pdf

3.1 IDENTIFY THREATS AND HAZARDS TO INFRASTRUCTURE

There are myriad threats and hazards to which infrastructure systems/assets may be exposed. Table 7 identifies potential natural, deliberate, and accidental threats and hazards that should be considered for current and future applicability to priority critical infrastructure.

Table 7. Example Threats & Hazards by Category

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		

**Accidental hazards can be standalone incidents or may be the result of a Deliberate threat or Natural hazard event.*

While all hazards and threats can be considered, communities may want to evaluate the likelihood that each one will occur in order 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.

PLEASE NOTE

It is important to recognize that threat/hazard exposure will change over time, and the type, frequency, or magnitude of impacts may vary from past 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.

3.1.1 Sources of Threat & 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)
- 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

THERE'S A RESOURCE FOR THAT!

Hazard Information and Analysis Resources

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.

View resource in the Infrastructure Resilience Planning Resources.

Drought and Infrastructure: A Planning Guide

Developed by CISA with the National Drought Resilience Partnership, this guide provides an overview of the drought hazard, examples of direct and indirect impacts it can have on infrastructure systems, and identifies federal resources for assessing and mitigating drought risk.

View resource in the Infrastructure Resilience Planning Resources.

3.1.2 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
  - Adware
  - Bot
  - Ransomware
  - Rootkit
  - Spyware
  - Trojan Horse
  - Virus
  - Worm
- Distributed Denial of Service (DDoS) & Denial of Service (DoS)

3.2 ASSESS VULNERABILITY OF INFRASTRUCTURE

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 help in the development of actions for enhancing security and resilience. Key elements of vulnerability to consider during the assessment are:

- **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 taking into account 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 or not an asset represents a single point of failure within its overall system.

3.3 ASSESS CONSEQUENCES TO INFRASTRUCTURE SYSTEMS

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:

1. **Human** (injury, illness, or loss of life)
2. **Economic** (costs associated with loss of infrastructure business continuity, and replacement costs)
3. **Mission** (ability of an organization or group to meet a strategic objective or perform a function)
4. **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.

3.4 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.

THERE'S A RESOURCE FOR THAT!

Risk Assessment Methodologies

This resource summarizes various risk analysis methods and provides links to external resources for conducting risk analysis.

View resource in the Infrastructure Resilience Planning Resources.

4. Develop Actions

This section addresses the following:

4.1 REFINE GOALS AND OBJECTIVES

4.2 IDENTIFY RESILIENCE SOLUTIONS

4.3 ASSESS EXISTING RESOURCES AND CAPABILITIES

4.4 SELECT RESILIENCE SOLUTIONS

4.5 DEVELOP IMPLEMENTATION STRATEGIES

4. Develop Actions

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

4.1 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.

4.2 IDENTIFY RESILIENCE SOLUTIONS TO MITIGATE RISKS

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.

- **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.

THERE'S A RESOURCE FOR THAT!

Sources for Resilient Solutions

A list of sources for resilient solution ideas is provided in **Infrastructure Resilience Planning Resources**.

FEMA MITIGATION ACTION RESOURCES

Potential mitigation activities are highlighted in the following FEMA resources (located under Resources for Mitigation Activities).

- **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.
- **Hazard Mitigation 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.

4.2.1 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.

CYBERSECURITY RESOURCES

- **CISA** is responsible for enhancing the security, resiliency, and reliability of the nation's cyber and communications infrastructure. Information about CISA's cybersecurity training and education, publications and guidance, alerts and newsletters, technical assistance, and programs and services is included at this link.
- **CISA's cybersecurity assessments** provide a range of products and technical services. Free, voluntary assessments can be requested by partners and range from self-administered surveys to on-site visits.
- **CISA develops and provides a range of information sharing and awareness products**, ranging from threat indicator information to bulletins and advisories. CISA also sponsors sector-based Information Sharing and Analysis Centers as well as Information Sharing and Analysis Organizations to promote the sharing of cyber information and best practices. Additional information can be found at this link.
- **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.
- **The CISA Critical Infrastructure Cyber Community Voluntary Program** helps critical infrastructure owners and operators align with existing resources to assist them in using the Cybersecurity Framework and managing their cyber risks and provides sector-specific guidance and practices.

4.3 IDENTIFY 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 2 illustrates some of the most common types of existing resources and capabilities that should be considered when prioritizing identification solutions.

Planning & Regulatory authorities	A community is often legally required to abide by or enforce these to ensure public safety, environmental standards, etc. E.g., ordinances, codes, etc.
Existing Plans, Policies & Programs	Can be used as vehicles to incorporate new resilience solutions and expedite implementation as long as there is consistency and alignment with the goals and objectives or the plans, policies, and programs. E.g., comprehensive plans, capital improvement plans
Administrative & Technical Skills within the Community	Knowing existing capabilities within the community helps to identify if and what additional skills or expertise is required for the implementation or resilience solutions.
Financial Resources	Knowing the available financial capabilities and resources that exist to steer and prioritize planning efforts to identify what potential external funding will be required for implementation of resilience solutions. E.g., grants, impact fees, etc.

Figure 2. Common Types of Community Capabilities

THERE'S A RESOURCE FOR THAT!

Sample Capability Assessment Worksheet

A sample capabilities worksheet is provided to assist the community in assessing its existing resources and capabilities. The sample capabilities worksheet can be revised as the community sees fit to suit its needs.

This worksheet asks the planning group 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 group 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.

View resource in the Infrastructure Resilience Planning Resources.

4.4 SELECT RESILIENCE SOLUTIONS FOR IMPLEMENTATION

After producing a list of resilience solutions and identifying capacity, a community should focus their efforts on identifying which public and private entities will need to take action 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.)
- Funding limitations, including operations and maintenance
- Partnership opportunities
- Relevant political priorities
- Community concerns
- Economic impacts

Other evaluation criteria is described in FEMA's Local Hazard Mitigation Planning Handbook. Whatever evaluation criteria are used, they should be agreed upon by planning participants/stakeholders.

THERE'S A RESOURCE FOR THAT!

Mitigation Alternatives Evaluation Questions

This set of questions can be used to support facilitated discussions and qualitatively analyze alternatives for enhancing resilience.

View resource in Infrastructure Resilience Planning Resources.

Economic Evaluation of Solutions

NIST has developed the Economic Decision Guide Software (EDGe$) to help communities evaluate the economic impact (costs and benefits) of resilience investments.

View resource in the Infrastructure Resilience Planning Resources.

Benefit-Cost Analysis (BCA) Toolkit

FEMA has a Benefit-Cost Analysis (BCA) Toolkit that can be used to determine the cost-effectiveness of a mitigation project by weighing the risk reduction benefits of the project against the overall project cost.

The toolkit is available for download at:
fema.gov/grants/guidance-tools/benefit-cost-analysis

CRITERIA FOR EVALUATING SOLUTIONS

FEMA's Local Hazard Mitigation Planning Handbook, March 2013 suggests the following evaluation criteria when analyzing potential solutions:

- **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?

4.5 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.

THERE'S A RESOURCE FOR THAT!

Resilient Solution Strategy Worksheet

The Resilience Solution Strategy Worksheet is a sample worksheet that communities can use to fill out implementation strategy elements for each resilience solution.

View resource in the Infrastructure Resilience Planning Resources.

5. Implement & Evaluate

This section addresses the following:

5.1 IMPLEMENT THROUGH EXISTING PLANNING MECHANISMS

5.2 MONITOR AND EVALUATE EFFECTIVENESS

5.3 UPDATE PLANS

5. Implement & Evaluate

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.

THERE'S A RESOURCE FOR THAT!

IRPF Plan Integration

This document provides an overview of possible integrations with other community planning efforts/processes.

View resource in the Infrastructure Resilience Planning Resources.

5.1 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:

- 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

5.1.1 Potential Funding and Technical Assistance Sources for Implementation

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.

Various departments and agencies at the Federal and SLTT 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.

5.2 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.

THERE'S A RESOURCE FOR THAT!

Compendium of Programs and Mechanisms for Funding Infrastructure Resilience

The Compendium of Programs and Mechanisms for Funding Infrastructure Resilience provides a list of potential funding and technical assistance sources with links.

View resource in the Infrastructure Resilience Planning Resources.

In addition to this compendium, the FEMA Hazard Mitigation Assistance Grants page provides additional detail and information about FEMA grants.

KEY CONSIDERATIONS FOR EVALUATING PLANS

- 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?

5.2.1 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?

5.3 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

- 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.

All Resources

This section includes resources for:

OVERVIEW

STEP 1: LAY THE FOUNDATION

STEP 2: CRITICAL INFRASTRUCTURE IDENTIFICATION

STEP 3: RISK ASSESSMENT

STEP 4: DEVELOP ACTIONS

STEP 5: IMPLEMENT & EVALUATE

Overview

ALIGNMENT OF IRPF TO FEDERAL PLANNING AND RISK MANAGEMENT PROCESSES

Format: Matrix

Type: PDF

Pages: 2

Summary: This matrix illustrates how the Infrastructure Resilience Planning Framework is in alignment with and complimentary to the various other existing federal risk and/or resilience planning processes and guidelines.

[VIEW PDF]

METHODOLOGY FOR ASSESSING REGIONAL INFRASTRUCTURE RESILIENCE

Format: Document

Type: PDF

Pages: 118

Summary: Based on lessons learned from CISA's Regional Resiliency Assessment Program, this assessment methodology provides a common process for assessing and addressing complex infrastructure resilience issues validated through a decade of RRAP project experience.

[VIEW PDF]

Step 1. Lay the Foundation

DATA COLLECTION SAMPLE LIST OF RESOURCES

Format: Table

Type: PDF document with embedded tables

Pages: 2

Summary: Provides general overview of potential reference resources, sorted by resource owners/creators. Creators include: Local/County/Regional Agencies, Critical Infrastructure Owner/Operator, State Agencies, Federal Agencies. List assists planners in the process of employing the IRPF to identify all previous relevant efforts.

[VIEW PDF]

COMPARISON OF EXISTING COMMUNITY PLANS

Format: Guidebook

Type: Online PDF

Pages: 142

Summary: The Plan Integration for Resilience Scorecard is a plan evaluation method developed by DHS Science and Technology through its Coastal Resilience Center of Excellence partner at Texas A&M University. The scorecard can help communities evaluate and coordinate their various plans (e.g., transportation, economic development, hazard mitigation, emergency management, etc.) so that they present consistent strategies and work together to reduce vulnerabilities to hazards.

[RESOURCE LINK]

PLANNING PARTICIPANT CONTACT INFORMATION SHEET

Format: Template (data sheet)

Type: PDF document

Pages: 2

Summary: This spreadsheet provides planning officials with a place to keep track of contact information for various planning group participants (including points of contact, phone numbers, email addresses, etc). These stakeholders are sorted by agency/sector type.

[VIEW PDF]

STAKEHOLDER INVITATION LETTER

Format: Template (letter)

Type: PDF document

Pages: 1

Summary: This sample letter provides the project champion and/or planning team lead with example content for use in inviting and encouraging participation in the planning process. All or portions of the sample content can be used as it best applies to the various types of stakeholders being invited.

[VIEW PDF]

SAMPLE GOALS AND OBJECTIVES

Format: Template (list)

Type: PDF document

Pages: 2

Summary: This template lists more goals that could guide infrastructure resilience discussions.

[VIEW PDF]

Step 2. Critical Infrastructure Identification

INFRASTRUCTURE ASSETS MATRIX: SUGGESTED DATA FIELDS

Format: Table

Type: PDF document with embedded table

Pages: 3

Summary: This table identifies key data collection suggestions for critical infrastructure asset assessment. Data fields include relevant contact information, owner names, latitude/longitude, type, status, and more.

[VIEW PDF]

INFRASTRUCTURE DEPENDENCY PRIMER

Format: Website

Type: Online Website

Pages: -

Summary: The Infrastructure Dependency Primer is an online, educational supplement to the IRPF and aims to answer fundamental questions planners and decision-makers may have, including:

- *What are infrastructure dependencies and why should I care?*
- *What is resilience, how does it relate to dependencies, and how do I plan for it?*
- *What resources are there to help me reduce dependency risks and enhance the resilience of my community?*

This web-based resource is publicly accessible to be independently explored by users based on their interests and needs. No prerequisite training or knowledge is needed to benefit from content.

[RESOURCE LINK]

DATASETS FOR INFRASTRUCTURE IDENTIFICATION

Format: Document

Type: PDF document

Pages: 7

Summary: This resource is centered around the Homeland Infrastructure Foundation Level Data (HIFLD). The document provides various datasets to explore sorted by category (Communication, Energy, Transportation, Water, Other, Hazards).

[VIEW PDF]

DEPENDENCY IDENTIFICATION WORKSHEET

Format: Worksheet

Type: Fillable PDF form

Pages: 7

Summary: This worksheet asks planning participants to identify the following potential dependencies for each infrastructure asset: energy, natural gas, communications, transportation, water, wastewater, cyber, and critical products.

[VIEW PDF]

COMMUNITY SYSTEMS DEPENDENCY DISCUSSION GUIDE

Format: Guide

Type: PDF document

Pages: 2

Summary: This guide can be used to facilitate a dependency discussion with the planning team, other participants, or stakeholder groups. The guide includes a list of questions to spark conversation and lead to identification of critical community function and/or facility dependencies on infrastructure systems.

[VIEW PDF]

SYSTEM OWNER/ OPERATOR DEPENDENCY INTERVIEW GUIDE

Format: Guide

Type: PDF document

Pages: 1

Summary: This guide contains a series of questions that can be used to conduct individual interviews with owners and/or operators of critical infrastructure systems. The questions will help identify and understand the system's dependencies and capabilities to provide service during a disruptive event.

[VIEW PDF]

MEETING FACILITATION GUIDE

Format: Guide

Type: PDF document

Pages: 2

Summary: This guide can be used to facilitate a meeting with planning participants to identify community functions, facilities, infrastructure systems, and interdependencies that are most critical to the resilience of the community.

[VIEW PDF]

Step 3. Risk Assessment

HAZARD INFORMATION AND ANALYSIS RESOURCES

Format: Table with external links

Type: PDF 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.

[VIEW PDF]

DROUGHT AND INFRASTRUCTURE: A PLANNING GUIDE

Format: Guide

Type: PDF document

Pages: 10

Summary: Developed by CISA with the National Drought Resilience Partnership, this guide provides an overview of the drought hazard, examples of direct and indirect impacts it can have on infrastructure systems, and identifies federal resources for assessing and mitigating drought risk.

[VIEW PDF]

RISK ASSESSMENT METHODOLOGIES

Format: Guide

Type: PDF document with images and external links

Pages: 6

Summary: Summarizes the NIST CRPG risk analysis process. Provides links to external resources for conducting risk analysis, including:

- Seismic Hazards
- Sea Level Rise and Coastal Flooding
- Floods
- Landslides
- What-If Hazard Analysis
- Sector-Specific Plans (SSPs) Analysis
- Infrastructure Survey Tool (IST)
- Integrated Rapid Visual Screening (IRVS)
- FEMA's HAZUS-MH
- Methodology for Assessing Regional Infrastructure Resilience

[VIEW PDF]

Step 4. Develop Actions

SOURCES FOR RESILIENT SOLUTIONS

Format: Table with external links

Type: PDF 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.

[VIEW PDF]

SAMPLE CAPABILITY ASSESSMENT WORKSHEET

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.

[VIEW PDF]

MITIGATION ALTERNATIVES EVALUATION GUIDE

Format: Guide

Type: PDF document

Pages: 1

Summary: Questions that can be used to support facilitated discussions and qualitatively analyze alternatives for enhancing resilience.

[VIEW PDF]

NIST ECONOMIC DECISION GUIDE SOFTWARE (EDGE$)

Format: Software

Type: Online software

Pages: -

Summary: NIST has created the Economic Decision Guide Software (EDGe$) to help evaluate the economic impact of investments. The resource helps to identify and compare the relevant present and future resilience costs and benefits associated with new capital investment. EDGe$ can be found at **edges.nist.gov**

[RESOURCE LINK]

RESILIENT SOLUTION STRATEGY WORKSHEET

Format: Worksheet

Type: Fillable PDF form

Pages: 3

Summary: This sample worksheet can be used by communities to fill out implementation strategy elements for each identified resilience solution.

[VIEW PDF]

Step 5. Implement & Evaluate

PLAN INTEGRATION

Format: Table

Type: PDF document with embedded table

Pages: 3

Summary: Provides an overview of possible integrations with other community planning efforts/processes. General suggestions.

[VIEW PDF]

COMPENDIUM OF PROGRAMS AND MECHANISMS FOR FUNDING INFRASTRUCTURE RESILIENCE

Format: Guide

Type: PDF document

Pages: 40

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.

[VIEW PDF]

Glossary

This section includes the following:

KEY TERMS

ABBREVIATIONS & ACRONYMS

CRITICAL INFRASTRUCTURE SECTORS

Key Terms

TERM	DEFINITION
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.

TERM	DEFINITION
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 & Acronyms

ACRONYM	DEFINITION
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

ACRONYM	DEFINITION
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
SRMA	Sector Risk Management 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 Sectors

SECTOR	SECTOR RISK MANAGEMENT AGENCY (SRMA)
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

Infrastructure Resilience Planning Framework (IRPF)

November 2022 | Version 1.1

Infrastructure Development and Recovery Program - IDR@cisa.dhs.gov