Pacific Northwest
NATIONAL LABORATORY

PNNL-30208

Hawaii Critical Infrastructure Interdependency Analysis Guide

January 2020

Kim M. Fowler
Janelle Downs
Delphine Appriou
Andrew Costinett

U.S. DEPARTMENT OF ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
email: orders@ntis.gov <https://www.ntis.gov/about>
Online ordering: http://www.ntis.gov

Acknowledgments

The Pacific Northwest National Laboratory (PNNL) was contracted by the United States Indo-Pacific Command (INDOPACOM) to support the Interdependencies of Critical Energy Infrastructure (ICE-I) Working Group on the implementation of the Critical Energy Infrastructure Interdependencies (CEII) Memorandum of Understanding (MOU). Jimmie Collins was the lead for the INDOPACOM contract and facilitates the ICE-I Working Group. The PNNL team would like to thank Ms. Collins for her insightful guidance of the PNNL activities and her excellent and unwavering leadership role on the ICE-I Working Group. Her passion for the resilience and security of the State of Hawaii is unquestionable and an inspiration.

PNNL would also like to acknowledge the tremendous efforts of the ICE-I Working Group members. This team has been dedicated to bettering the State of Hawaii's energy resilience and security position for years and will continue to push to make a state safe for all its citizens, even in times of stress.

- Dee Cook for her priceless ability to make relevant connections between people and organizations across the state, and her tireless efforts to identify funding sources for the resilience and security solutions. (Hawaii State Department of Defense Office of Homeland Security, Administrator)

- James Cruz for his dedication to bringing as many US Department of Homeland Security (DHS) resources as possible to the resilience and security challenges of Hawaii, and his infectious positive attitude. (DHS CISA Region IX, Physical Security Advisor)

- Mark Want, Chris Yunker and Kym Sparlin for consistently bringing forward creative ideas, their steadfast commitment to solving Hawaii's energy resilience and security challenges, and their willingness to bring the full support of their office and state connections to this cause. (Hawaii State Energy Office)

- Carolyn Gay for her dependably attentive, remote participation and bringing the US Department of Energy's (DOE) Headquarters perspective to the Working Group. (US Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response [CESER])

The PNNL team was honored to be a part of this team and looks forward to learning about the amazing things this Working Group will accomplish for the great State of Hawaii.

Acronyms and Abbreviations

AOC	Area of concern
CI	Critical Infrastructure
CEII	Critical Energy Infrastructure Interdependencies
DHS	US Department of Homeland Security
DOE	US Department of Energy
EDA	Economic Development Administration
EUI	Energy Use Intensity
FEMA	Federal Emergency Management Administration
ICE-I	Interdependencies of Critical Energy Infrastructure
GIS	Geographic Information System
kW	kilowatt
kWh	kilowatt hour
MOU	Memorandum of Understanding
PNNL	Pacific Northwest National Laboratory
SOH	State of Hawaii
UPS	uninterruptible power supply
US	United States

Contents

Figures

Tables

Introduction

State of Hawaii (SOH) *Critical Infrastructure (CI) is defined as interdependent systems and assets (existing, proposed, physical or virtual), of which when compromised, incapacitated or destroyed would negatively affect security, economic security, public health or safety, or any combination thereof*. This guide provides a five-step process (Figure 1) to address the resilience of SOH's CI. The process can be used to inform stakeholder decision-making and reduce potential consequences of threats to Hawaii's CI. This process is dynamic, iterative and likely will not be linear. That is, the information gathered, and the analyses completed during a step may uncover new data or concerns that need to be considered relevant to a previous step.

Step 1: Identify Critical Infrastructure (CI) and CI Interdependencies/Dependencies

A. Set resilience goals
B. Identify & engage stakeholders
C. Prepare initial CI list
D. Identify infrastructure dependencies & interdependencies
E. Collect energy data

Step 2: Prioritize Identified CI

A. Develop tailored prioritization criteria
B. Evaluate each asset with prioritization criteria
C. "Finalize" the CI list
D. Refine data collected for priority CI

Step 3: Assess Vulnerabilities

A. Identify potential threats of concern
B. Determine threat geographic area of concern
C. Collect & analyze threat data for prioritized CI
D. Evaluate CI resilience to threat(s)
E. Identify CI resilience gaps

Step 4: Develop, Prioritize and Implement Mitigation Strategies

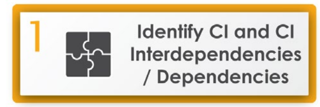
A. Identify mitigation strategies
B. Determine risk reduction
C. Prioritize mitigation strategies
D. Identify funding & implement mitigation strategies

Step 5: Evaluate and Re-assess

A. Assess progress toward resilience goals
B. Re-assess CI lists
C. Re-evaluate CI list prioritization
D. Update threat information
E. Re-prioritize mitigation strategies

Figure 1: Steps to Identify, Analyze, and Improve Resilience of Critical Infrastructure

Step 1: Develop List of Critical Infrastructure and Identify Dependencies and Interdependencies



A. Set resilience goals
B. Identify & engage stakeholders
C. Prepare initial CI list
D. Identify infrastructure dependencies & interdependencies
E. Collect energy data

Creating a Critical Infrastructure (CI) list requires interactions with many stakeholders and thus the process will not be linear, and the list will be dynamic. The following activities will be part of an iterative process that will result in a State of Hawaii (SOH) CI list that includes dependences and interdependencies. In other words, the list could be considered a “living document”.

A. Set Resilience Goals

Defining the resilience goals creates boundaries for the identification of CI. Draft goals can be identified by an executive group, such as the Interdependencies of Critical Energy Infrastructure (ICE-I) Working Group and then socialized and refined by the stakeholder community.

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

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

B. Identify & Engage Stakeholders

Stakeholders can help refine goals, define and prioritize the CI list, and identify CI dependencies and interdependencies. Some stakeholders will have the responsibility of maintaining CI in an emergency and thus will need to understand and agree to the resilience goals. The Department of Homeland Security (DHS) has identified “lifeline” sectors central to recovery and sustaining life following a threat. (DHS 2019) Those sectors include:

- Safety and Security
- Food, Water, Shelter
- Health and Medical
- Energy
- Communications
- Transportation
- Hazardous Material

Based on the draft resilience goals, the ICE-I Working Group can identify stakeholders that are CI owners, public and private partners with an interest in enhancing resilience, and potential funding sources. There may be a need for multiple, smaller stakeholder groups as different CI partners may view criticality differently based on their unique situations, operating models, and associated risks. Defining one or multiple stakeholder teams with specific goals will help create structure to the CI assessment efforts and will allow for engagement and coordination across the diverse set of stakeholders. In September 2018 the ICE-I identified the following potential stakeholders:

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

There will be many times throughout this process when stakeholders will need to be engaged, including:

- Resilience goal development and refinement
- CI list development and prioritization
- CI data collection
- Mitigation strategy development and implementation

C. Prepare Initial CI List

The CI list will likely change over time given the identification of dependencies and interdependencies and prioritization. An initial CI list is prepared to start the discussion with stakeholders. Each stakeholder will likely have their own formal (or informal) CI list. The initial list can be created reviewing an existing list of all CI against a set of criteria. Or if a list does not exist, a new CI list can be created based on the same criteria. The review criteria may need to be adapted based on the SOH resilience goals. When reviewing an infrastructure list, if the answer is "yes" to any of the following questions (adapted from DHS 2012), the asset could be considered CI:

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

- Would an incident at the asset result in an adverse environmental impact?
- Is the asset significant to the state's economic stability?
- Is the asset significant to the region's economic stability?
- Is the asset significant to the nation's economic stability?

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

D. Identify Infrastructure Dependencies & Interdependencies

The process of identifying the dependencies and interdependencies will likely increase the number of assets on the SOH CI list, and it will provide useful information for the CI prioritization efforts. For the purposes of CI, an asset is considered *dependent* if it is reliant on another asset or capability of that asset to function, and an asset is considered *interdependent* if it and another asset are mutually reliant on each other. Discussing the three primary types of asset failure with stakeholders will assist in the identification of CI and identify dependencies and interdependencies (Table 1). Stakeholder engagement, via a workshop or a series of meetings, is necessary to identify and assess dependencies and interdependencies for an asset's potential for cascading, escalating or common cause failures.

Table 1: Asset Failures that Identify Dependencies and Interdependencies (DHS 2012)

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

Figure 2 illustrates the concept of interdependencies using a gas station as an example. While the presence of an operating gas station is essential to ensure movement of emergency vehicles, fuel delivery relies on multiple

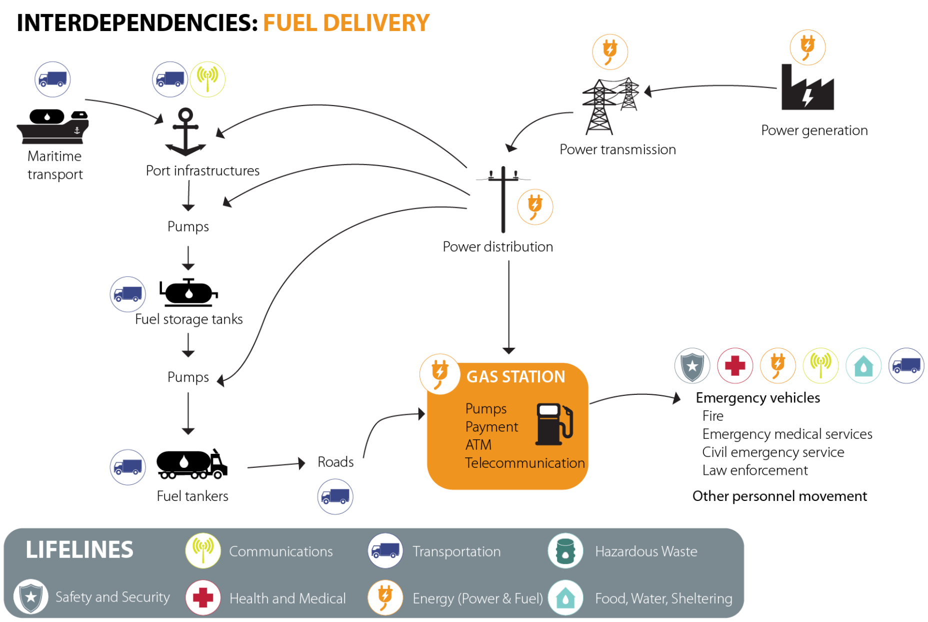


Figure 2: Dependencies and Interdependencies Example

upstream infrastructures (e.g., power transmission, transportation, etc.). Any operating failure of one of these infrastructures could lead to cascading effects.

Dependency and interdependency evaluations include examining:

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

E. Collect Energy Data

Data collection for each CI will likely take time to be completed. The first action is for the team to seek information from readily available or centralized sources. Appendix A lists the information needed to assess an asset's state of resilience. Examples of the types of data to be collected include:

- Data regarding the utilities supporting an asset's operations (e.g., electricity, gas, steam)
- Utility consumption and CI demand data (operating load estimates may be different than the critical emergency load)
- Existing backup systems and storage
- Maps and engineering drawings—this may include GIS layers for utility systems, one-line/single-line diagrams for electric service

As the information is compiled it will need to be analyzed and characterized to determine energy demand and load for baseline operating conditions and for emergency scenarios. For example, there is a need to determine if the energy demands during an emergency are intermittent or continuous. Long-term *stationary or fixed* solutions, such as a microgrid, may be more appropriate for assets requiring *continuous* energy. A data center or a hospital are examples of facilities with continuous demand. Facilities with *intermittent* energy demand potentially could be served by *mobile or deployable* solutions, such as a mobile generator and fuel tank. A facility that requires energy to operate, but only operates periodically throughout the day is an example of intermittent demand.

For facility or building assets, the simplest and most accurate approach to determining energy demand and load is to collect building-level interval meter data. When interval data are not available, various estimation techniques can be applied as described in Appendix C. The team should review options for estimating infrastructure utility demand with stakeholders to select the most appropriate approach given data and resource availability.

CI asset energy data are needed for three purposes:

- to establish the average daily and peak energy use,
- to establish load profiles that enable sizing and configuration of generation/production and storage solutions, and
- to identify energy savings opportunities associated with demand reduction measures, including efficiency retrofits and operational changes.

Step 2: Prioritize Critical Infrastructure

2 Prioritize Identified CI

A. Develop tailored prioritization criteria
B. Evaluate each asset with prioritization criteria
C. "Finalize" the CI list
D. Refine data collected for priority CI

A resilience assessment team needs to be formed consisting of stakeholders knowledgeable about CI in their sector and stakeholders with a clear understanding of the SOH's resilience goals. The resilience assessment team, with input from the broader stakeholder community, will prioritize the CI for maintaining safety and security and ensuring recovery, and to address the SOH resilience goals.

This step outlines the types of criteria and considerations that can be applied to prioritize CI assets. The prioritization process examines the impacts of loss of operation/function of each CI asset as well as evaluating the potential risks to the asset. The assessment team will likely need to iterate between Steps 1, 2 and Step 3 to complete the prioritization process.

> **Prioritizing CI**
> "Critical infrastructure and protective measures should be prioritized based on risk to ensure that resources are applied where they contribute most to the mitigation of risk. Systematic methods of prioritizing assets, systems, and networks – as well as protective actions – offer transparency and increase the defensibility of resource allocation decisions, whether they involve Federal or State funds." (DHS 2008)

A. Develop Tailored Prioritization Criteria

One starting point for prioritization criteria is the list of questions used to identify the SOH CI list. In addition to those questions, whether an asset has dependencies or interdependencies, and whether an asset has the potential of a cascading, escalating or common-cause failure (Table 2). Additional criteria specific to the SOH resilience goals can be added to further tailor the prioritization effort. For example, a criterion could be specifically focused on the availability of diabetes services within each community that could become isolated during a natural disaster.

Table 2: Example Prioritization Criteria

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

18	Is there potential for a cascading failure?
19	Is there potential for an escalating failure?
20	Is there potential for a common-cause failure?

One method for scoring each asset against the prioritization criteria is to give it a score between 0-5 and sum the total score. The 0-5 scale would represent:

- 0 = not applicable
- 1 = low impact
- 2 = medium-low impact
- 3 = medium impact
- 4 = medium-high impact
- 5 = high impact

B. Evaluate each asset with prioritization criteria

Scoring each of the assets will be somewhat subjective. There are multiple ways this can be managed including having each member of the resilience assessment team score the assets on the CI list and then meeting to reconcile the major differences. An example of assets scored against the criteria in Table 2 is shown in Table 3.

Table 3: Example of Prioritized Assets

	Prioritization Criteria																				
Asset Name	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**Score**
Hawaiian Electric Company	3	3	5	5	3	5	5	5	5	5	5	3	5	3	3	5	5	5	5	5	88
Queen's Medical Center	5	5	2	5	0	0	0	0	5	5	5	1	1	0	0	5	1	2	2	1	45
Hawaiian Telecom Switching Facility	2	1	3	4	4	1	2	4	5	5	5	0	5	5	3	5	5	5	5	5	74

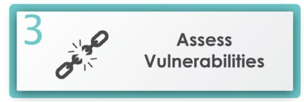
C. "Finalize" the CI list

Once the resilience assessment team has developed a prioritized CI list, it will share those results with the broader group of stakeholders to review and address recommended changes as needed. Categorizing the prioritized CI into groupings from highest priority to lower priorities can help with the validation of the prioritized list. For example, the prioritized list could be parsed into the top 10%, top 25%, bottom 10%, and then provide that information for a separate prioritization of assets by owners/stakeholders. Agreeing to the highest priority assets will help focus the near-term efforts toward addressing the SOH resilience goals. Sharing how a stakeholder's assets ranked will offer them an opportunity to see if their assets are similarly prioritized by the SOH as they are within their own organization.

D. Refine Data Collected for Priority CI

Once the CI have been prioritized, additional effort needs to focus on collecting key utility data for the highest priority assets. The data needs are the those outlined in Appendix A. If no energy consumption data are available, techniques to estimate energy consumption can be found in Appendix C. (PNNL 2019)

Step 3: Evaluate Vulnerabilities, Threats, and Associated Risk



A. Identify potential threats of concern
B. Determine threat geographic area of concern
C. Collect & analyze threat data for prioritized CI
D. Evaluate CI resilience to threat(s)
E. Identify CI resilience gaps

Step 3 focuses on identifying and assessing potential natural hazards, but the general process may also be followed for pandemic, physical, and cyber threats. Assessing the risk to CI and prioritizing response and recovery actions requires understanding the probability of the hazard, the vulnerability of the asset or system, and determining the potential impacts to operation (Figure 3). There are experts in the region that can perform the natural hazards analysis for CI, thus this step is only outlined here. Expert analysis of the threats and risks associated with pandemic, physical, and cyber threats is also a best practice. If resources are not available for external analysis, the resilience assessment team and stakeholders can use publicly available resources to qualitatively assess the risk for the prioritized CI. Geospatial analysts will help identify which CI could be affected by different threats. The CI List tool in Appendix A can be used to document the findings. The SOH and stakeholders can use the threat and risk analysis to align policies and procedures and identify mitigation strategies.

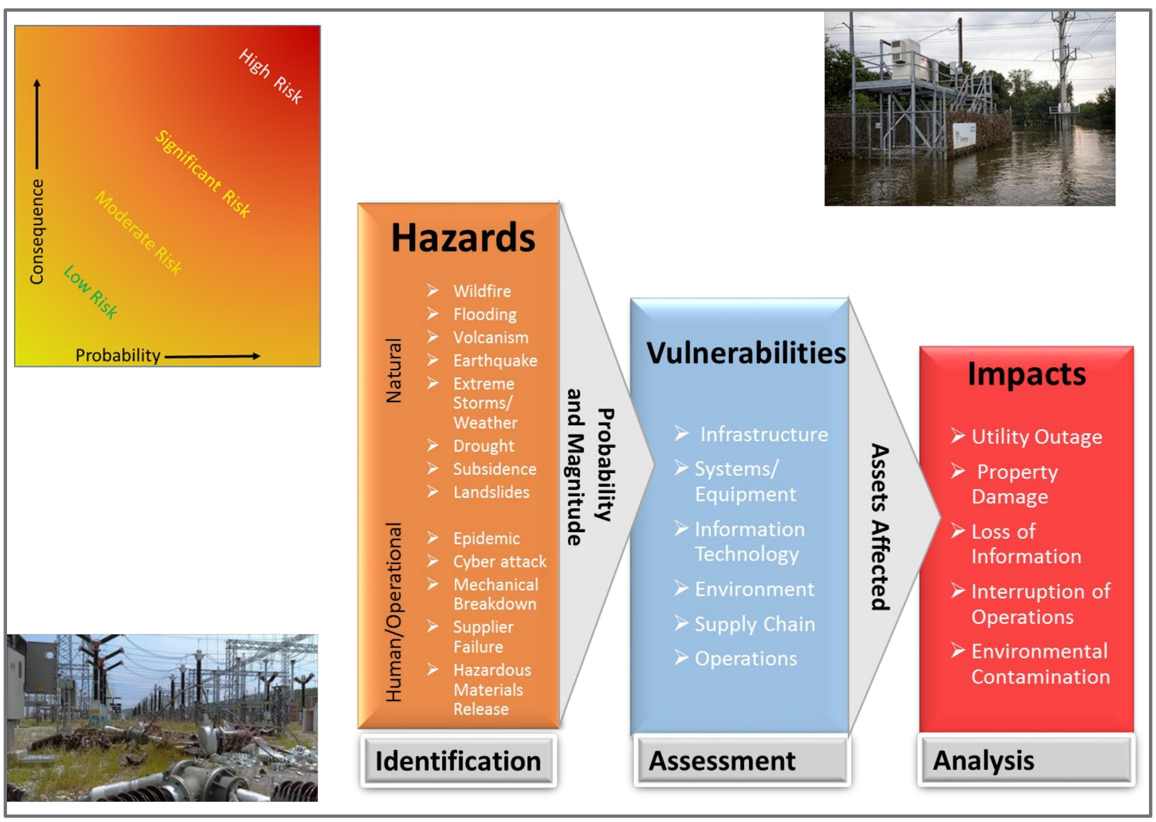


Figure 3: Hazard Assessment Process

A. Identify Potential Threats of Concern

When determining vulnerability, the first action is to identify the potential site-specific or regional hazards, or threats, that pose a risk to CI. These risks can be *human* or *natural*. Human risks include physical threats such as a cyber-attack, or a "bad actor" targeting an asset. The human risks are highly unpredictable as to what might be the target and when the event may occur. Currently, most natural hazards offer pre-event warnings regarding generally when and where they might occur. Potential natural hazards that pose a risk to CI in the SOH include drought, earthquake, tsunami, extreme storms/weather, flooding, hurricane, landslide, pandemic, subsidence, wildfire, and volcanism. For human and natural threats, the preparation for, and the government response to the event(s) can impact the speed of recovery. The remainder of this section focuses on preparation and response to natural threats.

B. Determine Threat Geographic Area of Concern

To identify the geographic area of concern, the resilience assessment team will need to consider the floodplains, storm path projections, earthquake zone, plume models, and other threat-specific information as appropriate. To determine the likelihood of individual hazards, hazard assessments draw on historical information and models anticipating the future to assess the likelihood or frequency of various hazards and the location of potential impacts. Data and information on hazards are available from many federal and state agencies (see Appendix B) including:

- Federal Emergency Management Agency (FEMA) for floodplain data
- U.S. Coast Guard for maritime data
- National Oceanic and Atmospheric Administration (NOAA) for hurricane tracking and storm surge data
- U.S. Geological Survey (USGS) for earthquake magnitude and extent
- National Cybersecurity and Communications Integration Center (NCICC) for cyber-related incidents
- Centers for Disease Control and Prevention (CDC) and DHS for pandemics
- DHS Intelligence and Analysis (I&A) for terrorist related events

C. Collect & Analyze Threat Data for Prioritized CI

Collecting and mapping the available threat data for the prioritized CI is a key step in understanding the risks to the SOH. Figure 4 provides an example, prepared by a geospatial analyst, of how CI and hazards mapping can be used to inform decision makers. The health facilities identified by green dots have indicated they have sufficient back-up power generation to function during an emergency. The storm surge model shows whether the health facilities are likely to be impacted by flooding during a category 4 hurricane. Images like this coupled with energy data will help identify where the greatest risks are and whether those can be mitigated on-site or if alternative plans are needed to address the medical needs of the local community.

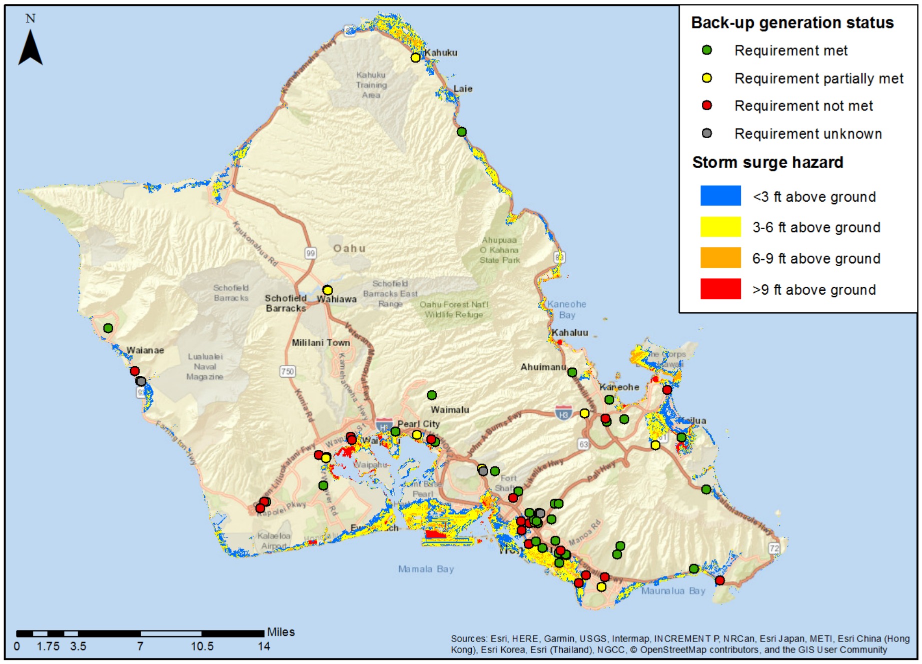


Figure 4: Example CI Map of the Category-4 Hurricane Flooding Modeled Impact on Health Facilities

Once the threats to CI are known, additional CI vulnerabilities can be considered. For example, if the roads are likely to be damaged during a hurricane, does the CI asset have a sufficient supply of needed materials and fuel for generators, or is there a plan for resupply that does not involve ground transportation. When evaluating CI vulnerabilities to specific threats consider the impacts on the following:

- Infrastructure Condition/Configuration
- Systems/Equipment
- Information Technology
- Environmental
- Supply Chain/Fuel Storage
- Operations

When considering the potential impacts of natural hazards and physical/cyber threats, Table 4 summarizes the actions to take, the data needed, and the analysis approaches necessary to evaluate each hazard.

Table 4: Actions, Data, and Analysis Approach Required to Evaluate CI with Respect to Threats

Actions	Data and Analysis Approach
Determine hazard extent and buffers	✓ Area and location of anticipated impact ✓ Buffering distances to cover uncertainties
Identify the geographic area of concern (AOC)	✓ Floodplain ✓ Storm path ✓ Earthquake zone ✓ Tsunami inundation zone ✓ Plume model (nuclear/chemical) ✓ Credible threat ✓ Other defined area

Delineate the geographic AOC	✓ GIS-based approach—offers greater precision, conducted through geospatial analysis techniques on geospatial software (e.g., ArcGIS) ✓ Non-GIS approach—lower precision, conducted by selecting sectors of concern from the AOC (e.g., using metropolitan statistical area, county, city, zip code, etc.)
Collect available data to determine the hazard extent and magnitude	✓ Hazard potential (e.g., wildfire potential, earthquake potential, prior hurricane tracks) ✓ Model simulation and predictions (e.g., storm surge, tsunami inundation zones) ✓ Initial conditions
Compare with geographic/location information for infrastructure assets	✓ Private, state and federal data sources for CI locations

Once the threat data are collected, they need to be analyzed for potential impacts to the CI, as it relates to their specific vulnerabilities. For example, a power surge or loss that causes a significant loss of data may impact an organization's ability to function in the near- and/or long-term. The following is a list of potential vulnerabilities that may negatively impact CI:

- Utility Outage Effects
- Communication Outage/Delays
- Transportation Disruption
- Property Damage
- Data Loss
- Interruption of Operations
- Supply Chain Disruption
- Lack of Adequate Contingency Plans

D. Evaluate CI Resilience to Threat(s)

Putting a value to the potential risk for the priority CI will further inform where mitigation investments will have the greatest impact. If the resilience assessment team is responsible for evaluating the risks, the first thing to consider is the frequency or probability that each threat might impact an asset. To enable a scoring technique, the three categories and associated points for frequency and probability are not applicable (0), occasional (1), likely (3), and highly likely (5).

The other key elements of a risk equation are the impacts of the event, which are, the potential vulnerability or likelihood that an existing asset will fail when exposed to a hazard, and the consequences associated with losing the CI asset. The four categories and associated points for failure and consequence are not applicable (0), negligible (1), limited (2), moderate (3), high (4), and critical (5). Figure 5 shows how these factors can be combined to assess and prioritize risks.

Hazard	Frequency/ Probability	Potential Failure	Consequence	Risk
Flooding	Highly Likely	Limited	Limited	Moderate
Hurricane	Likely	Significant	Critical	High
Landslide	Occasional	Negligible	Negligible	Low

Figure 5: Example of Assessing Risks to Hazards

E. Identify CI Resilience Gaps

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

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

Step 4: Develop, Prioritize, and Implement Mitigation Strategies

4 Develop, Prioritize and Implement Mitigation

A. Identify mitigation strategies
B. Determine risk reduction
C. Prioritize mitigation strategies
D. Identify funding & implement mitigation strategies

Mitigation strategies involve developing the plans to implement the projects, tasks, or activities that will increase the resilience of the SOH as defined by the SOH resilience goals. CI utility data are needed to develop detailed, actionable mitigation strategies. (See Appendix C)

A. Identify Mitigation Strategies

The resilience assessment team with stakeholder engagement and potentially technical assistance from a consultant will develop mitigation strategies that will address the resilience gaps identified in the previous step. There are three general types of mitigation strategies:

- Generation, storage, and distribution infrastructure needed to ensure operations for CI assets. Examples include:
    - Generators
    - Solar panels
    - Grid improvements/hardening
    - Batteries
    - Microgrids
- Efficiency measures to minimize energy demand and thus the need for resources during emergency operations. Examples include:
    - Passive solar design
    - Equipment upgrades
    - Shading techniques
- Operations measures to address potential emergency operations preparation gaps. Examples include:
    - Fuel management contracts
    - Exercises
    - Personnel communication plans

Mitigation strategies are developed for a specific CI asset. There can be more than one mitigation strategy for each CI asset. Appendix A offers the table for tracking mitigation strategies and encourages tracking the following information:

- Project Title
- Description (or reference to where a detailed description can be found)
- Implementation cost
- Projected payback
- Risk reduction
- Potential Funding source(s)

Data from the CI resilience assessment, such as the hazard analysis, and additional more detailed information to track outcomes can also be helpful in the management of mitigation strategies. The list above is likely the minimum amount of information needed to support mitigation strategy implementation tracking.

B. Determine Risk Reduction

Prioritizing mitigation strategies that are focused on risk reduction will offer a greater benefit for the financial and time investment. Risk reduction includes addressing the CI that is most vulnerable to specific threats and identifying and addressing potential infrastructure deficiencies in response to likely threats. Qualitative and quantitative information can be used to assess the potential for risk reduction. For example, installing a solar power system with battery backup could reduce the risk for a CI asset that currently has a generator, minimal fuel storage, and no guarantee of refueling during an emergency. Risk reduction criteria can be defined by the resilience assessment team, using the resilience goals as a guideline.

C. Prioritize Mitigation Strategies

Not all mitigation strategies can be implemented simultaneously because some activities are dependent on others, some are expensive and will require time and effort to identify funding sources, and some will not have the personnel resources to be implemented at this time. The intent of prioritizing mitigation strategies is to optimize the risk reduction and attainment of resilience goals, while addressing as many resilience gaps as is feasible. Table 5 provides some example criteria that could be used to prioritize mitigation strategy investments. (PNNL 2019)

There will likely be some activities that will be funded by the owners of the CI asset, funded by a third-party and managed either by the owner of the CI asset or the third-party, and funded through efforts of the resilience assessment team (e.g., grants). Given the diversity of funding options, the resilience assessment team will benefit from bringing the stakeholders together for the prioritization of the mitigation strategy investments. This prioritization effort could be through workshops to identify, refine and prioritize mitigation strategies. The workshop outcome is a prioritized list of projects/solutions, resourcing plan, and identification of areas requiring further investigation.

Table 5: Example Criteria for Prioritizing Mitigation Strategy Investments

Criteria	Metrics
Strategy provides operational efficiency or cost savings (e.g., from peak shaving, reduced operations and maintenance requirements)	✓ Payback calculation using life cycle cost ✓ Annual operational savings
Strategy reduces energy or use or intensity	✓ Annual energy saved per square foot
Strategy incorporates infrastructure improvements	✓ Yes/No
Strategy reduces environmental impact	✓ Greenhouse gas emissions reduced
Strategy increases fuel and fuel type diversity	✓ Yes/No
Strategy provides sufficient scale and savings for attracting third-party investment	✓ First cost estimate ✓ Life cycle cost savings estimate
Strategy minimizes operations and maintenance burden	✓ Operations and maintenance labor hours or cost savings or increase
Strategy benefits energy security	✓ Yes/No
Strategy is feasible to implement (e.g., technology is ready for deployment, funding is available, personnel are available and trained to maintain the equipment, can be implemented quickly)	✓ Yes/No

D. Identify Funding & Implement Mitigation Strategies

As described above, implementation funding may come from a variety of sources, including CI asset owners. The resilience assessment team is encouraged to coordinate with stakeholders to track the implementation progress and resulting risk reduction from projects that are being managed outside of the team. The spreadsheet link in Appendix A has a tab focused on mitigation strategy implementation tracking. For those activities/projects that are not funded by the CI asset owners, the resilience assessment team can offer assistance in identifying third-party funding for implementation. Potential federal implementation funding resources include, but are not limited to:

- US Department of Defense Office of Economic Adjustment (https://www.oea.gov/): Grants are available for efforts that improve the resilience of military installations and their surrounding communities, and for improving military installation sustainability.

- US Federal Emergency Management Program (FEMA) Hazard Mitigation Grant Program (https://www.fema.gov/hazard-mitigation-grant-program): Grants focused on implementing long-term hazard mitigation measures to improve resilience.

- FEMA Building Resilient Infrastructure and Communities (BRIC) grants (https://www.fema.gov/grants/mitigation/building-resilient-infrastructure-communities): Grants focused on capability- and capacity-building, direct technical assistance, and national competition criteria, which place an emphasis on projects that mitigate risk to infrastructure and community lifelines.

- FEMA Emergency Management Performance Grant Program (https://www.fema.gov/media-library-data/1581717192496-3736b5626f11012c3750de5efb6a4d37/FY_2020_EMPG_NOFO_FINAL_508SA2.pdf): Grants focused on all-hazards emergency preparedness with the following priority areas in fiscal year 2020: logistics, evacuation planning, disaster financial management, catastrophic disaster housing, resilient communications, and community lifeline implementation.

- FEMA Regional Catastrophic Preparedness Grant Program (https://www.fema.gov/media-library/assets/documents/188196): This annual grant program is targeted at closing known preparedness capability gaps, encouraging innovative regional solutions to issues related to catastrophic incidents, and building on existing regional preparedness efforts, including pandemic preparedness.

- US Department of Homeland Security (DHS) Cybersecurity Services Catalog (https://us-cert.cisa.gov/sites/default/files/c3vp/sltt/SLTT_Hands_On_Support.pdf): DHS has a catalog of cybersecurity related services available to state and local governments. The services include cybersecurity assessments, awareness, consulting, information sharing and threat analysis, incident response, and network protection.

- US Department of Agriculture Rural Development (https://www.rd.usda.gov/onerdguarantee): Loan guarantee programs for energy projects, including renewable energy.

- US National Oceanic and Atmospheric Administration Office for Coast Management Coastal Resilience Grants Program (https://coast.noaa.gov/resilience-grant/): Grants are available to help coastal communities prepare for and recover from extreme weather events, climate hazards and changing ocean conditions.

- US Economic Development Administration (EDA) Public Works and Economic Adjustment Assistance Programs (https://www.grants.gov/web/grants/view-opportunity.html?oppId=321695): This program is focused on elements of economic development that could be an outcome of resilience investments, such as the creation and retention of jobs, advancing innovation, enhancing the manufacturing capacities of regions, providing workforce development opportunities, and growing ecosystems that attract foreign direct investment.

- EDA Disaster Supplemental Notice of Funding Opportunity (https://www.grants.gov/web/grants/view-opportunity.html?oppId=319126 and https://www.grants.gov/web/grants/view-opportunity.html?oppId=302953): Grants are available for communities impacted by natural disasters in 2017 – 2019.

- HUD Community Development Block Grant Disaster Recovery Program (https://www.hudexchange.info/programs/cdbg-dr/): CDBG Disaster Recovery (CDBG-DR) assistance may fund a broad range of recovery activities that go to rebuild an affected area and provide crucial seed money to start the recovery process.

- HUD Community Development Block Grant Mitigation Program (https://www.hudexchange.info/programs/cdbg-mit/): Provides assistance in areas impacted by recent disasters to carry out strategic and high-impact activities to mitigate disaster risks and reduce future losses.

Step 5: Evaluate and Re-Assess Critical Infrastructure

5 Evaluate and Reassess

A. Assess progress toward resilience goals
B. Re-assess CI lists
C. Re-evaluate CI list prioritization
D. Update threat information
E. Re-prioritize mitigation strategies

Re-assessment of the CI list, dependencies and interdependencies, threat and vulnerability analyses, and mitigation project implementation strategy will be necessary to maintain current information and track the status of the SOH's CI.

A. Assess Progress Toward Resilience Goals

As mitigation projects are implemented and new information becomes available regarding the SOH's CI, the ICE-I Working Group can track how these CI improvements impact the SOH's resilience goals. As time progresses, goals may be met or need to be updated based on the CI resilience progress.

B. Re-assess CI Lists

The CI list will be most useful if it is treated as a living document and regularly updated with new data. At a minimum, a thorough review and reassessment, including updating the energy data, should be performed every 5 years to address changes to the operations and relative importance of the SOH's CI list. Additionally, performing an annual review and update of the CI list focused on the following, is recommended:

- New CI assets (e.g., solar power system added to the grid)
- CI asset point of contact, if necessary
- Energy consumption and generation data
- Any notes on activity over the year
- Mitigation projects that are recommended or being implemented

C. Re-evaluate CI List Prioritization

Over time there will likely be a need to re-evaluate and re-prioritize the SOH CI list. At a minimum, it is recommended to review the prioritization status every 5 years. Re-evaluation could be needed because of changes in prioritization criteria or changes in what is known about the CI assets. Some reasons for re-evaluating priorities include:

- Changes in the SOH's resilience goals
- New CI assets added to the list
- CI assets removed from the list
- Changes to dependencies/interdependencies
- New information regarding the CI assets, especially higher quality energy data
- New information regarding the threats/hazards
- New CI vulnerability information
- Implemented mitigation projects

D. Update Threat Information

The threat information related to CI assets may remain stable for some threats or change frequently and require seasonal reviews for other threats. Changes in natural hazard models could change for specific storm models or as the general models are updated with new historical data or climate change projections. Intelligence information regarding specific human or cyber threats could change rapidly. New hazards, such as a pandemic, may also come forward as threat information that could need updating. It is recommended the threat information is updated as needed, but again, at a minimum every 5 years.

E. Re-prioritize Mitigation Strategies

Similar to the effort to re-evaluate the CI list prioritization, the mitigation strategy list needs to be re-evaluated and re-prioritized as projects are implemented, the SOH's resilience goals change, and new CI assets are added to the list.

References

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

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

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

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

Appendix A – Methods for Collection and Summation of Energy Data for Critical Infrastructure Assets

A spreadsheet tool is included that can be used to support identification and prioritization of the SOH's CI, document risks, and track the implementation of mitigation strategies.

Hawaii CI Data.xlsx

This workbook tabs serve the following purposes:

- Assessment Checklist: This tab has a printable list of the steps and sub-steps that could be used for tracking actions.

- Critical Infrastructure (CI) List: This tab includes key information associated with each CI asset (the first three lines are example assets), including:
    - Asset name and description
    - Point of contact and contact information
    - Asset address
    - Owner type
    - DHS sector, sub-sector (if relevant), and community lifeline
    - Energy use data
    - Backup system data
    - Power stability tolerance
    - Utility providers
    - Energy generation data
    - Prioritization scores and ranking
    - Threat analysis and risk score
    - Ability to keep notes for each data type

- State of Hawaii (SOH) Resilience Goals: This tab documents the SOH resilience goals.

- Prioritization Criteria: This tab documents the prioritization criteria.

- Mitigation Strategy: This tab is linked to the CI List and can be used to document, prioritize, and track the implementation of mitigation strategies.

- Data Validation: This tab hosts the lists that manage the entries in the CI List tab.

The following tables provide definitions for the type of CI asset and energy data needed for the resilience assessment activity. (PNNL 2019)

Table 6: Critical Infrastructure Energy Characterization Data

Description	Format/Information	Purpose	Examples/Discussion
Infrastructure **Name**	Any	Identification of each infrastructure asset	
Infrastructure Applicable FEMA **Lifeline**	(1) Safety and Security, (2) Food Water Sheltering, (3) Health and Medical, (4) Energy (Power and Fuel), (5) Communications, (6) Transportation, (7) Hazardous Material	Sort for interdependency analysis	Any or multiple of the (7) lifelines listed
Infrastructure **Sector**	(1) Private: (1a) Commercial, (1b) Residential, (1c) Industrial), (2) Municipal, (3) State, (4) Federal, (5) Other	Sort for interdependency analysis, identify potential revenue streams for project implementation after gap analysis	Any of the instances listed
Infrastructure **Address**	Any	Develop impact assessments based on location, ability to map interdependencies	
Infrastructure **Type**	State should define values "Type" category can take as initial list is created	Sort for interdependency analysis	Types include Airport, Aviation Fuel, BSL-3 Lab, Facility, Fuel, Harbor, Hospital, Plant, Power, Pumping Station, Reservoir, Shaft, State Capitol, Substation, Switching Station, Tank, Terminal, Well, Other

Infrastructure **Use/description**	Brief description of critical function (emergency services provided)	Characterize common systems or uses within assets, identify and trace interdependencies from site to source utility	ex: Water pump #15 provides up to 50,000 gallons per day of potable water to Generic Hospital Complex
Infrastructure **stakeholder**/site manager/other contact(s)	Name, Position, and Contact Information	Contact for data requests per asset, generate list of personnel to help develop planning procedures	Ideally this will be an individual person or small group of people
Infrastructure **utility category**	Utilities may including: (1) electricity, (2) natural gas, (3) heating fuel oil, (4) propane, (5) potable water, (6) non-potable water, (7) wastewater, transportation fuel such as (8) gasoline, (9) diesel, (10) aviation fuel, and central plant utilities such as (11) steam, (12) hot water, (13) chilled water, or others.	Designate utilities infrastructure that needs to be maintained. Create list for utility quantification addressed in the following questions	In addition to utilities, an individual asset/infrastructure may also require other consumable goods to maintain critical services provided.
Infrastructure critical **demand side utility requirement**, for each applicable utility	Value and units. Characterization of how load was determined	Characterization/estimation of the critical demand side utility requirement for infrastructure, either through continuity of utility or backup sources. Peak demand or average operating utility load may be easier to determine for initial quantification and categorization than critical utility demand requirement. Service equipment capacities for utilities (electrical transformer size, water supply main size, etc.) can provide estimations of the design utility capacity if operational data are not available	ex: 750 kW peak electrical load, 400 MMBH peak natural gas load, 1,000 gallons per hour average potable water consumption, 1000 kW electrical transformer, 8" water supply main, 6" steam main, etc. Operating load estimates may be larger than the critical emergency load, depending on whether the critical infrastructure operation scales up or down from peak/average load, while estimates based on equipment capacities should always be higher than the critical load

Infrastructure existing **backup systems** (or local generation) **size** and **storage** capacity for each applicable utility	System, utility, value, and units	The available supply capacity of any existing backup systems can offset the demand side utility requirement while backup systems have capacity to supply utility to infrastructure	ex: Diesel or natural gas generators for electric utility, generator size (kW), and storage capacity (gallons); ex: Solar photovoltaic: design size (kW), any potential battery storage (Amp hours) ex: On-site water storage tanks for non-potable water: capacity (gallons)
Infrastructure delineation of **continuous and intermittent** critical loads	Continuous or Intermittent designation	Characterizing continuous and intermittent loads is necessary for solution development as part of gap analysis. Continuous loads require both backup sources (ex: electrical generator) and bridging system (ex: UPS-uninterruptible power supply) to ensure utility load is not lost during transfer to backup power	What (if any) systems of an asset have to run continuously compared against what (if any) systems can operate intermittently while still maintain ability to provide critical services ex: Continuous electric service is required to sustain data center ex: Police station operation is required, however, a 2 minute interruption in electrical power during generator switchover from grid to generator backup is acceptable
Infrastructure utility **downtime** that would result in interruption of critical service provided for each applicable utility	Utility and maximum acceptable time of interruption during an event	Identify gaps in ability to provide demand side utility requirements and help generate potential solutions during gap analysis	ex: 6 hours [existing generator will sustain electrical load for 6 hours based on stored fuel capacity, loss of electrical power for longer will result in service interruption]
Infrastructure **supply side critical utility source**	Name or description of provider of each critical utility supplied	Identify interconnections and potential supply side critical utility sources if not already included in list	Should align with Name in Asset List
Infrastructure **Size**	Value and units	Categorize critical infrastructure by size, help quantify impacts of hazards, use for projections of supply or demand side utility requirements if information is not available	ex: covered square footage for a building or collection of buildings, linear feet for pipeline, acre-feet for a water reservoir

Infrastructure **critical utility category (if applicable)**	Utilities may including: (1) electricity, 2) natural gas, (3) heating fuel oil, (4) propane, (5) potable water, (6) non-potable water, (7) wastewater, transportation fuel such as (8) gasoline, (9) diesel, (10) aviation fuel, and central plant utilities such as (11) steam, (12) hot water, (13) chilled water, or others.	Categorize critical infrastructure by impact, use to develop interdependency analysis	Utility service provided to state by critical infrastructure
Infrastructure **quantification of critical service** provided (supply side utility capacity or other quantification for non-utility)	Value and units	Categorize critical infrastructure by impact, use to develop interdependency analysis, use for projections of demand side utility requirements (for non-utility infrastructure) if information is not available	ex: 1000 kW, 500 meals/day, 10,000 lbs goods processed/hour, $2M exchanged/day, 5MGD Characterization of critical service provided, utility or other
Infrastructure **occupancy: critical staff**	Number of people and type (if applicable/necessary for demand side requirement projections)	*Occupancy is not a key characteristic*, but is used primarily to categorize critical infrastructure by impact, develop interdependency analysis, and generate projections of demand side utility requirements if information is not available	Critical staff for maintaining critical service, asset/infrastructure maintenance staff, management staff, etc.
Infrastructure **occupancy: customer/users of service**	Number of people and type (if applicable/necessary for demand side requirement projections)	*Occupancy is not a key characteristic*, but is used primarily to categorize critical infrastructure by impact, develop interdependency analysis, and generate projections of demand side utility requirements if information is not available	How many people rely on the service provided as a part of each asset/infrastructure

Table 7: Description of Available Types of Energy Characterization Data

Utility Service Data – Utility service data describes both the physical and contractual configurations for energy utilities, including energy utility providers and associated contracts (electricity, natural gas, primary fuels, thermal energy), physical descriptions of energy infrastructure, physical and contractual relationships with energy generation providers. Outage data covering disruptions can be requested from the utility. Utility rate or similar analyses (demand response, interruptible rates, etc.) are useful resources to review, when available.

Existing Systems and System Operations – In addition to the utility service data, information characterizing energy generation and supply systems needs to be collected. Data should cover the location and specifications for:

1. Existing renewable/alternative energy generation and storage systems
2. Central plants for heating and/or cooling
3. Existing backup generators (both fixed and mobile)
4. Onsite fuel storage
5. Building-scale UPS
6. Documents describing the operations and maintenance (O&M) activities associated with existing systems.

Plans and Reports by others – A survey of past and current assets/infrastructures assessments and/or planning documents helps with the collection of relevant CI information. Where available, the following documents may be useful:

1. Previous resilience or outage planning reports
2. Master planning documents
3. Sustainability plans and/or Net Zero reports
4. Energy audits and evaluations
5. Controls optimization and/or building returning reports
6. Vulnerability assessments
7. Utilities management plans

Emergency Procedure Documents – In order to understand system operations and the response activities planned for energy disruptions, asset-level emergency procedure documents, standard operating procedure documents, continuity of operations plans, emergency preparedness and response plans, service restoration plans, generator refueling plans, spill prevention containment and control plans, and similar plans should be collected and reviewed.

Engineering Drawings / Documents / Data – The variety of engineering documents used during the energy analysis can include: GIS layers for utility systems that include all system elements for the energy utilities, one-line/single-line diagrams for electric service, lists of buildings with utility meters and/or a centralized energy management control system, and building floor plans.

Utility Consumption / Load Data – Utility consumption data will exist in numerous formats and time scales, ranging from monthly utility bills to daily consumption or generation totals to granular data in hourly or 15-minute intervals for the CI asset. The availability of such data, and the time and resources required to collect it and analyze the data will vary by asset. Where possible, primary sources (e.g., the utility account management website) should be used to minimize the time and resource burden of data collection. Consumption or load data for all utilities (electricity, natural gas, primary fuels, thermal energy production, etc.) can be obtained from the following:

1**. Monthly utility bills** may be requested as original scans, spreadsheets, obtained directly from the utility website, or other formats. At a minimum, they should include monthly totals and peak demand values, and detailed charges and/or rate information for the energy provided. Initial efforts may not require detailed utility analysis, but project development will likely require a minimum amount of baseline utility data to generate effective solutions and baseline characteristics. more detailed analysis will benefit from multiple years' worth of data in order to identify consumption and cost trends and understand seasonal variability.

2**. Interval data from utility**, at the smallest time-step available, is used to develop an accurate load profile for the entire facility or asset. These data are obtained from the utility – often via a customer account management website. As with the utility bills, at least one year of data is optimum to evaluate the overall consumption and potential peak power demand, but it may not accurately represent seasonal and annual variation in consumption. As many years' worth of data as can be obtained will improve the accuracy of the analysis.

3. **Building or Asset-level interval meter data** provides the best granularity and highest fidelity of load data for the assessment. Monthly utility data may be captured by a site energy manager for reimbursable billing customers. Centralized energy management control systems should be leveraged as a resource for facility level interval data where they exist.

4. **Where interval data are unavailable**, techniques to **characterize energy consumption** for individual facilities can be found in Appendix C.

Utility Outage Data – recorded utility outage information for outages from both the utility and consumers.

Asset/Infrastructure Resource Data – On-site energy resource information may be available from the asset owners – particularly in instances where renewable energy assessments have been conducted. Some information on resource availability (solar insolation values, wind resource data) will be obtained from external sources.

Asset/Infrastructure Related Control Systems – Cataloging the supervisor control systems that monitor and/or manage energy systems for an asset can be important to developing a continuity of operation plan. Staff who manage supervisory control and data acquisition (SCADA) systems should be able to provide information on the facility related control systems (also known as operational technology or industrial control systems) in use, from building control systems to a centralized energy management control system. Useful information includes the system type/brand, buildings covered, system components covered (e.g., electric distribution automation), data types collected, management and control capabilities, and interface with other systems.

Appendix B – Hazard Assessment Resources

Table 8: Map and Data Sources for Natural Hazard Assessment

Map/Data	Name	Date	Source
Earthquake	Earthquake Locations > 2.5	1900-2018	USGS Earthquake catalog https://earthquake.usgs.gov/data/comcat/
	Fault Slip Rate	2006	USGS Earthquake Hazards Program https://earthquake.usgs.gov/hazards/qfaults/
	Probability of exceedance (2%, 50 year)	2015	USGS Earthquake Hazards Program
Flood	National Flood Hazard Layer	2015	Federal Emergency Management Agency (FEMA)
Severe Weather	Historical Tornado Tracks	1950-2015	National Weather Service, Storm Prediction Center (SPC)
	Historical Hail Events	1955-2017	National Weather Service, Storm Prediction Center (SPC)
	Historical Wind Events	1955-2017	National Weather Service, Storm Prediction Center (SPC)
	Lightning Density	1986-2012	National Centers for Environmental Information (NOAA-NCEI)
	Tropical Storm Tracks	1851-2008	Homeland Infrastructure Foundation Level Data (HIFLD) Open Source Data for Natural Hazards
Wildfire	Wildfire Starts	1980-2016	The Department of the Interior, Office of Wildland Fire
	Historic Fire Boundaries	1986-2017	USFS/USGS Monitoring Trends in Burn Severity (MTBS)
	Wildfire Hazard Potential	2018	USDA Forest Service, Fire Modeling Institute
Coastal Flooding	Flood-Prone Coastal Areas	2012	NOAA Digital Coast
Drought	U.S. Drought Monitor	2000-2019	National Drought Mitigation Center at the University of Nebraska-Lincoln, the United States Department of Agriculture, and the National Oceanic and Atmospheric Administration,
Pandemic	Probabilistic Analysis for National Threats Hazards and Risks (PANTHR)	2020	Department of Homeland (DHS) Security Science and Technology Directorate (S&T)

Appendix C – Estimating Energy Demand

CI asset energy consumption data are needed for three purposes:

- to establish the *average daily* and *peak* energy use
- to establish load profiles that enable sizing and configuration of generation/production and storage solutions
- to identify energy savings opportunities associated with demand reduction measures, including efficiency retrofits and operational changes

When metered interval data are not available the following is a list of other, less accurate techniques for estimating energy consumption: (PNNL 2019)

- Modeled consumption estimates based on software generated models of buildings (e.g. Energy Plus)
- Feeder or substation interval data – Use when single facilities or clusters of critical facilities are on a single feeder or substation, or when non-critical facilities on the feeder can be easily pulled out
- Monthly facility metered data – If meters are read and recorded on a monthly basis, the data can be used to estimate a single kWh value and single kW value per building (or metered circuit)
- Temporary facility meters – If no facility-level data are available, temporary meters that log interval data may be installed on a facility for a few weeks to estimate peak and total demand
- Interval data from similar facilities – Metered data from similar facilities can be used as a proxy
- Energy use intensity (EUI) estimates – Estimate monthly energy use with EUIs typical of the building type using the US Environmental Protection Agency's Portfolio Manager
- Backup generator sizing – The capacity of the installed generator can be assumed to be a proxy for peak demand (kW)
- Service transformer sizing – The capacity of the transformer can be assumed to be a proxy for peak demand (kW)
- Central plants system (heating/cooling) sizing and configuration – Values can be assumed to represent peak thermal demand in whole or apportioned at the facility level depending on number and types of facilities
- Central plants (heating /cooling) recorded output or fuel consumption data – Daily production values or daily fuel consumption values are used or apportioned at the facility level depending on number and types of facilities
- Mechanical equipment schedules – Equipment maintenance schedules for major HVAC equipment may include sizing data

Pacific Northwest National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354
1-888-375-PNNL (7665)

www.pnnl.gov