DHS RESILIENCE FRAMEWORK

Providing a roadmap for the Department in Operational Resilience and Readiness

Homeland Security

RESILIENCE FRAMEWORK

U.S. DEPARTMENT OF HOMELAND SECURITY

Claire M. Grady
Under Secretary for Management

13 Ag 2018
Date

EXECUTIVE SUMMARY

Since May 1998, Presidential and Federal Directives and Executive Orders have been issued on protecting national critical infrastructure. Critical infrastructure are those assets and systems that are so vital to the United States that the incapacity or destruction of them would have a debilitating impact on security, national economic security, national public health, or safety. Since Hurricane Katrina in 2005, there has been a notable shift in emphasis from protecting critical infrastructure but to also ensuring that communities and Federal agency infrastructure are resilient. Simply stated, *resilience* is the ability to adapt to changing conditions and withstand and rapidly recover from disruption. Hazards and threats that can cause disruptions can take many forms, including natural, technological, and human-caused. These could entail, for example, severe weather, power outages, roadway failures, acts of terror, and cyberattacks.

Under Federal Directives and Executive Orders, the Department of Homeland Security (DHS) is designated to provide strategic guidance, promote a national unity of effort, and coordinate the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure. Within DHS the major responsibility for these activities resides within the National Protection and Programs Directorate (NPPD). Federal requirements also direct each agency to ensure the resiliency of its own internal critical infrastructure. As a result, DHS formalized development of Continuity processes and plans to maintain DHS mission essential functions and their associated critical infrastructure assets, especially during hazard and threat events. These activities are led by the DHS Office of Operations Coordination.

Additionally, the Department strives to improve the efficiency and security of its facilities by reducing energy and water use and cost and increasing use of renewable energy sources, driven by other Federal requirements and the desire to reduce operating utility costs and enhance energy security.

Following the 2017 hurricane and wildfire season, DHS initiated a more focused effort to formalize a Department-wide process that integrates the activities for incorporating resilience into our critical infrastructure through a holistic framework to ensure sustained resilience of mission essential functions and related supporting critical infrastructure assets during all phases of mission operations (normal operations, disruptive event, response, and recovery/reconstitution). This effort has been led by the DHS Office of the Chief Readiness Support Officer (OCRSO) with participation in a DHS Tiger Team by all Components and key Headquarters organizations, and in partnership under a Memorandum of Understanding with the Department of Energy (DOE), Federal Energy Management Program (FEMP). The result of this effort is the development of a six-step DHS Resilience Framework (Figure 1). This Framework establishes a process for the Department to use as a roadmap for incorporating Continuity into normal operations and building resilience into critical infrastructure assets that ensures DHS can sustain its mission essential functions in times of threats and disasters, as well as during normal operations.

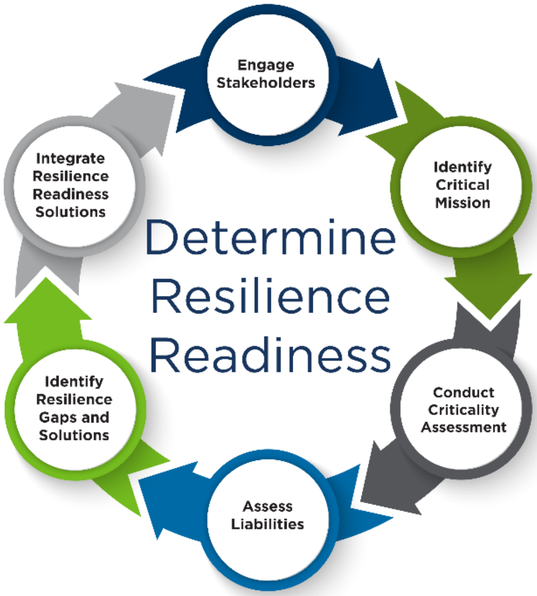

Engage Stakeholders
Identify Critical Mission
Conduct Criticality Assessment
Assess Liabilities
Identify Resilience Gaps and Solutions
Integrate Resilience Readiness Solutions
Determine Resilience Readiness

Figure 1. Resilience Framework Process

The Resilience Framework establishes guidelines for implementing, monitoring, and identifying DHS resilience readiness.[1] In doing so, the Framework process focuses on four critical infrastructure areas: Energy and Water, Facilities, Information and Communication Technology, and Transportation. These four areas are in alignment with the critical infrastructure sectors categorized as "lifeline systems," which, taken individually or in the aggregate, are intimately linked with the economic well-being, security, and social fabric of the communities they serve. Based on past experience, these focus areas have also been identified as where key DHS infrastructure assets have shown distinct vulnerabilities to hazards and threats, such as hurricanes.

The Resilience Framework capitalizes on existing DHS Continuity planning by incorporating Continuity processes and analyses into the first four steps of the overall Resilience planning process, followed by identification and integration of resilience solutions into life cycle planning and execution. This unification of business processes provides a common lexicon and an objective, systematic analysis to determine the current state of the Department's infrastructure resilience and to identify and prioritize solutions and projects needed to ensure resilient critical infrastructure to maintain mission essential functions during all phases of DHS operations. Implementation of the Resilience Framework process and the resultant Component Plans for Resilience will provide informed, risk-based decision making for long-term planning and budgeting across the Department.

DHS Components will apply the Resilience Framework, along with additional information from other assessments, such as facility energy, water, and sustainability audits, facility condition assessments, and physical and vulnerability assessments to develop Component Plans for Resilience within one year following the issuance of this Resilience Framework document. The Component plans will coordinate with the Continuity Plans to identify and prioritize mission assets, identify the current overall level of resilience of Component critical infrastructure assets, and the solutions and projects required to make these assets fully resilient. Shared across the Department, these Component Plans for Resilience will help DHS in formulating overall long-term planning and budgeting strategies.

[1] DHS Under Secretary for Management memorandum, March 28, 2018.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF APPENDICES

1 INTRODUCTION

In May 1998, Presidential Decision Directive (PDD)-63 was issued addressing critical infrastructure protection. This PDD recognized certain parts of the national infrastructure as critical to the national and economic security of the United States and the well-being of its citizenry, and required steps to be taken to protect it. This was updated in December 2003 by the Homeland Security Presidential Directive (HSPD)-7 for *Critical Infrastructure Identification, Prioritization, and Protection*. This Directive describes the United States as having some critical infrastructure that is "so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety." Since then, new Directives and Executive Orders have expanded upon these policies and directed agencies to assess their internal critical infrastructure and ensure it is resilient to maintain mission essential functions during disruption from threat and hazard events, as well as during normal operations. In the aftermath of Hurricane Katrina in 2005, there has been a notable shift in emphasis from protecting critical infrastructure to ensuring that communities are resilient.

> *Resilience is the ability to adapt to changing conditions and withstand and rapidly recover from disruption.*

Mission essential functions (MEFs) enable an organization to provide vital services, exercise civil authority, maintain the safety of the public, and sustain the industrial/economic base during disruption of normal operations.[2] *Resilience* is the ability to adapt to changing conditions and withstand and rapidly recover from disruption. Hazards and threats that can cause disruptions can take many forms, including natural, technological, and human-caused. These could entail, for example, severe weather, power outages, roadway failures, acts of terror, and cyberattacks.

As a result of these Federal requirements for resilient critical infrastructure, the Department formalized development of Continuity of Operations processes and plans that focused on maintaining mission essential functions and their associated critical infrastructure, especially during hazard and threat events. Concurrent with these Continuity activities, DHS strives to improve the efficiency and security of its facilities by reducing energy and water use and cost and increasing use of renewable energy sources, all driven by Federal legal requirements and the desire to reduce operating utility costs. Implementing

[2] DHS Lexicon, page 345. http://dhsconnect.dhs.gov/org/comp/esec/Documents/DHS%20Lexicon%20Publication.pdf

these energy and water performance improvements has also resulted in making DHS facilities and energy and water infrastructure more resilient in supporting mission essential functions.

Following the 2017 hurricanes and wildfire events that occurred on the mainland United States, Puerto Rico, and Virgin Islands, DHS broadened their focused effort to formalize a Department-wide process that integrates Continuity and other facility and infrastructure performance improvement planning and implementation processes into a holistic framework to ensure sustained resilience of mission essential functions and related supporting infrastructure during all phases of mission operations (normal operations, disruptive event, response, and recovery) as outlined in this document.

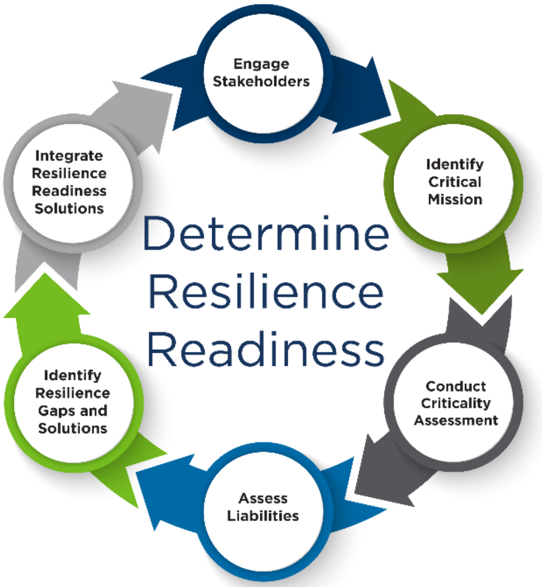

Engage Stakeholders
Identify Critical Mission
Conduct Criticality Assessment
Assess Liabilities
Identify Resilience Gaps and Solutions
Integrate Resilience Readiness Solutions
Determine Resilience Readiness

Figure 1. Resilience Framework Process

The Resilience Framework focuses on four key critical infrastructure areas where the Framework process is applied. These four focus areas, which are described in detail in Section 4.0., are:

- Energy and Water,
- Facilities,
- Information and Communication Technology, and
- Transportation.

As depicted in Figure 2 and discussed in more detail in Section 5.0, the Resilience Framework is formulated to support a process that ***Engages Appropriate Stakeholders*** to:

- ***Identify Critical Mission*** using a Business Process Analysis (BPA) to identify mission essential systems, functions, and their associated critical infrastructure mission essential assets (MEAs);
- ***Conduct a Criticality Assessment*** using Business Impact Analysis (BIA) to determine how important, or critical, are the identified mission essential functions and assets;
- ***Assess Liabilities*** by analyzing the level of risk posed by potential hazards and threats to, and vulnerabilities of, the mission critical functions and assets;
- ***Identify Resilience Gaps and Determine Resilience Solutions*** that will ensure MEAs are sufficiently resilient so that no loss of critical mission essential functions occurs beyond the maximum tolerable downtime during and after disaster events. In association with the Resilience Framework, a *Resilience Readiness Planning Assessment* guide was developed to score the level of resilience within each of the four focus areas that can be applied to DHS sites; and
- ***Integrate Resilience Readiness Solutions*** that will close the gaps between the current state and a resilient state of MEAs to ensure continuous performance of critical mission essential functions as needed during times of hazard or threat disruption, as well as during normal operations.

The Resilience Framework capitalizes on existing DHS Continuity planning by incorporating Continuity processes and analyses into steps 2, 3, and 4 of the overall Resilience planning process, followed by identification and integration of resilience solutions into life cycle planning and execution. This unification of business processes provides a common lexicon and an objective, systematic analysis to determine the current state of the Department's infrastructure resilience and to identify and prioritize needed solutions and projects aimed at ensuring resilient critical infrastructure can support mission essential functions during all phases of DHS operations. Implementation of the Resilience Framework process and the resultant Component Plans for Resilience will provide informed, risk-based decision making for long-term planning and budgeting across the Department.

DHS Components will apply the Resilience Framework and Resilience Readiness Planning Assessment, along with additional information from other assessments such as facility energy, water, and sustainability audits and physical and vulnerability assessments, to develop Component Plans for Resilience. These plans will identify the current overall level of resilience of Component critical infrastructure MEAs and the solutions and projects required to make these assets fully resilient. Shared across the Department, these Component Plans for Resilience will help DHS in formulating overall long-term planning and budgeting strategies.

The following sections in this document provide references for Federal and DHS drivers for the Resilience Framework process and more detailed discussion about the four resilience infrastructure focus areas, steps of the Resilience Framework process, resilience assessment, the Component Plan for Resilience template, and supplementary appendices.

2 RESILIENCE DRIVERS

Since 2013, resilience and energy security have been at the forefront for Federal Government agencies to plan for, and incorporate into, their strategies. The following Federal and DHS requirements direct DHS to become more secure and resilient and support the Department's Resilience Framework initiative and activities.

- Presidential Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, issued February 12, 2013: Outlines the Nation's policy to enhance the security and resilience of critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties.[3]
- Presidential Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,* issued May 11, 2017: Holds heads of Executive Departments and Agencies accountable for managing cybersecurity risk to their enterprises.[4]
- Presidential Executive Order 13834, *Efficient Federal Operations*, issued May 17, 2018: In meeting statutory requirements related to energy and environmental performance, Agencies shall increase efficiency, optimize performance, eliminate unnecessary use of resources, and protect the environment, prioritizing actions that reduce waste, cut costs, enhance the resilience of Federal infrastructure and operations, and enable more effective accomplishments of its mission.[5] (Revokes EO 13693)
- Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, issued February 12, 2013: Requires Departments and Agencies to identify, prioritize, assess, remediate, and secure internal critical infrastructure that supports Primary Mission Essential Functions (PMEFs).[6]

[3] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[4] https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

[5] https://www.federalregister.gov/documents/2018/05/22/2018-11101/efficient-federal-operations

[6] https://fas.org/irp/offdocs/ppd/ppd-21.pdf.

- Presidential Policy Directive 40, *National Continuity Policy*, issued July 15, 2016: Requires Departments and Agencies to apply Risk Management principles to ensure operational readiness decisions are based on the probability of the occurrence of a catastrophic emergency and its consequences.[7]
- Federal Continuity Directive (FCD)-1, *Federal Executive Branch National Continuity Program and Requirements*, issued January 17, 2017: Identifies minimum standards for Departments and Agencies to maintain an effective continuity capability, to ensure resiliency and continued performance of their organizations' essential functions under all conditions.[8]
- Federal Continuity Directive (FCD)-2, *Federal Executive Branch National Continuity Program and Requirements*, issued June 13, 2017: Outlines the requirements to conduct Business Process Analyses and Business Impact Analyses on all essential functions to assist Departments and Agencies in identifying and assessing essential functions through a risk-based process.[9]
- DHS Directive 020-01, *Energy & Water Management*, issued January 4, 2016: Requires Components to prepare energy security plans for facilities that support mission-critical activities and maintain a list of critical operations with required infrastructure and their restoration priority.[10]
- DHS Directive 008-03, *Continuity Programs*, issued June 10, 2015: Establishes the DHS policy, responsibilities, and requirements regarding the Department's continuity programs.[11]
- DHS Instruction 008-03-01, *Department Business Impact Analysis Instruction*, issued May 29, 2018: Implements the requirement in DHS Directive 008-03, "Continuity Programs," to establish plans and procedures to identify, prioritize, assess, protect, and restore the Department's internal critical infrastructure and key resources that support the Department's Primary Mission Essential Functions (PMEF).[12]

[7] https://fas.org/irp/offdocs/ppd/index.html.

[8] https://www.fema.gov/media-library-data/1486472423990-f640b42b9073d78693795bb7da4a7af2/January2017FCD1.pdf.

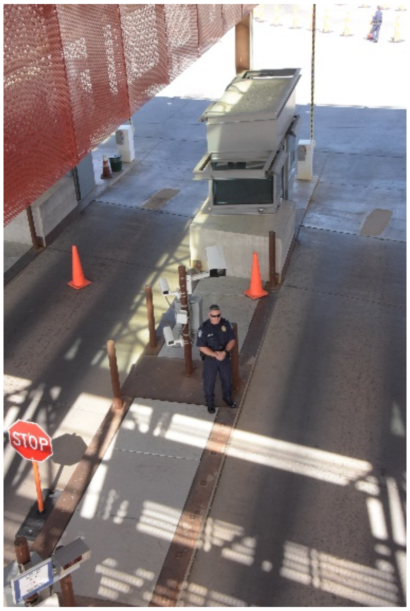
[9] https://www.fema.gov/media-library-data/1499702987348-c8eb5e5746bfc5a7a3cb954039df7fc2/FCD-2June132017.pdf

[10] http://dhsconnect.dhs.gov/policies/Instructions/020-01_Energy_Management_Directive.pdf

[11] http://dhsconnect.dhs.gov/org/comp/ops/CDD/PublishingImages/008-03_Continuity_Programs_Directive.pdf

[12] http://dhsconnect.dhs.gov/policies/Instruction%20Supplements/008-03-001.pdf

3 CRITICAL INFRASTRUCTURE



Presidential Policy Directive (PPD)-21, *Critical Infrastructure Security and Resilience*, states the term "critical infrastructure" has the meaning provided in Section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c(e)), namely systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.[13] PPD-21 identifies 16 critical infrastructure sectors and designates individual Sector-Specific Agencies (SSAs) to serve as the day-to-day Federal interface for the dynamic prioritization and coordination of sector-specific activities for each of the 16 critical infrastructure sectors (Appendix A). PPD-21 directs SSAs to coordinate with DHS and other relevant Federal Departments and Agencies and collaborate with critical infrastructure owners and operators, where appropriate with independent regulatory agencies, and with state, local, tribal, and territorial entities, as appropriate, to implement PPD-21. Each critical infrastructure sector has unique characteristics, operating models, and risk profiles that benefit from an identified SSA that has institutional knowledge and specialized expertise about the sector.

While allowing for the list of critical infrastructure sectors to reflect current concerns over time has provided for flexibility and adaptability, it has also led to some ambiguities about which assets are critical and which criteria should be used to define them. The proliferation of critical infrastructure sectors has added complexity to an already complex field. To develop basic principles that govern performance and clarify interdependencies, it was helpful to consolidate unifying concepts into a smaller number of sectors based on common traits. The concept of a “lifeline system” was developed to evaluate the performance of large, geographically distributed networks during earthquakes, hurricanes, and other hazardous natural events. Lifelines are grouped into six principal systems: telecommunications, electric power, gas and liquid fuels, water supply, transportation, and waste disposal. According to the 2013 National Infrastructure Protection Plan (NIPP), lifeline infrastructure encompasses Communications, Energy, Water, and Transportation, four of the sixteen sectors identified in PPD-21. Taken individually or in the aggregate, all of these systems are intimately linked with the economic well-being, security, and social fabric of the communities they serve. Viewing critical infrastructure through the subset of lifelines helps clarify features that are common to essential

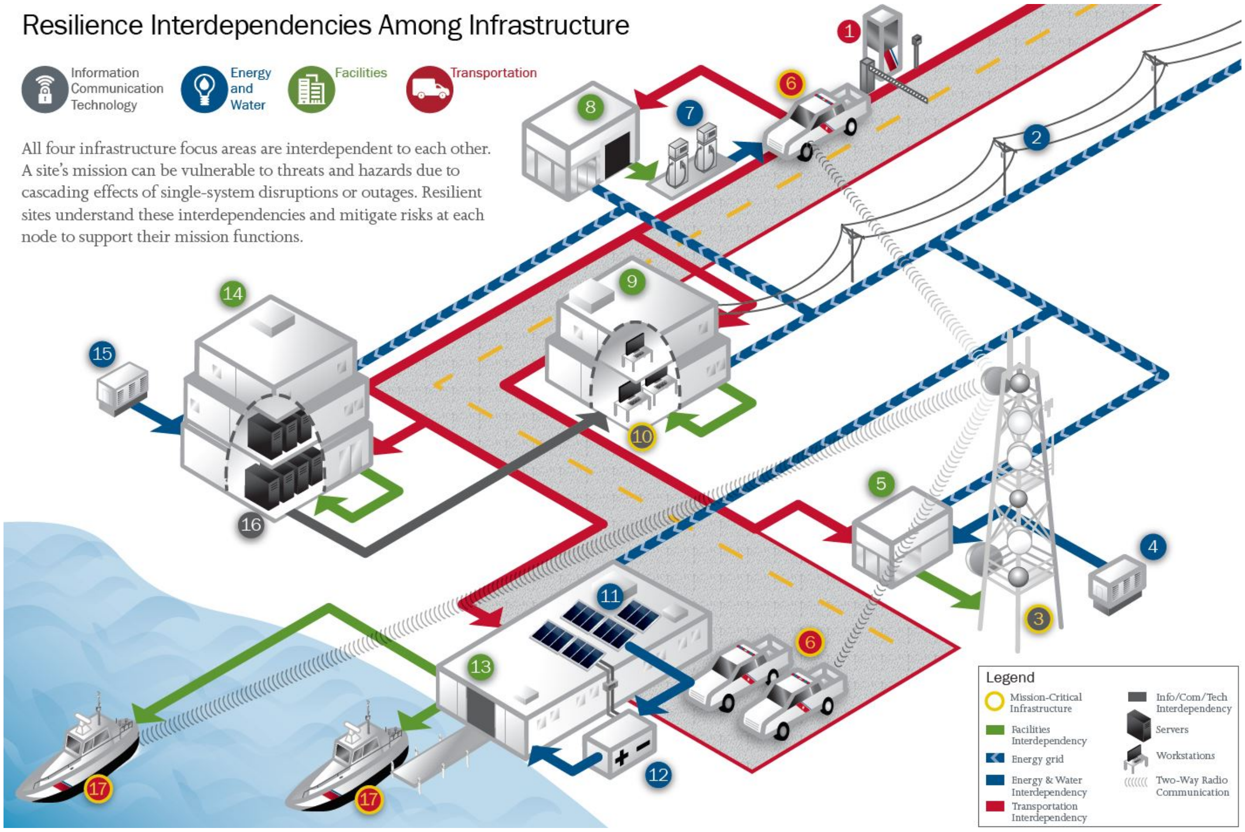
[13] The DHS Lexicon (page 112) defines Critical Infrastructure as systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of those matters, across any federal, state, regional, territorial, or local jurisdiction.

support systems and provides insights into the engineering challenges to improving the performance of large networks.

Lifeline systems are interdependent, primarily by virtue of physical proximity and operational interaction. For instance, damage to one infrastructural component, such as a cast-iron water main, can rapidly cascade into damage to surrounding components, such as electric and telecommunications cables and gas mains, with system-wide consequences. Lifeline systems all influence each other. Electric power networks, for example, provide energy for pumping stations, storage facilities, and equipment control for transmission and distribution systems for oil and natural gas. Oil provides fuel and lubricants for generators, and natural gas provides energy for generating stations, compressors, and storage, all of which are necessary for the operation of electric power networks. This interdependency can be found among all lifeline systems (Figure 3).

In addition, the concept of resilience, like the concept of critical infrastructure, is evolving. In its current form, the resilience of a community is an overarching attribute that reflects the degree of community preparedness and the ability to respond to and recover from a disaster. Because lifelines are intimately linked to the economic well-being, security, and social fabric of a community, the initial strength and rapid recovery of lifelines are closely related to community resilience. Globally applied, resilience is the ability of systems, infrastructures, government, business, and citizenry to resist, absorb, recover from, or adapt to an adverse occurrence that may cause harm, destruction, or loss of national significance, and the capacity of an organization to recognize hazards and threats and make adjustments that will improve future protection efforts and risk reduction measures.

Resilience is the ability of systems, infrastructures, government, business, and citizenry to resist, absorb, recover from, or adapt to an adverse occurrence that may cause harm, destruction, or loss of national significance, and the capacity of an organization to recognize hazards and threats and make adjustments that will improve future protection efforts and risk reduction measures.



Resilience Interdependencies Among Infrastructure

All four infrastructure focus areas are interdependent to each other. A site's mission can be vulnerable to threats and hazards due to cascading effects of single-system disruptions or outages. Resilient sites understand these interdependencies and mitigate risks at each node to support their mission functions.

Information Communication Technology
Energy and Water
Facilities
Transportation
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
+ −
Legend
Mission-Critical Infrastructure
Facilities Interdependency
Energy grid
Energy & Water Interdependency
Transportation Interdependency
Info/Com/Tech Interdependency
Servers
Workstations
Two-Way Radio Communication

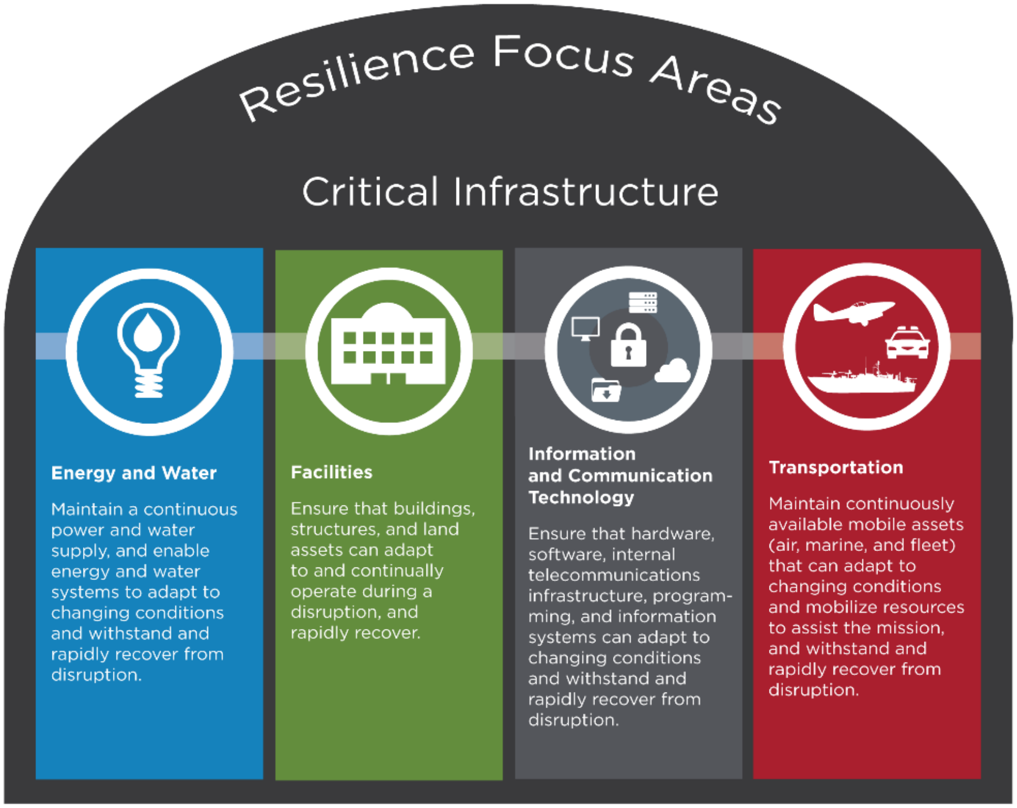
Figure 2. Resilience Interdependencies among Infrastructure

4 RESILIENCE FOCUS AREAS

PPD-21 states the Secretary of Homeland Security shall provide strategic guidance, promote a national unity of effort, and coordinate the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure. In carrying out the responsibilities assigned in the Homeland Security Act of 2002, as amended, the Secretary of Homeland Security evaluates national capabilities, opportunities, and challenges in protecting critical infrastructure; analyzes threats to, vulnerabilities of, and potential consequences from all hazards on critical infrastructure; identifies security and resilience functions that are necessary for effective public-private engagement with all critical infrastructure sectors; develops a national plan and metrics, in coordination with SSAs and other critical infrastructure partners; integrates and coordinates Federal cross-sector security and resilience activities; identifies and analyzes key interdependencies among critical infrastructure sectors; and reports on the effectiveness of national efforts to strengthen the Nation's security and resilience posture for critical infrastructure. Within DHS the major responsibility for these activities resides within the National Protection and Programs Directorate (NPPD).

PPD-21 also directs all Federal Department and Agency heads to be responsible for the identification, prioritization, assessment, remediation, and security of their respective internal critical infrastructure that supports primary mission essential functions. Such infrastructure shall be addressed in the plans and execution of the requirements in the National Continuity Policy. DHS Directive 008-03, *Continuity Programs*, requires the Department to establish plans and procedures to identify, prioritize, assess, protect, and restore the Department's internal critical infrastructure and key resources. Within DHS the major responsibility for overseeing these internal critical infrastructure activities resides within the Management Directorate (MGT). It should be noted that NPPD may include some DHS and Component facilities as part of its outward-focused regional resilience assessments. In these instances, NPPD, MGT, and relevant Components should coordinate to share information and results of analyses that may be incorporated into applicable Component Plans for Resilience.

In this Resilience Framework, DHS is focusing on four DHS infrastructure areas because they align with the lifeline critical infrastructure and based on experience and lessons learned from past natural disaster events, these areas have shown a high potential vulnerability to interruptions in continuity of mission essential functions during events and required substantial efforts to reconstitute operations after these events. These four resilience focus areas are: (1) energy and water, (2) facilities, (3) information and communication technology (ICT), and (4) transportation (Figure 3).



Resilience Focus Areas

Critical Infrastructure

Energy and Water

Maintain a continuous power and water supply, and enable energy and water systems to adapt to changing conditions and withstand and rapidly recover from disruption.

Facilities

Ensure that buildings, structures, and land assets can adapt to and continually operate during a disruption, and rapidly recover.

Information and Communication Technology

Ensure that hardware, software, internal telecommunications infrastructure, programming, and information systems can adapt to changing conditions and withstand and rapidly recover from disruption.

Transportation

Maintain continuously available mobile assets (air, marine, and fleet) that can adapt to changing conditions and mobilize resources to assist the mission, and withstand and rapidly recover from disruption.

Figure 3. Resilience Focus Areas

For each focus area, being resilient entails the ability to adapt to changing conditions and withstand and rapidly recover from disruption. This means that infrastructure and systems need to be able to provide adequate energy and water supplies, facility operations, information and communication technology capability, and transportation availability when it is needed, where it is needed, and for how long it is needed to maintain, at the very least, mission essential functions during normal operating conditions as well as during and after threats and hazardous events (Figure 4).

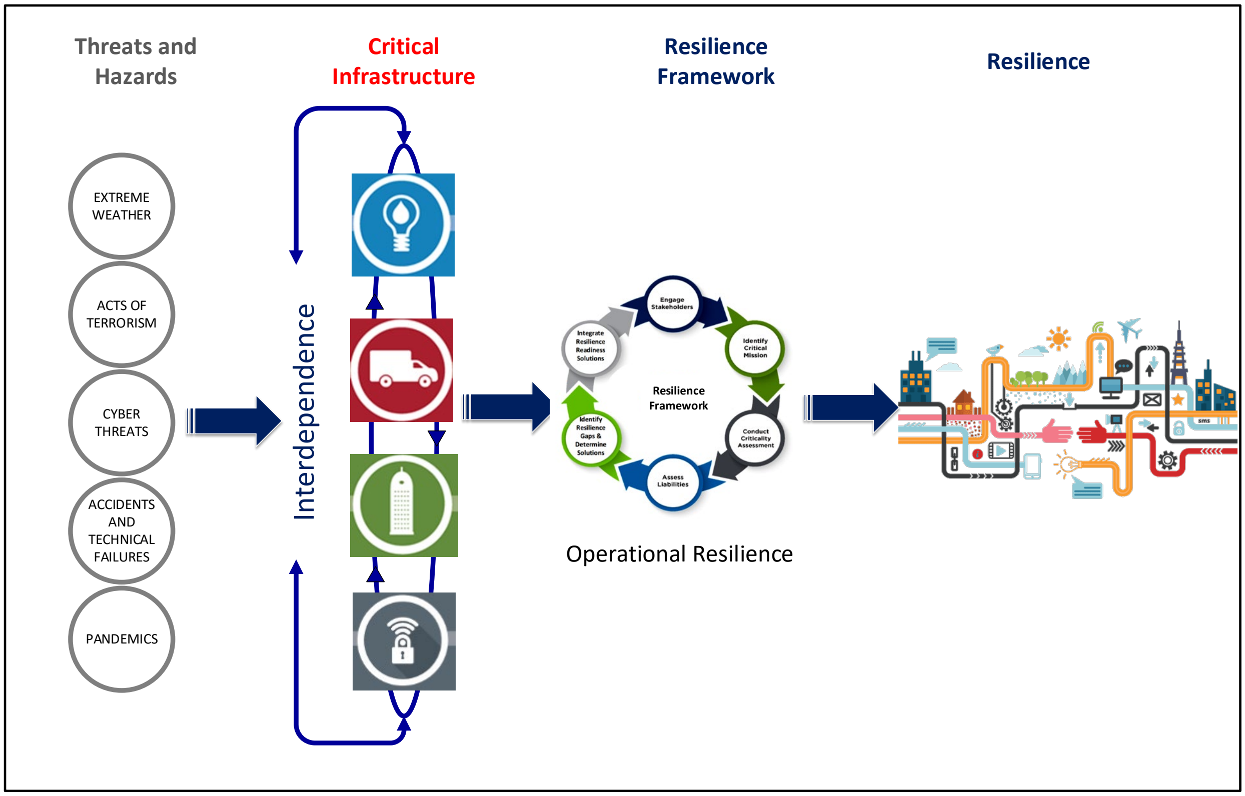


Figure 4. Effects of Vulnerabilities on Critical Infrastructure and Resilience

4.1 Energy and Water

PPD-21 critical infrastructure energy systems, including those providing electricity and fuels are vital to mission essential functions and their associated essential infrastructure, including powering facility operations and communication networks, heating buildings, or fueling land, air, and marine transportation mobile assets. PPD-21 water and wastewater critical infrastructure systems are also vital. Without water many daily activities come to a standstill, be it for human consumption or related to power generation and mobile asset operation. Probably the most readily visible interdependency among the four resilience focus areas is how the need for energy or water utilities cuts across all three of the other focus areas—facilities, ICT, and transportation.

External to DHS facilities, public utilities service is highly complicated to manage and under limited control by DHS facility managers. However, facility managers may have full control of onsite energy and water utilities by using, for instance, backup power generators, combined heat and power generators, renewable energy, onsite water wells or cisterns, and onsite water treatment facilities.

4.2 Facilities

In this Framework, the term facilities refers to real property buildings, structures, and land assets. Campuses and individual assets have their own associated unique mission essential functions and business operations, so solutions and projects that may be required to make them fully resilient are likely to be unique to them as well. Resilience should be addressed for both owned and leased facilities where DHS manages facility operations. When DHS and Components may not have direct control over leased facilities where we operate mission essential functions, the status of facility resilience should still be assessed and requirements for resilience should be incorporated into lease agreements where applicable.

4.3 Information and Communication Technology

The critical infrastructure sectors identified in PPD-21 include information technology, which is central to the nation's security, economy, and public health and safety as businesses, governments, academia, and private citizens are increasingly dependent on information technology sector functions. This critical infrastructure sector operates in conjunction with the communications sector, particularly through the internet. ICT encompasses the hardware, software, internal telecommunications infrastructure, programming, and information systems that comprise the assets, networks, and systems under communications and related information technology. The communications sector may include broadcast, cable, satellite, wireless, and wireline. Communication resilience enables personnel who need to request support, assistance, or other services during an incident or in the aftermath. Communication methods can vary, especially during disaster events, from use of technologies such as landline, cellular or satellite phone, IT Satellite Dish for internet, public and private radio, over the air TV, the Postal Service, or simply an assembly area where to meet if communications technologies are not available. Resilience measures need to address both the physical protection and cybersecurity of these ICT related systems, activities, and missions so they are available when and where required. Many DHS ICT systems are dependent on the commercial communications infrastructure, which may be susceptible to damage from natural and man-made disasters, resulting in partial or total loss of data or communications capability. Therefore, Components must be diligent in building resilience into the systems they acquire and operate (See Figure 5).

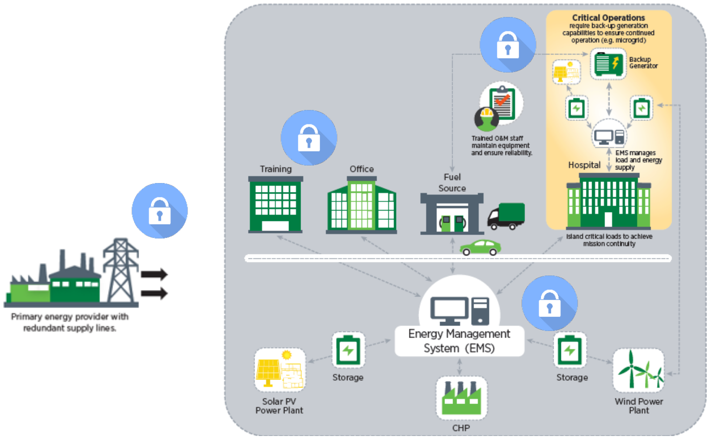

Critical Operations
require back-up generation capabilities to ensure continued operation (e.g. microgrid)
Backup Generator
Trained O&M staff maintain equipment and ensure reliability.
EMS manages load and energy supply
Hospital
Training
Office
Fuel Source
Island critical loads to achieve mission continuity
Primary energy provider with redundant supply lines.
Energy Management System (EMS)
Storage
Storage
Solar PV Power Plant
CHP
Wind Power Plant

Figure 5. Resilience Interdependencies

4.4 Transportation

Transportation includes DHS operated land fleet, air, and marine mobile assets, as well as the public/private transportation infrastructure that, for instance, fuel suppliers use to provide mobile fuels for DHS assets to operate and employees require to commute to work. Dependence on transportation varies by DHS Component, site, local operations, and employee. Therefore, considerations can be wide ranging for transportation resilience solutions necessary to ensure, at least, mission essential functions are sustained.

Mobile assets can be compromised by natural and physical threats, or cyberattacks. Resilient practices should place mobile assets in protected areas, such as above grade away from potential flooding and behind fences to protect them from vandalism. Mobile assets may also be vulnerable to remote cyberattacks through vehicle infotainment systems, telematics, and other network devices. The security measures built into these IT related systems should be verified before they are installed and updates to security patches maintained as needed.

Considerations for transportation resilience solutions need to go beyond thinking only about DHS-operated land, air, and marine vehicles. These considerations might include necessary avenues of travel, such as key roads and bridges that provide access between the site and offsite operations and suppliers; the infrastructure and logistics required to provide an adequate supply of mobile fuels when and where they are needed; and alternative modes of commuting for employees who are needed onsite to guarantee continued site operations or other mission essential functions like search and rescue, or offsite teleworking for those who can work remotely.

Because mobile assets depend on some type of fuel, ensuring access to adequate supplies of clean fuels is a high priority for critical assets. This may include onsite fuel storage, priority contracts with local fuel providers or national fuel suppliers, such as the Defense Logistics Agency (DLA), and reciprocal arrangements with other DHS Components or other Agencies. When one type of mobile fuel is unavailable, dual-fueled vehicles may improve resilience by offering operators the choice between multiple types of fuel at any given time. Resilience planning should consider fueling infrastructure, such as how to pump liquid fuel out of above ground and underground storage tanks or pipeline infrastructure in the event of an electric grid outage and where pumps require electricity. During extreme weather events, stored fuel can become contaminated with water or other elements, so ways to filter out contaminants should also be considered (Figure 5).

Critical infrastructure does not exist in isolation. Due to the various dependencies and interdependencies between infrastructure sectors, a disruption or breakdown in any one area could create cascading effects that impact other areas.

4.5 Resilience Focus Areas Interdependencies

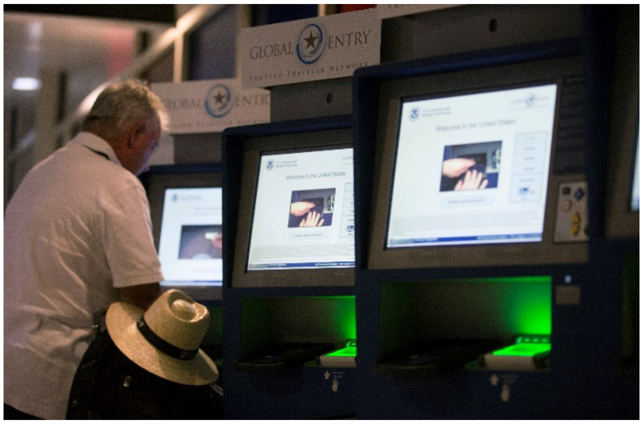
Critical infrastructure does not exist in isolation. Due to the various dependencies and interdependencies between infrastructure sectors, a disruption or breakdown in any one area could create cascading effects that impact other areas. As shown in Table 1, each of the four focus areas is dependent on the other focus areas in some way. Understanding the interdependencies of critical infrastructure assets required to meet mission essential functions and the effects of disruption of these assets are key to the Continuity program and process, and in turn, to developing resilient solutions that ensure sustained mission essential functions. The interdependencies among the four focus areas become clear when considering real-world site or facility applications.

Table 1. Focus Area Interdependencies

		Energy and Water	Facilities	Information and Communication Technology	Transportation
Energy and Water	*Depends on…*	▨	Facilities infrastructure to house monitoring and metering of energy and water utilities.	ICT for data networking and monitoring and systems of energy and water utilities.	Accessible routes and transportation assets to access energy and water service areas.
Facilities		Energy and water utilities for power, heat, and water to critical facility functions.	▨	ICT for data networking and building automation systems to maintain indoor environment quality.	Accessible routes and transportation assets to access critical facilities.
Information and Communication Technology		Energy to power networking elements. ICT is not dependent on water utilities.	Facilities infrastructure to house communication and data network systems.	▨	Accessible routes for ICT professionals to access service equipment.
Transportation		Mobile fuels to power vehicles. Energy to power fueling stations and applicable alternative charging stations. Transportation is not dependent on water utilities.	Facility infrastructure parking areas and barricades to protect mobile assets and access routes.	ICT for physical and cloud communication systems to protect various mobile asset data, systems, and networks.	▨

Energy and water infrastructure can be supplied from offsite utilities or produced onsite with various power generation and water supply (e.g., well, cistern) and treatment plants. Energy and water utilities depend on facility infrastructure to protect energy and water metering equipment and in the case of onsite water or waste water treatment plants, single facilities may be devoted to the function of cleaning water. Energy and water utilities rely on information and communication technology to monitor and manage operations, store and transmit energy data, and communicate system failures or outages. Energy and water infrastructure depends on transportation routes and appropriate vehicles to access and maintain service areas.

Most functions in a building are highly dependent on energy and water systems to operate, such as the heating, ventilation, and air conditioning (HVAC) system, lighting, plug loads, and drinking water and sanitation. Facilities depend on information and communications technologies for data networking, computing, and building automation systems that control indoor HVAC systems. Facilities are also dependent on any routes and transportation modes needed to access the facilities.



Information and communication technology infrastructure depends on energy infrastructure to maintain power and provide its various services; facilities to house the physical ICT assets; and transportation to access critical communication assets, such as communication towers or remote communication facilities.

Transportation infrastructure depends on energy infrastructure to deliver fuels for vehicles and to power fueling station pumps and applicable alternative charging stations. Facilities provide physical protection in the form of parking areas and barriers to prevent vehicle tampering. Information and communication technologies provide physical or cloud communication systems used to communicate and store data from mobile asset systems, such as telematics.

5 RESILIENCE FRAMEWORK PROCESS

Resilience is the ability to adapt to changing conditions and withstand and rapidly recover from disruption. Resilience for both physical and social systems can be conceptualized as having the following four infrastructural qualities.

- *Robustness* is the inherent strength or resistance in a system to withstand external demands without degradation or loss of functionality.
- *Redundancy* is system properties that allow for alternate options, choices, and substitutions under stress.
- *Resourcefulness* is the capacity to mobilize needed resources and services in emergencies.
- *Rapid Recovery* is the speed with which disruption can be overcome and safety, services, and financial stability restored.

Table 2 describes these four resilient qualities with examples related to the technical, organizational, social, and economic dimensions of infrastructure. When determining resilience solutions, these characteristic qualities of resilient infrastructure and systems should be considered.

Table 2. Resilience Qualities with Examples Related to Infrastructure Dimensions

Dimension/Quality	Technical	Organizational	Social	Economic
Robustness	Building codes and construction procedures for new and retrofitted structures	Emergency operations planning	Social vulnerability and degree of community preparedness	Extent of regional economic diversification
Redundancy	Capacity for technical substitutions and "work-arounds"	Alternate sites for managing disaster operations	Availability of housing options for disaster victims	Ability to substitute and conserve needed inputs
Resourcefulness	Availability of equipment and materials for restoration and repair	Capacity to improvise, innovate, and expand operations	Capacity to address human needs	Business and industry capacity to improvise
Rapidity	System downtime, restoration time	Time between impact and early recovery	Time to restore lifeline services	Time to regain capacity, lost revenue

5.1 Resilience Framework Integration of Continuity and Reconstitution

Continuity requirements must be incorporated into the operational activities of all Components to ensure the sustainment of mission essential functions. As highlighted in Federal Continuity Directive (FCD)-1, Federal Executive Branch National Continuity Program and Requirements, there are four phases of continuity implementation: readiness and preparedness, activation, continuity operations, and reconstitution. As depicted in Figure 6, these continuity implementation phases represent the full spectrum of activities during all phases of operation from normal operations, throughout a disaster event, and to recovery.

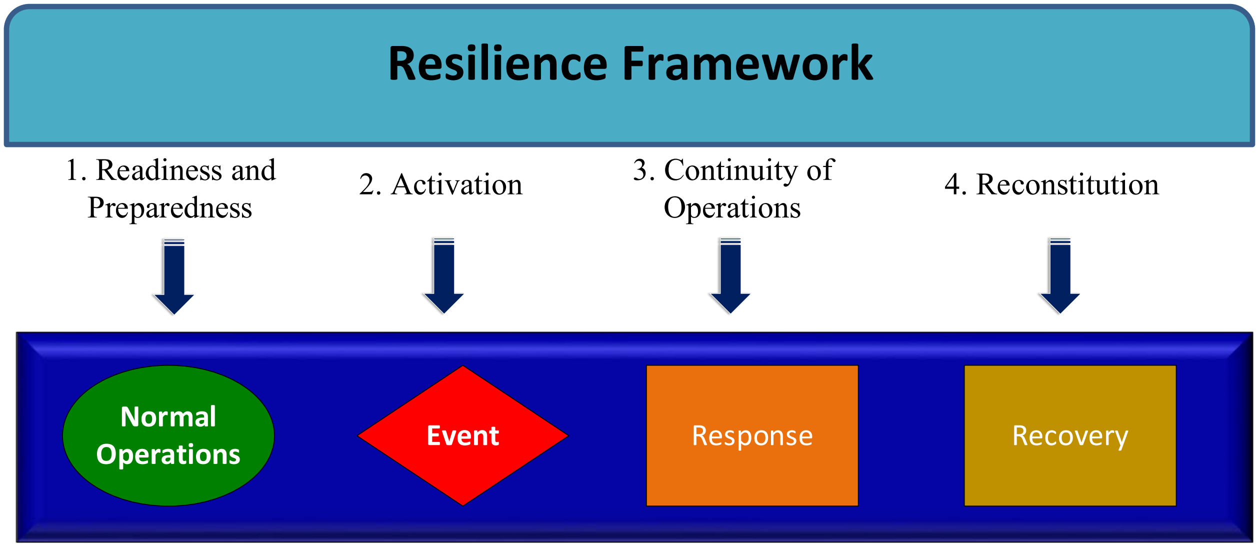


Figure 6. Resilience Phases of Operations/Continuity and Reconstitution Implementation

Readiness and preparedness refers to priority measures taken during normal operations to prepare for, and reduce the effects of disruption to essential functions. This pre-event/threat function primarily consists of the required planning and training necessary to enhance the resilience of continuity mission and to ensure that a viable framework exists to support and facilitate the execution process. During normal operations is the time to perform Continuity processes and analyses and prepare the required Continuity Plan and Reconstitution Plan. This is also the time to implement the Resilience Framework process and prepare the Plan for Resilience to ensure that critical infrastructure that support mission essential functions are sufficiently resilient to maintain those essential functions during hazard and threat events, as well as during normal operations.

Activation focuses on executing the Department's initial response to an event or threat and those actions taken to execute that response according to the Continuity plan.

Continuity operations focus on the commencement of operational activities after emergency response group (ERG) members have arrived at their designated alternate site and/or after designated ERG members begin operating from devolution sites. This phase represents the transition from relocation and/or devolution to continuity operations to ensure continuation of essential functions.

Reconstitution activities focus on the transition of normal operating functions back to the designated primary operating facility according to the Reconstitution plan, or potentially to a temporary replacement operating facility at the conclusion of a continuity or devolution event (once the probability of the event reoccurring does not exist). This last phase of the continuity implementation life cycle involves actions taken to rebuild or restore a critical asset capability after it has been damaged or destroyed. Extensive coordination may be necessary to procure a new operating facility if the complete loss of a facility occurs or in the event that collateral damage from a disaster renders a facility structure unsafe for reoccupation.

The Resilience Framework provides a process that incorporates into steps 2, 3, and 4 the existing processes and analyses for Continuity planning, along with additional processes and analyses to (1) identify potential gaps in the resilience of critical infrastructure to be able to fully support mission essential functions during and after a disruption event, as well as during normal operations, and (2) determine and integrate the resilience solutions and projects necessary to close these gaps (Figure 7).

As the Component stakeholders implement the Resilience Framework process steps, starting with identifying critical mission essential functions and MEAs, the resilience readiness of these assets will begin to be determined, and gaps will be identified. This will lead to solutions and projects that must be implemented to close those gaps and reach a state of full resilience readiness. These activities should answer three essential questions:

- What is critical?
- Is it vulnerable?
- What can be done to make it resilient?

The outcome of these steps will result in development of the Component's Plan for Resilience, as well as the Continuity and Reconstitution Plans. The Resilience Framework's holistic approach will ensure resilience is considered, planned, and incorporated into the performance of critical infrastructure during all phases of operations—normal, event, response, recovery, and mitigation.[14]

[14] The DHS Lexicon (page 112). "Mitigation capabilities include…efforts to improve the resilience of critical infrastructure and key resource lifelines".

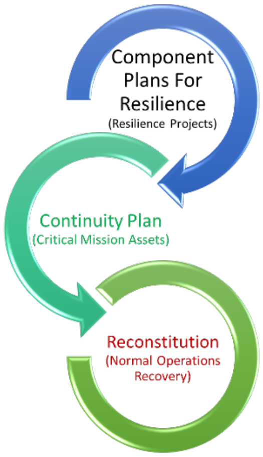

Component Plans For Resilience
(Resilience Projects)
Continuity Plan
(Critical Mission Assets)
Reconstitution
(Normal Operations Recovery)

Figure 7. Holistic Approach to Resilience Planning

5.2 Resilience Readiness Assessment Planning Score

To help assess the current condition of MEAs in terms of their resilience, Component sites must be evaluated across the different systems that support its mission. The resilience readiness assessment planning guide is a set of questions developed by DHS to capture site information and qualitatively score the site's resilience factor—an outcome of scoring continuity, reconstitution, and resilience—assists the Component in determining their resilience readiness. This factor integrates continuity, reconstitution, and resilience processes and solutions that strengthen our systems and assets, properly manages our resources, provides ability to rapidly recover, and implements adaptable processes.

This is generally accomplished with an onsite visit and/or responses to the assessment questionnaire provided by site personnel. The scoring process is applied to each of the four resilience critical infrastructure focus areas. It is advisable to ensure participation in the scoring process of site stakeholders who are knowledgeable about the site's business processes and infrastructure related to each of the focus areas.

Appendix B contains a Baseline Assessment Checklist to help guide Components in executing each step of the Resilience Framework process. This baseline assessment checklist should be initially reviewed to determine the Component's current status with regard to executing the six steps of the process. For instance, currently many or all Components may have already completed their Continuity planning steps as Components should have been implementing Continuity planning for at least the last several years. However, with the aid of the checklist, Components may identify gaps in their existing Continuity planning that should be completed or specific areas of these steps that need to be revisited to ensure the Component has derived all the information necessary to continue with the subsequent Resilience Framework process steps and be able to accurately determine the right resilience solutions required to make the Component sites fully resilient where needed.

The resilience readiness planning assessment categorizes site information and data into four types: process-based information, operational data, geospatial data, and historical data. These categories outline some of the information relevant to each focus area. Interdependencies among the four focus areas, including identifying places where an interruption in one focus area will cause an interruption in other focus areas should also be examined. This information can be used to help establish the baseline condition of the site and identifying the gaps between the current site condition and the site's required resilient state.

Each of the six steps of the Resilience Framework process is shown in Figure 8 and discussed in the following sections. Note that steps 2, 3, and 4 are directly aligned with the existing DHS Continuity planning process and its terminology. This Resilience Framework document provides an overview discussion of the Continuity planning steps. Greater detail for conducting Continuity planning can be found in references cited in Section 2.0 Resilience Drivers.

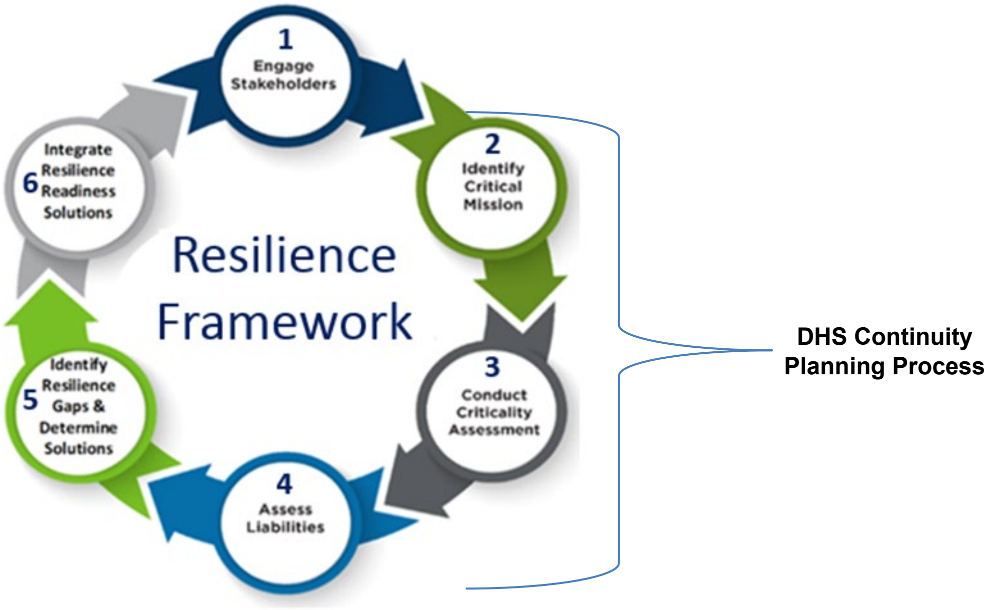
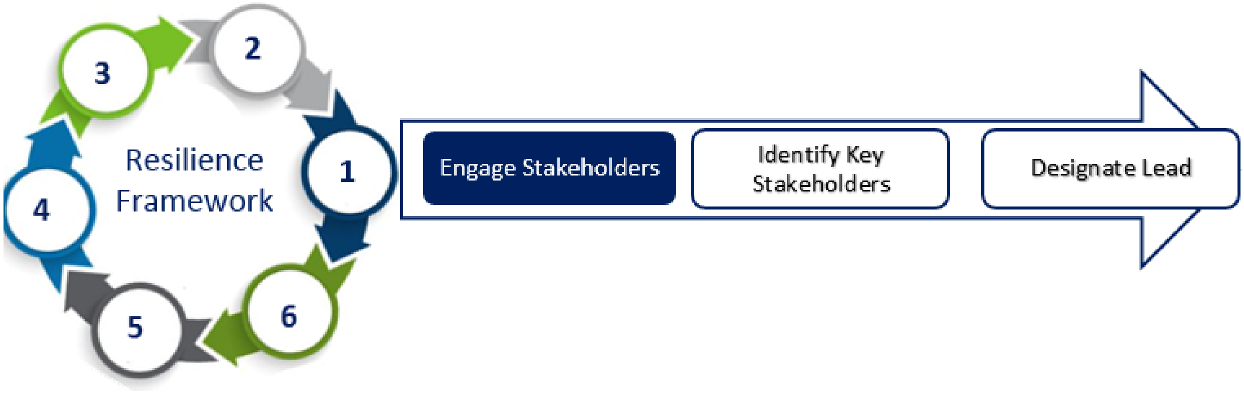

1
Engage Stakeholders
2
Identify Critical Mission
3
Conduct Criticality Assessment
4
Assess Liabilities
5
Identify Resilience Gaps & Determine Solutions
6
Integrate Resilience Readiness Solutions
Resilience Framework
DHS Continuity Planning Process

Figure 8. Six-Step Resilience Framework Process

5.3 STEP 1: ENGAGE STAKEHOLDERS



Planning for resilience requires convening appropriate stakeholders who represent a diverse range of perspectives and expertise on various issues. The number and types of stakeholders may vary depending on the Component mission, geographic location, size, and real property and mobile assets portfolios. It is essential to assemble the right team of stakeholders to implement each step of the Resilience Framework process, so that the appropriate expertise and decision-making authority actively participate when needed. Understanding gaps in stakeholders and filling those gaps accordingly will be essential to the success of the resilience plan. The mix of stakeholders may vary to some extent throughout the Resilience Framework process depending on which step of the process is being implemented and which of the four resilience focus areas is being examined. It should be noted that because of the high degree of interdependencies among the four focus areas, it is advisable that expertise from each focus area participate together throughout the process to help ensure that important interdependencies are not overlooked.

Stakeholders should be engaged to actively participate throughout the process. Assigning tasks to stakeholders and reporting to the team regularly are good ways to get stakeholder buy-in and ownership of the outcome of the planning process, and to maintain communication among the team members. To facilitate stakeholder engagement, Components should carefully select the most appropriate person or persons to lead the stakeholder team in navigating through the entire Resilience Framework process, taking into consideration the leader(s)'s expertise, group facilitation skills, decision-making authority, etc.

Steps 2, 3, and 4 of the Resilience Framework process are equivalent to the established DHS Continuity planning process, namely *Identify Critical Mission, Conduct Criticality Assessment,* and *Assess Liabilities*. Therefore, designating a continuity manager with expertise in Continuity planning to lead the stakeholder team through these steps is a good approach. For Steps 5 and 6, *Identify Resilience Gaps and Determine Resilience Solutions* and *Integrate Resilience Solutions*, the stakeholder team might be led by someone with a different type of expertise, such as

Understanding gaps in stakeholders and filling those gaps accordingly will be essential to the success of the resilience plan.

facility or energy management. If more than one lead is designated and each will be focusing on different steps of the Framework process, it is important that all the leads actively participate as part of the team, start to finish, and collaborate with each other throughout the entire process. This will ensure smooth transition from one step to the next and continuity and integration throughout.

Table 3 lists potential stakeholder roles that should be considered when assembling a stakeholder team to implement the resilience process. Note that this list does not necessarily comprise all possible stakeholders that should be considered. Stakeholders could be drawn from both DHS headquarters and Components, depending on which steps of the Resilience Framework are being implemented and at what level (e.g., individual site, Component portfolio). Additionally, external stakeholders from outside of the Department may also be needed, such as utility service vendors, other local or Federal agency representatives, or technical support contractors.

Table 3. Potential Stakeholders for Resilience Planning

Role	Responsibility
Agency leadership	Supports development of the plan and development of resilience projects
Continuity manager/Point of contact (POC)	Oversees and manages the day-to-day operations of the Component Continuity program
Energy manager	Ensures energy measures are incorporated into resilience plans and actions
Chief Information Officer (CIO)	Exercises responsibility for approval, management, and oversight of information technology systems and assets
Fleet, Air, and Marine Mobile Assets managers	Conducts oversight of the management of DHS activities for mobile assets
Environmental/Sustainability/Environmental Planning managers	Ensures compliance with environmental, sustainability, and environmental planning/historic preservation requirements for assets and functions
Safety and Health manager	Ensures compliance with safety and health requirements for personnel, functions, and assets
Real Property manager / Facility manager	Maintains facility conditions and ensures performance of real property assets (buildings, structures, land); supports maintenance and operations of a specific site and serves as a guide to potential projects
Strategic long-range planners for installations, campuses, buildings	Recognized planning specialist, providing advice on high-level and long-range planning activities, and incorporates resilience measures into new planning
Chief Security Officer (CSO) / Security manager	Supervises, oversees and directs the security program to safeguard Department/Component people, information technology and communication systems, facilities, property, equipment, information, and other material resources
Chief Readiness Support Officer (CRSO) / Chief Administrative Officer (CAO)	Responsible for coordination, policy, and planning of Readiness Support programs and operations across (the Component), including facilities, property, equipment, and other material resources; logistics programs; and environmental programs
Chief Financial Officer (CFO)	Oversees and directs the (Component) budget, appropriations, expenditures of funds, accounting, internal controls, and finances

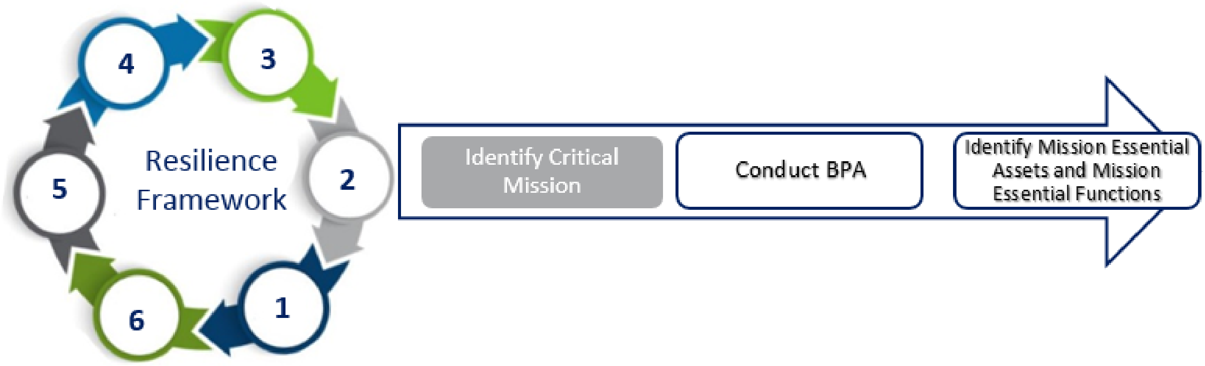
National Protection and Programs Directorate (NPPD) representative	Leads the national effort to protect and enhance the resilience of the nation's physical and cyber infrastructure
OCRSO Systems Information and Integration manager/Component Real and Personal Property Data Management System manager	Provides authoritative real property and mobile asset data and information from DHS Consolidated Asset Portfolio and Sustainability Information System (CAPSIS).[15] If needed can also provide data from the DHS MGMT Cube, such as number of personnel assigned to a site.[16] Components may also use data from their in-house real property data management systems (e.g., TRIRIGA).[17]
Federal Emergency Management Agency (FEMA) representative	Leads recovery and response activities for the Federal government at a national level
Utility manager / service provider	Provides utility services at the site and may provide alternative financing and assistance for projects
Contractors for supplies / delivery	Ensures supplies are delivered during daily operations and could identify potential contingency plans during emergencies
Emergency Management officer	Creates continuity of operations (COOP) plans and response plans for organizations and communities at various levels of government
Local government representatives	Ensures DHS/external partnerships and may enter into agreements to provide mutual aid or benefits during long-term disruptive events
Department of Transportation (DOT) representative	Creates emergency plans and knowledge as applied to resilience opportunities within transportation networks

[15] DHS CAPSIS is the Department's authoritative source for real property data, including building locations, as well as mobile assets data. CAPSIS also provides a geographic information system (GIS) interface that maps all Department real property assets.

[16] DHS MGMT Cube is an integrated data management system with modules from the Offices within the Management Directorate, such as the Chief Readiness Support Officer (CAPSIS module), Chief Financial Officer, Chief Human Capital Officer, etc.

[17] Components using data from their in-house enterprise real property data management systems, such as TRIRIGA, should ensure their data match the authoritative data in CAPSIS.

5.4 Step 2: Identify Critical Mission


4
3
Resilience
Framework
5
2
6
1
Identify Critical Mission
Conduct BPA
Identify Mission Essential Assets and Mission Essential Functions

Because it is crucial to target the right assets for infrastructure protection, determining these assets is the first phase in the Continuity planning and Resilience Framework life cycle. After orienting the stakeholders so they understand the meaning of critical infrastructure, and in particular the four Resilience Framework critical infrastructure focus areas (i.e., energy and water, facilities, information and communication technology, and transportation), the team should be ready to begin Step 2: *Identify Critical Mission*. Critical mission activities and assets are those activities and assets so vital to the Department that their incapacity or destruction would have a debilitating impact on security. Per FCD-2, *Federal Executive Branch National Continuity Program and Requirements*, the Department must identify and prioritize those critical services that must continue during an emergency. The Department must set those priorities as part of its preparedness posture and not wait for a crisis or a continuity event to determine which activities must be sustained throughout the event. This charge to the Department translates to the DHS Continuity planning process and development of the Continuity Plan. *Identifying Critical Mission* is the first step in Continuity planning and incorporated into the Resilience Framework as Step 2 (following Step 1: *Stakeholder Engagement*).

> *Critical mission activities and assets are those activities and assets so vital to the Department that their incapacity or destruction would have a debilitating impact on security.*

Identifying Critical Mission entails using the Business Process Analysis (BPA), outlined in FCD-2, to identify mission essential functions and their associated infrastructure MEAs. This activity will likely be spearheaded by the continuity team lead or manager leading the stakeholder team. The first activity in identifying the critical mission is to identify mission essential functions. A mission essential function enables an organization to provide vital services, exercise civil authority, maintain the safety of the public, and sustain the industrial/economic base during disruption of normal operations.[18] Essential functions are directly related to accomplishing the organization's mission as set forth in statutory or executive charter. Generally, mission essential functions are unique to each organization.[19] The distinction between mission essential and non-essential categories is whether a Component must perform a function or continue to perform the function during a disruption to normal operations or during emergencies. Functions that can be deferred until after an emergency are identified as non-essential (FCD-2).

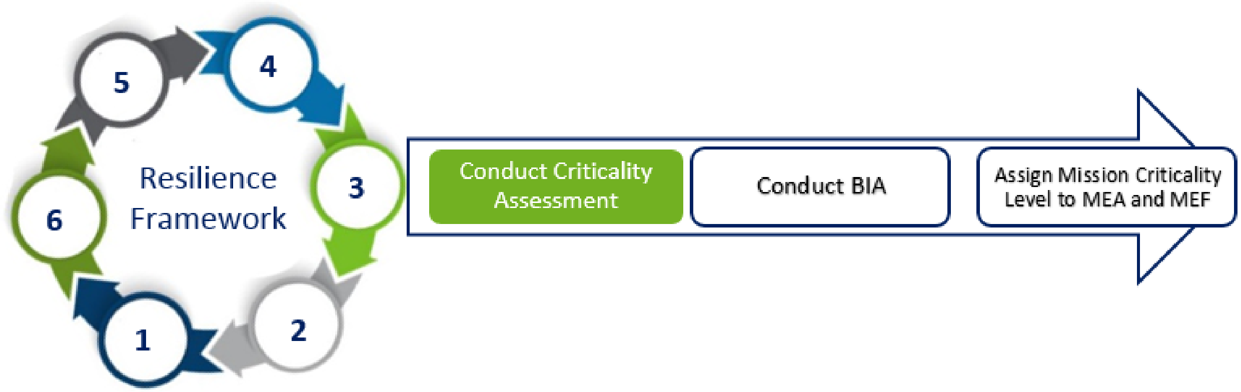
The Component will apply the Business Process Analysis found in FCD-2 to help define its mission essential functions. Business Process Analysis is a systematic method that dissects missions and examines how essential functions are accomplished by identifying and mapping the functional processes, workflows, activities, personnel expertise, systems, data, essential/vital records, facilities, alternate locations for devolution, dependencies, and interdependencies inherent to the execution of the mission essential functions. The outcome of this analysis is a clear understanding of mission essential functions and the associated assets critical to performing those functions. Determining these critical assets is the key and foundation of the six-step Resilience Framework life cycle process, as these assets are the targets for infrastructure protection and resilience. Without this solid foundation, the remaining life cycle steps of the Framework may be flawed, resulting in a Plan for Resilience that fails to protect the appropriate critical infrastructure and therefore, mission assurance.

A key piece of information needed at this step is an accurate list of applicable assets to review. The DHS Consolidated Asset Portfolio and Sustainability Information System (CAPSIS) is the Department's authoritative source for real property data, including building locations. CAPSIS also contains data on the Department's land, air, and marine mobile assets. The CAPSIS geographic information system (GIS) can be a useful tool for mapping asset locations and assessing how they might be impacted based on their geographic relationship to land and water features and other infrastructure, such as roads, electricity transmission, and gas pipelines. The stakeholders are additionally responsible to provide to the team other assessments, processes, and documentation relevant to the critical mission and resilience to include in the Business Process Analysis and help develop a baseline of the current state of the Component's functions, assets, and policies. All DHS essential functions must be supported by a completed Business Process Analysis and Business Impact Analysis (performed in Resilience Framework Step 3) conducted biennially in accordance with FCD-2 and DHS internal processes.

[18] DHS Lexicon, pages 461-462

[19] PPD-40, page 3

5.5 Step 3: Conduct Criticality Assessment



5
4
Resilience Framework
3
6
1
2
Conduct Criticality Assessment
Conduct BIA
Assign Mission Criticality Level to MEA and MEF

Step 3 of the Resilience Framework process is *Conduct Criticality Assessment*. Criticality is the level of "importance to a mission or function, or continuity of operations."[20] A criticality assessment establishes a baseline from which to prioritize projects to improve resilience. It prioritizes mission essential functions and associated MEAs based on consequence factors, thus enabling DHS to use risk-based decision-making on mitigation strategies and resilience requirements. When conducting criticality assessments, it is important to ask key stakeholders the following questions about the asset or function.

- Why is it important?
- What quantitative and qualitative factors will assist in assessing its level of criticality?
- Where does it rank in priority relative to other critical assets and functions?
- How can this asset or function be prioritized for implementing projects at each level of criticality?

A Business Impact Analysis is essential in identifying and prioritizing what is critical to the Department by prioritizing services that must continue during an emergency, as well as during normal operations.

An asset's criticality is a function of both time and situation, based on the asset's operational or business value. Value depends on several factors. First is what mission essential functions rely on an asset and how those dependencies change across time. Second is how sensitive the functional operation is to the loss or compromise of the asset; in other words, what is the maximum allowable downtime if the asset is compromised. Finally is whether the asset can be restored after an interruption or if a switch to a backup can be made within the allowable downtime.

A Business Impact Analysis (BIA) is essential in identifying and prioritizing what is critical to the Department by prioritizing services that must continue during an emergency, as well as during normal operations. Business Impact Analysis is a method of identifying the potential negative impacts of failing to perform an essential function through quantitative and qualitative assessments of continuity

[20] DHS Lexicon, 2016 Edition, page 114

criticality. It determines the consequence of loss of essential functions, assets, and systems that are critical in supporting the execution of mission essential functions. Further, it requires the application of organization-wide risk analysis to inform decision making and strengthen operations through effective risk management. The results of Business Impact Analysis, integrated with intelligence and threat reporting, inform risk management activities to ensure the continued performance of essential functions. A Business Impact Analysis supports the risk analysis and risk management of the essential functions, essential supporting activities, and supporting internal critical infrastructure previously identified in the Business Process Analysis.

Business Impact Analysis provides the scoring of DHS "mission criticality levels." Part of the purpose in conducting a Business Impact Analysis is to plan, prepare, and respond to any kind of threat, by identifying the criticality levels and resiliency of various systems and assets. In order to do this, a Component should:

- Identify the potential impacts on the performance of essential functions and MEAs from a disruptive event.
- Enable assessments of DHS's critical dependencies on the Homeland Security Enterprise and critical infrastructure sectors.

The Department's Business Impact Analysis provides scoring metrics to assess the criticality of MEAs and functions (Table 4). Scores are based on the consequence of loss or disruption over an extended period. Higher values indicate greater impact on the successful execution of mission essential functions, or greater consequence of loss. A Continuity Criticality Level 4 has greater impact on the Department's ability to execute its mission essential functions, and has a greater consequence of loss, than a Continuity Criticality Level 1.

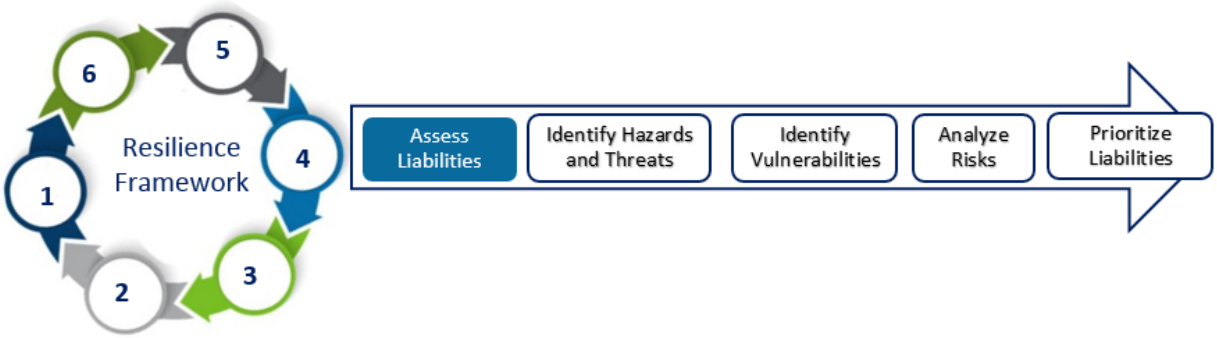
Table 4. Continuity Criticality Quantitative Scoring Definitions (Table D-2 from FCD-2)

Continuity Criticality Level 4	**Very high consequence**—Loss or disruption of the asset or function has exceptionally grave consequences; such as extensive loss of life, widespread severe injuries, and total loss of primary services, core functions, and processes.
Continuity Criticality Level 3	**High consequence**—Loss or disruption of the asset or function has grave consequences; such as loss of life, severe injuries, loss of primary services, and major loss of core processes and functions for an extended period.
Continuity Criticality Level 2	**Medium consequence**—Loss or disruption of the asset or function has moderate to serious consequences; such as injuries or impairment of core functions and processes.
Continuity Criticality Level 1	**Low consequence**—Loss or disruption of the asset or function has minor consequences or impact; such as a slight impact on core functions and processes for a short period of time.

When prioritizing the need for and implementation of resilience solutions and projects, first consideration should be given to addressing those associated with mission essential functions and assets falling into Continuity Criticality Level 4. Furthermore, as discussed in Section 4.5, interdependencies among critical infrastructure MEAs can produce significant cascading impacts across the assets. That is why it is important to perform dependency analysis to map functions and relationships among the critical assets. As a result of the dependency analysis, the criticality attributes for previously identified assets may be updated and additional critical assets may be identified. Tools and resources to help with prioritization include:

- Essential Function and Mission Essential Asset Qualitative and Quantitative scoring;
- The "Prioritized" Classified DHS Mission Essential Asset List;
- Continuity criticality levels for each MEA list; and
- Assessment of essential function dependencies through the Continuity Dependency Analysis.

5.6 Step 4: Assess Liabilities



For critical infrastructure protection, risk management requires leveraging resources to address the most critical infrastructure assets that are also the most vulnerable and that have the greatest threat exposure. In Step 4: *Assess Liabilities*, the Component identifies the hazards, threats, risks, and vulnerabilities of the critical MEAs. The end goal of assessing liabilities is to determine the level of risk that exists under each critical infrastructure focus area. The level of risk is a function of the threat that exists, combined with the vulnerability to the threat, taking into account the consequence of the action and impact on mission. Based on a comprehensive risk assessment and risk management, the Component should understand what can happen (hazards and outcomes), the likelihood of it happening (the combined probability of hazards and vulnerabilities), and the consequences if it does happen (severity of outcomes).

Liabilities should be evaluated based on the degree of mission impact and the extent to which a liability will cause interruption. Evaluators should refer back to the four critical infrastructure focus areas and determine how a liability will affect each focus area independently, as well as how a liability in one focus area will affect other focus areas due to their interdependencies. For each Component and site, a comprehensive evaluation must be performed to determine the unique threats that exist, and how these may have an impact on the mission of the facility.

The Business Process Analysis and Business Impact Analysis, conducted as part of the Component’s Continuity of Operations program, are used to support risk assessment and are integrated into the Department's Enterprise Risk Management processes. These analyses aid in identifying obvious and non-obvious, emerging, and future risks or threats to an organization’s operations. As an end result, structured and in-depth analysis enables organizations to consider and allocate resources to those areas of greatest risk and where the most benefit from investment may be achieved.

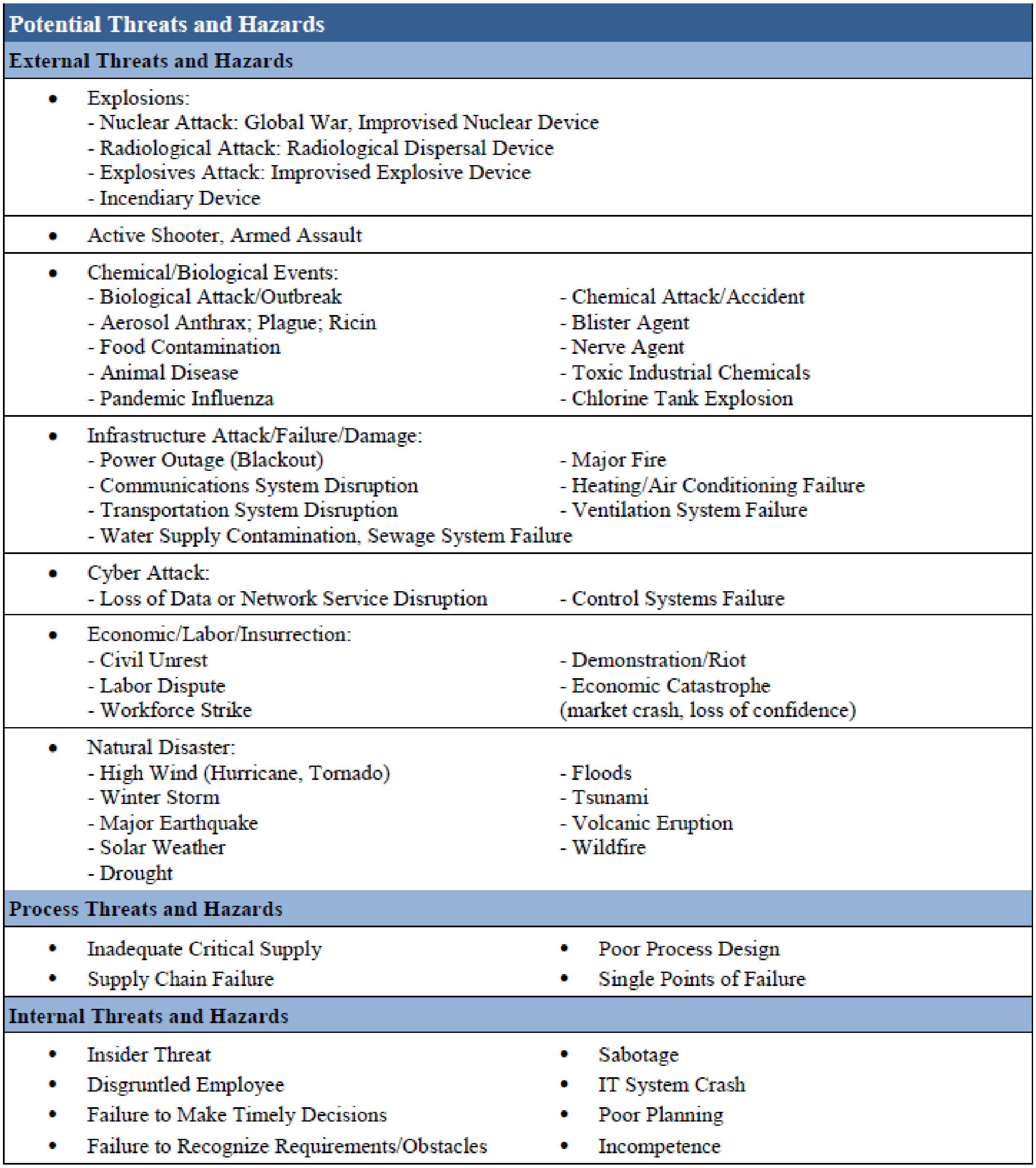
5.6.1 Ascertain Hazards and Threats

The Federal Emergency Management Agency (FEMA) generally organizes hazards into three main categories: natural, technological, and human-caused. Natural hazards result from acts of nature, severe weather, or changes in climate (e.g., increased precipitation, increased intensity, increases in temperature). Technological hazards, also referred to as infrastructure hazards, result from accidents or the failures of systems and structures. Examples of common technological hazards include power disruptions or outages, and roadway or bridge failures. Human-caused hazards are threats or intentional actions of an adversary, such as acts of terror and cyberattacks. The process for identifying and addressing many of the aforementioned hazards is similar. Taking an all-hazards approach to resilience planning will help Components become much more robust and assist with reacting to and withstanding events of many different types. For example, extreme weather (natural hazard) is the leading cause of power outages (technological hazard) in the United States and cyberattacks (human caused) to communication infrastructure may hamper recovery efforts after major weather events or power outages. Identifying solutions to address one type of hazard may apply to all three types. It is most effective to address all hazards when conducting resilience planning as focusing on one set of hazards may not enhance resilience as a whole.

Liabilities should be evaluated based on the degree of mission impact and the extent to which a liability will cause interruption.

Table 5 shows the potential threats and hazards from FCD-2.

Table 5. Potential Threats and Hazards (Table D-1 from FCD 2)



Potential Threats and Hazards	
External Threats and Hazards	
• Explosions: - Nuclear Attack: Global War, Improvised Nuclear Device - Radiological Attack: Radiological Dispersal Device - Explosives Attack: Improvised Explosive Device - Incendiary Device	
• Active Shooter, Armed Assault	
• Chemical/Biological Events: - Biological Attack/Outbreak - Aerosol Anthrax; Plague; Ricin - Food Contamination - Animal Disease - Pandemic Influenza	- Chemical Attack/Accident - Blister Agent - Nerve Agent - Toxic Industrial Chemicals - Chlorine Tank Explosion
• Infrastructure Attack/Failure/Damage: - Power Outage (Blackout) - Communications System Disruption - Transportation System Disruption - Water Supply Contamination, Sewage System Failure	- Major Fire - Heating/Air Conditioning Failure - Ventilation System Failure
• Cyber Attack: - Loss of Data or Network Service Disruption	- Control Systems Failure
• Economic/Labor/Insurrection: - Civil Unrest - Labor Dispute - Workforce Strike	- Demonstration/Riot - Economic Catastrophe (market crash, loss of confidence)
• Natural Disaster: - High Wind (Hurricane, Tornado) - Winter Storm - Major Earthquake - Solar Weather - Drought	- Floods - Tsunami - Volcanic Eruption - Wildfire
Process Threats and Hazards	
• Inadequate Critical Supply • Supply Chain Failure	• Poor Process Design • Single Points of Failure
Internal Threats and Hazards	
• Insider Threat • Disgruntled Employee • Failure to Make Timely Decisions • Failure to Recognize Requirements/Obstacles	• Sabotage • IT System Crash • Poor Planning • Incompetence

Identifying top risks to Component infrastructure supports the determination and prioritization of resilience solutions and projects. As Components conduct and coordinate assessments of risk to essential functions, they can leverage other potential sources of risk assessment information that may provide useful information for the locales the Components are assessing. These sources might include National Threat and Risk Assessments, Regional Threat and Hazard Identification and Risk Assessment

(THIRA), and the Stakeholder Preparedness Review (SPR), as well as the DHS Regional Resilience Assessment Program (RRAP).[21] Components can obtain a copy of the most up to date THIRA and SPR that has been developed if it covers the location the Component is considering and use the document to direct their efforts into where threats and hazards have been identified (reach out to FEMA-SPR@fema.dhs.gov for access). Note that according to FEMA-SPR, "*The Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) are submitted by Homeland Security Grant Program (HSGP) grantees, including Urban Area Security Initiative (UASI) and Tribal Homeland Security Grant Program (THSGP) grantees each year. This means that we have THIRA data from states, territories, UASI grantees, and THSGP grantees, and SPR data for states and territories. We do not have access to THIRA/SPR submissions from more specific locations".*

The THIRA process helps communities understand the normal set of risks they face. By identifying and prioritizing those threats, a community can make smarter decisions and manage the risks through appropriate planning, mitigation strategies, and developing needed capabilities. The steps of the THIRA process entail:

1. **Identify Threats and Hazards of Concern:** Based on a combination of experience, forecasting, subject matter expertise, and other available resources, identify a list of the threats and hazards of primary concern to the community.
2. **Give the Threats and Hazards Context:** Describe the threats and hazards of concern, showing how they may affect the community.
3. **Establish Capability Targets:** Assess each threat and hazard in context to develop a specific capability target for each core capability identified in the National Preparedness Goal. The capability target defines success for the capability. The five core capability areas include: planning, organization, equipment, training, and exercises.
4. **Apply the Results:** For each core capability, estimate the resources required to achieve the capability targets through the use of community assets and mutual aid, while also considering preparedness activities, including mitigation opportunities.

The State Preparedness Report is a self-assessment of a jurisdiction's current capability levels against the capability targets it identified in the THIRA. The report supports the National Preparedness System by helping to identify state and territory preparedness capability gaps. States, territories, and the Federal Government use this information to help make programmatic decisions to build and sustain capabilities, plan to deliver capabilities, and validate capabilities. Jurisdictions assess their preparedness levels in each of the five core capability solution areas: planning, organization, equipment, training, and exercises. States and territories use a five-point scale for each assessment, where one (1) indicates little-to-no capability, and five (5) indicates they have all or nearly all of the capability required to meet their

[21] The Regional Resiliency Assessment Program (RRAP) is a DHS program which offers a "cooperative assessment of specific critical infrastructure within a designated geographic area and a regional analysis of the surrounding infrastructure to address a range of infrastructure resilience issues that could have regionally and nationally significant consequences." The RRAP projects are voluntary and led by DHS, selected each year by DHS, with input from federal, state, and local partners. The goal of the RRAP is to generate greater understanding and action among public and private sector partners to improve the resilience of a region's critical infrastructure. For more information visit: https://www.dhs.gov/regional-resiliency-assessment-program. As a point of clarification, NPPD does not make a blanket offering to perform RRAP projects for DHS sites as the purpose of the RRAP is not inwardly (i.e., DHS) focused. However, NPPD recommends Components take advantage of any applicable past work.

targets. States and territories also provide context for their assessments. Respondents assign a low, medium, or high relative priority level to each core capability based on its impact on preparedness, and the degree to which respondents plan to build and/or sustain the capability in the near-term. In cases where their current preparedness levels fall short of their targets, states and territories explain the specific improvements they would need to address the capability gaps in their jurisdictions. In addition, states and territories provide their perceptions of the Federal Government's role for filling capability gaps in the future. The outputs of this process inform a variety of emergency management efforts, including emergency operations planning, mutual aid agreements, and hazard mitigation planning.

If THIRA has not been performed for a site the Component is considering, use the FEMA-developed THIRA framework to conduct the four-step, common risk assessment process that helps the whole community[22] and leverage regional and local partners to stay up to date on evolving threats in the local area. Other local and regional organizations in the area may have published or institutional knowledge of hazards. Becoming involved with local trade organizations and opening lines of communication with other facilities is a good way to keep abreast of threats and hazards.

There is also an alternative effects-based approach that is hazard agnostic, wherein you begin with a disruptive event that will have an impacts on facility operations (e.g., loss of power, loss of water service, loss of communications). Once you have identified all of the ways in which facility functions could be disrupted, you then work backwards to consider what events could cause those disruptions—the hazard scenarios. In this case, you mainly plan for dealing with the impact of the disruption, with some unique tailoring as needed to account for the one or many hazards that might cause it. This process often identifies disruptive scenarios, such as labor strikes at ports that disrupt operations, fuel shortages, and supply chain disruptions. These types of hazards do not often come to mind when people think about typical hazards, such as storms, fires, and cyberattacks. FEMA planning guidance may offer some useful discussion as FEMA has a well-established process and understanding about the value and pitfalls of scenario based planning.

5.6.2 Identify Vulnerabilities and Risks

Vulnerabilities are defined as Component and site exposure to the possibility of harm. A general rule of thumb for remembering the differences between hazards and vulnerabilities is that hazards are typically not within a Component's control, but vulnerabilities could be within a Component's control. The vulnerabilities that arise in the risk assessment are the starting point for identifying resilience solutions.

Examples of vulnerabilities that may occur at a site include: a single electricity or water supply to a facility or campus; a single point of access to a facility or campus such as one road or bridge; drainage

[22] https://www.fema.gov/threat-and-hazard-identification-and-risk-assessment and https://www.fema.gov/media-library-data/8ca0a9e54dc8b037a55b402b2a269e94/CPG201_htirag_2nd_edition.pdf

challenges causing flooding or pooling, for instance as a result of the physical landscape and infrastructure; and the relationship of the geographic location to natural disasters, such as coastal storms, tornados, or forest fires.

5.6.3 Maximum Tolerable Downtime for Mission Sustainment

When assessing overall liabilities from hazards, threats, risks, and vulnerabilities, consideration should be given to the sustainability of potential solutions (e.g., renewable backup power vs. fossil fuel generation); duration of outage, which can be unique to each site or mission; and the interdependencies among the critical infrastructure focus areas. For instance, hazards and threats can impact the delivery of resources to conduct the mission, such as interruption of energy or water supplies. The Component needs to determine what is the maximum tolerable downtime for interruption of the specific mission essential functions performed at its sites. This downtime threshold can be used as a basis for determining how vulnerable is the site to exceed the threshold during a hazard event and what resilience solutions and projects might be necessary to ensure the actual downtime will not exceed the threshold. This might translate into the amount of time the Component needs to be able to store sufficient energy or water resources for the site to sustain mission essential functions during a hazard event. As an example, U.S. Army Directive 2017-07, *Installation Energy and Water Security Policy* established requirements for Army installations to provide necessary energy and water for a minimum of 14 days for critical missions.[23] Setting an appropriate maximum tolerable downtime for mission sustainment is an exercise in understanding the threats at the site and its critical functions. Components should coordinate across focus areas and with Continuity Plans to understand their mission sustainment needs (See Figure 9).

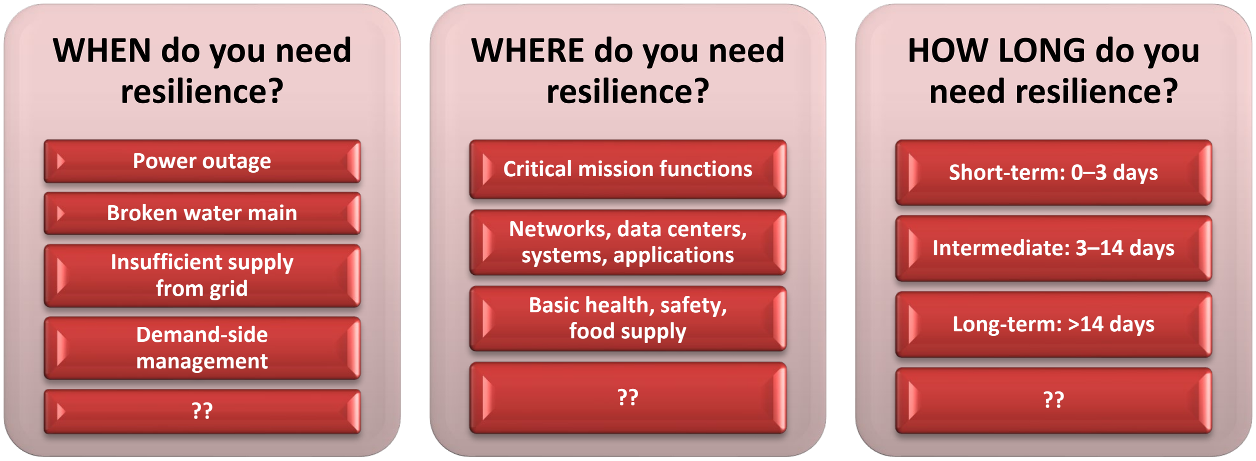
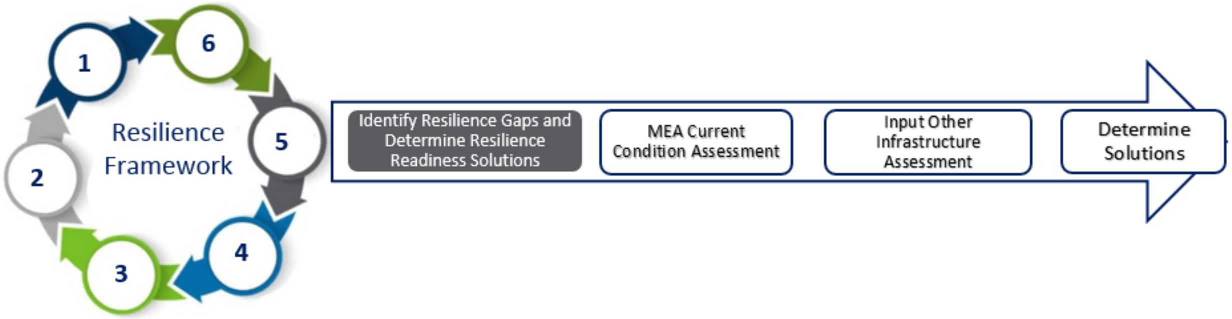

WHEN do you need resilience?
Power outage
Broken water main
Insufficient supply from grid
Demand-side management
??
WHERE do you need resilience?
Critical mission functions
Networks, data centers, systems, applications
Basic health, safety, food supply
??
HOW LONG do you need resilience?
Short-term: 0–3 days
Intermediate: 3–14 days
Long-term: >14 days
??

Figure 9. Resilience Criticality

[23] http://www.asaie.army.mil/Public/ES/doc/Army_Directive_2017-07.pdf

5.7 Step 5: Identify Resilience Gaps and Determine Resilience Readiness Solutions


1
6
Resilience
Framework
5
2
4
3
Identify Resilience Gaps and Determine Resilience Readiness Solutions
MEA Current Condition Assessment
Input Other Infrastructure Assessment
Determine Solutions

Step 5: *Identify Resilience Gaps and Determine Resilience Readiness Solutions* identifies the difference, or gap, between the current baseline conditions of a Component site and the conditions that would make the MEAs sufficiently resilient to maintain mission essential functions during and after a hazard or threat event, as well as during normal operations. Based upon identified gaps, the Component should determine the solutions and projects necessary to close the gaps and ensure that critical MEAs can support mission essential functions without loss beyond their maximum tolerable downtime during all phases of site operations. When determining resilience solutions, Components should consider the resilience qualities of infrastructure discussed in Section 5.0, namely robustness, redundancy, resourcefulness, and rapid recovery.

For critical infrastructure protection, risk management requires leveraging resources to address the most critical infrastructure assets that are also the most vulnerable and that have the greatest threat exposure. As Steps 1 through 4 of the Resilience Framework process are completed and mission essential functions and MEAs are defined and prioritized based on their levels of criticality and their associated liabilities, the gaps in resilience readiness of these assets should start to become apparent. Discussed in this section are additional considerations and tools to help identify resilience gaps and from these, determine solutions to improve the resilience of the Component critical MEAs.

5.7.1 Determining Resilience Readiness Solutions

Impacts on MEAs can be addressed via four generally characterized responses. These categories of responses are aligned with the four phases of site operations according to whether the responses are implemented during normal operations, during an event, or after an event.

- **Remediation (normal operations):** Remediation involves precautionary measures and actions taken before an event occurs to fix the known physical and cybersecurity vulnerabilities that could cause an outage or compromise a critical MEA. For example, remediation actions may include education and awareness, operational process or procedural changes, system configuration change, and infrastructure asset modifications.
- **Mitigation (normal operations and during an event):** Mitigation comprises preplanned coordinated actions in response to infrastructure warnings or incidents. These actions are designed to minimize the operational impact of the loss of a critical asset, facilitate incident response, and quickly restore the infrastructure service.

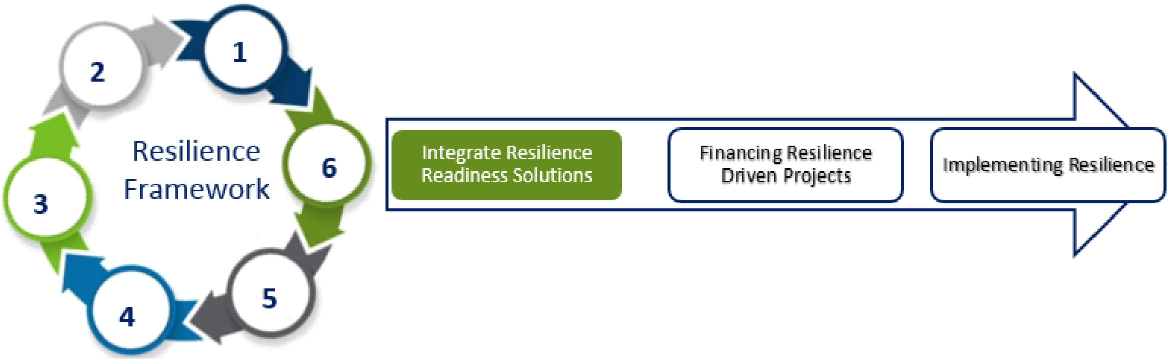
- **Incident Response (after an event):** Incident response comprises the plans and activities taken to eliminate the cause or source of an infrastructure event.
- **Reconstitution (after an event):** Reconstitution involves actions taken to rebuild or restore a critical asset capability after it has been damaged or destroyed.

Identification of resilience solutions and projects could arise out of any or all these response categories, based on the gaps between the MEAs' liabilities and their required resilience state. For instance, the gaps could be in policy, documentation, business process change, or physical projects. Experience and lessons learned during all phases of operations should help inform Components about the resilience solutions and projects they need to incorporate into their Plans for Resilience, which are generally prepared during normal operations. The better the planning and implementation of resilience solutions and projects during normal operations, the less likely will be the extent and need for mitigation, incident response, and reconstitution responses when a hazard or threat event occurs.

The purpose of resilience solutions is to improve the reliability, availability, and survivability of critical assets and infrastructures. Generally, these resilience solutions should also enhance the efficiency of site operations during the normal operations phase as well. For instance, energy demand load management systems should help reduce site energy use and costs during normal operations, as well as enhance the capability to allocate power to the most needed critical assets during a hazard or threat event. Site staff should be encouraged to integrate resilience as part of ongoing facility operations and maintenance, such as eliminating single points of failure. Tabletop exercises can be used to think through the order of operations and emergency duties to which different maintenance staff should be assigned.

If not already considered in the existing Continuity liabilities assessment, experience with past hazard and threat events should provide insight into where resilience solutions are needed. For instance, in the aftermath of the 2017 hurricane season, many lessons were learned based on the devastation of critical infrastructure and the difficult issues involved in reconstitution. Rather than building back to the former status quo, many opportunities to build back for resilience became evident. Components should also consider the results of other assessments performed during normal operations to help evaluate the current site conditions with regard to resilience. These assessments may include facility energy and water audits, commissioning, and recommissioning, facility sustainability assessments, and facility condition assessments. Similar assessments of information and communication technology infrastructure should also be viewed. Additionally, Physical and Vulnerability Assessments produce a scope of projects needed to comply with security requirements. These existing assessments can provide a wealth of information about site conditions and identified projects with opportunity for savings in energy and water use/cost and strengthening facility infrastructure. These projects should be examined for potential alignment with the liabilities assessment to help determine which can provide the best return on resilience, as well as economic return on investment.

5.8 Step 6: Integrate Resilience Readiness Solutions


1
2
3
4
5
6
Resilience Framework
Integrate Resilience Readiness Solutions
Financing Resilience Driven Projects
Implementing Resilience

Step 6: *Integrate Resilience Readiness Solutions* will close the gaps between the current state and a resilient state of critical MEAs to ensure continuous performance of critical mission essential functions as needed during times of hazard or threat disruption, as well as during normal operations. While prioritizing individual resilience solutions and projects for greatest impact and effectiveness, consider what is achievable and the following attributes:

- Responsiveness to the scale and impact of likely hazards and vulnerabilities;
- Ability to meet identified performance goals for resilient infrastructure systems and critical operations;
- Ability to address and strengthen interdependent infrastructure systems;
- Co-location opportunities to further the mission set;
- How to obtain and execute funding to implement capital projects or institutionalize resilience into existing activities;
- Administrative capacity necessary for implementation;
- Data and analysis required for implementation; and
- Implementation plan requirements.

A successful approach to resilience must integrate resilience considerations into normal site operations and identify opportunities to implement resilience projects as part of capital improvements. Often, resilience considerations can be incorporated into capital projects at little or no additional cost. Following are examples where resilience may be added into projects at potentially little to no cost:

- Spreading fleet vehicle parking across a site rather than in a single area where the vehicles could be vulnerable to a single event;
- Designing a facility with passive cooling features rather than relying on mechanical cooling;
- Laying out the electrical panel of a facility such that critical circuits are grouped together; and

- Installing values on heating and cooling equipment that allows for machines to be isolated in the event of a failure.

Integrating resilience readiness into all phases of operations requires Components to shift their focus toward prioritizing resilience as the main driver for a number of site assessment, planning, and implementation activities compared to those done in the past across DHS. For example, facility energy audits are traditionally performed to identify energy conservation measures (ECMs) that are driven by energy efficiency (i.e., reducing energy use and costs per gross square foot) and increasing use of renewable energy to replace fossil fuel use and consequently, reduce greenhouse gas emissions. Emphasizing energy resiliency would place more focus on ECMs that will help ensure uninterruptable power during electric grid outages, for instance by using backup generators, combined heat and power, or onsite renewable energy sources. When insufficient power is available to maintain the entire site, enhancing the ability to island the most critical MEAs on the site using a microgrid system might be the best resilience solution, although a microgrid may or may not directly result in energy savings during normal operations. Similarly, past facility condition assessments may have been geared toward identifying projects and repairs that maintain the status quo of facility functions under normal operating conditions, rather than identifying what modifications are necessary to ensure they can support mission essential functions during all phases of operations, especially during hazard events. Since Components are already implementing energy/water assessments on a regular four-year cycle for their EISA covered facilities, [24] Components should consider ensuring their critical MEAs, as identified through execution of the Resilience Framework process, are included in their covered facilities list so they are assessed on a regular basis as part of their covered facilities auditing program.

5.8.1 Financing Resilience-Driven Projects

Resilience requirements need to become a primary driving force for Department-wide project planning and implementation to assure sustained DHS critical mission essential functions. Once potential resilience readiness solutions have been identified and prioritized, these solutions should be integrated to the maximum extent feasible into the Component's project life cycle planning and budgeting. Consequently, senior DHS and Component leadership need to commit to resilience as a Department-wide policy to ensure support for these projects in the budgeting process.

Resilience requirements need to become a primary driving force for Department-wide project planning and implementation to assure sustained DHS critical mission essential functions.

Financing a resilience project involves identifying feasible funding authorities and procurement strategies. Resilience projects can be funded directly through government budget appropriations. Where appropriations are not available, alternative funding approaches such as public-private partnerships should be considered. For energy and water projects, alternative third-party financing strategies are a proven cost-effective procurement pathway. There are several procurement

[24] Energy Independence and Security Act (EISA) of 2007, Section 432 directs each Federal Agency to identify a list of covered facilities that constitutes at least 75% of the Agency's annual electricity use. An energy and water assessment must be performed on each of these covered facilities at least once every four years to identify ECMs to improve their energy and water use performance.

mechanisms available for third-party financing of energy or water projects. The three most widely used are: energy savings performance contracts (ESPCs), utility energy savings contracts (UESCs), and power purchase agreements (PPAs) for energy generation projects.

Investment in resilience driven projects may present a problem in some cases where alternative third-party financed contracts are needed to implement these projects due to insufficient available appropriations. Under third-party financed contracts, vendors providing the upfront financing will implement only those projects that can provide a positive dollar return on investment. Some resilience focused projects may not result in the positive return on investment required by the vendor, even though the project may provide a high return on resilience for the Department. In these cases, the Component may need to bundle the low or non-payback resilience driven project with other energy and water saving projects to make the bundled projects economically attractive to a third-party financing vendor. To the extent possible, the Component may also need to supplement the alternative finance contract with appropriations to help balance the return on investment required by the vendor.

Where feasible, Components should also identify profitable value streams for energy resilience investments. Value streams may include grant programs, monetary savings during normal operations, energy security, and avoided outage costs. Examples of common value streams include federal, state, and local incentives, peak shaving, time-of-use shifting, demand response programs, and aggregated green energy procurement. Due to the flexibility of some microgrid designs to provide a variety of grid services, “stacking” these value streams is a key strategy to improve the energy project’s economic feasibility.

5.8.2 Implementing Resilience at Leased Facilities

The facilities portfolios of most DHS Components include leased facilities where they operate and perform critical mission essential functions. In many leased facilities, particularly for full service leases, the Component may have little or no control of the day-to-day management of the facilities. Regardless of whether the facilities are DHS owned or leased, the critical infrastructure at facilities where mission essential functions are performed must be sufficiently resilient to maintain those functions during hazard and threat events, as well as during normal operations. Components are required to implement Continuity planning business processes and analyses for their leased facilities. The remaining steps of the Resilience Framework process (i.e., identify resilience gaps and determine and implement resilience solutions) will also need to be conducted, but the Component may need to do this in coordination with the facility owner. Components should also incorporate into their leasing agreements clauses that require the landlord to ensure resilient critical infrastructure is delivered that will meet the requirements for DHS mission essential functions. These kinds of lease clauses may be similar to those that require leased facilities over a certain size to be sustainable or meet Energy Star performance standards.

6 COMPONENT PLANS FOR RESILIENCE

Each DHS Component is required to prepare its Plan for Resilience, due one year after issuance of this Resilience Framework document. Thereafter, Components should annually review their Plans for Resilience and update them accordingly. The Plan for Resilience should be consistent with the Component's Continuity Plan and Reconstitution Plan.

A guiding template for the Component Plan for Resilience will be issued by DHS separate from this Resilience Framework document. It is understood that Components are diverse in mission and organization, and each faces a set of unique challenges. Therefore, each Component's Plan for Resilience will reflect its own mission, processes, geography, and capacity. However, these plans should show the prioritization of Component critical MEAs, solutions and projects required to make these assets resilient, the priorities for funding to implement these resilience solutions and projects, and overall pathways for implementing the resilience solutions and projects.

7 Conclusion

In the face of ongoing natural, physical, and man-made hazards and threats, it is imperative that resilience is fully integrated into all phases of mission essential operations across the Department. DHS and Components must deliberately plan for and implement resilience solutions to protect infrastructure critical to supporting their mission essential functions. The DHS Resilience Framework was formulated as a holistic process to meet this requirement by integrating resilience into the entire life cycle of planning and implementation of mission operations. Implementing the Resilience Framework process will greatly facilitate the Department-wide ability to prepare for and adapt to changing conditions and rapidly recover from disruption of normal operating conditions when and where they occur. The resulting Component Plans will provide a resilience driven basis for informed and sound decision making and ensure incorporation of resilience priorities into DHS' long-term planning and budgeting processes.

Implementing the Resilience Framework process will facilitate the Department-wide ability to prepare for and adapt to changing conditions and rapidly recover from disruption of normal operating conditions when and where they occur.

8 CONTACTS

8.1 DHS ENERGY MANAGEMENT STAFF

U.S. Department of Homeland Security
Management Directorate, OCRSO, Sustainability and Environmental Programs (SEP)
M/S 0075
650 Massachusetts Avenue, NW
Washington, DC 20528-0075

Dr. Teresa Pohlman, Executive Director
DHS Sustainability & Environmental Programs
teresa.pohlman@hq.dhs.gov

Crystall Merlino, LEED Green Associate
DHS Energy Program Manager
crystall.merlino@hq.dhs.gov

Joseph Anello
Manager, Wind Farm Policy
joseph.anello@hq.dhs.gov

Joyce (Marie) Britt, P.E., CEM
Energy Management Engineer
joyce.britt@hq.dhs.gov

Patricia Harrington, Ph.D., LEED AP, Registered Environmental Manager
Energy Program Analyst
patricia.harrington@hq.dhs.gov

APPENDIX A: GLOSSARY OF TERMS

Term	Definition
Asset	Person, structure, facility, information, material, or process that has value (Lexicon page 49).
Business Impact Analysis (BIA)	A method of identifying the consequences of failing to perform a function or requirement.
Business Process Analysis (BPA)	A method of examining, identifying, and mapping the functional processes, workflows, activities, personnel expertise, systems, data, interdependencies, and facilities inherent in the execution of a function or requirement.
Critical Infrastructure	Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of those matters, across any federal, state, regional, territorial, or local jurisdiction (Lexicon pages 161-162).
Energy and Water Resilience	Maintaining a continuous power and water supply, and enabling energy and water systems to adapt to changing conditions and withstand and rapidly recover from disruption.
Facilities Resilience	Ensuring that buildings, structures, and land assets can adapt to and continually operate during a disruption, and rapidly recover.
Fleet [motor vehicle]	Twenty or more motor vehicles that are used in the United States and that are not used for law enforcement, emergencies, and/or military use (Lexicon page 284).
Information and Communication Technology (ICT) Resilience	Ensuring that hardware, software, internal telecommunications infrastructure, programming, and information systems can adapt to changing conditions and withstand and rapidly recover from disruption.
Information Technology (IT)	Equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information (Lexicon page 364).
Infrastructure	Framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole. Consistent with the definition in the Homeland Security Act, infrastructure includes physical, cyber, and/or human elements (Lexicon page 367).
Interdependency	A relationship where the consequences of a positive or an adverse event affecting one will have cascading effects upon others (Lexicon page 389). Annotation: The degree of interdependency does not need to be equal in both directions.

Term	Definition
Mission Essential Asset (MEA)	An asset, whether physical or virtual, identified through a Business Process Analysis and Business Impact Analysis on Essential Functions as being critical to the execution of an essential function (OPS OI for BIA).
Mission Essential Function (MEF)	Function that enables an organization to provide vital services, exercise civil authority, maintain the safety of the public, and sustain the industrial/economic base during disruption of normal operations (Lexicon pages 461-462). Essential functions directly related to accomplishing the organization's mission as set forth in statutory or executive charter. Generally, MEFs are unique to each organization (PPD-40, p. 3).
Mission Essential System (MES)	Information systems that a Component Head or designee determines is necessary to perform one or more of its Mission Essential Functions. These systems provide IT capabilities across the DHS mission space and enterprise business services. DHS MES are a subset of DHS Mission Essential Assets.
National Essential Function (NEF)	Select functions that are necessary to lead and sustain the Nation during a catastrophic emergency and that, therefore, must be supported through Continuity of Operations (COOP) and Continuity of Government (COG) capabilities.(FCD-1)
Primary Mission Essential Function (PMEF)	Those mission essential functions that must be continuously performed to support or implement the uninterrupted performance of National Essential Functions (FCD-1).
Real Property	Property that includes land, structures, and buildings, as well as anything affixed to the land (Lexicon page 602).
Resilience	Ability to prepare for and adapt to changing conditions and withstand and rapidly recover from disruption; 1) ability of systems, infrastructures, government, business, and citizenry to resist, absorb, recover from, or adapt to an adverse occurrence that may cause harm, destruction, or loss of national significance 2) capacity of an organization to recognize threats and hazards and make adjustments that will improve future protection efforts and risk reduction measures 3) due to emergencies (Refer to PPD-8) (Lexicon page 627).
Transportation Resilience	Maintaining continuously available mobile assets (air, marine, and fleet) that can adapt to changing conditions and mobilize resources to assist the mission, and withstand and rapidly recover from disruption.

APPENDIX B: NATIONAL CRITICAL INFRASTRUCTURE SECTORS AND DESIGNATED SECTOR-SPECIFIC AGENCIES

Designated Critical Infrastructure Sectors and Sector-Specific Agencies
Chemical: Sector-Specific Agency: Department of Homeland Security
Commercial Facilities: Sector-Specific Agency: Department of Homeland Security
Communications: Sector-Specific Agency: Department of Homeland Security
Critical Manufacturing: Sector-Specific Agency: Department of Homeland Security
Dams: Sector-Specific Agency: Department of Homeland Security
Defense Industrial Base: Sector-Specific Agency: Department of Defense
Emergency Services: Sector-Specific Agency: Department of Homeland Security
Energy: Sector-Specific Agency: Department of Energy
Financial Services: Sector-Specific Agency: Department of the Treasury
Food and Agriculture: Co-Sector-Specific Agencies: U.S. Department of Agriculture and Department of Health and Human Services
Government Facilities: Co-Sector-Specific Agencies: Department of Homeland Security and General Services Administration
Healthcare and Public Health: Sector-Specific Agency: Department of Health and Human Services
Information Technology: Sector-Specific Agency: Department of Homeland Security
Nuclear Reactors, Materials, and Waste: Sector-Specific Agency: Department of Homeland Security
Transportation Systems: Co-Sector-Specific Agencies: Department of Homeland Security and Department of Transportation
Water and Wastewater Systems: Sector-Specific Agency: Environmental Protection Agency

APPENDIX C: RESILIENCE FRAMEWORK BASELINE ASSESSMENT CHECKLIST

Resilience Planning Guidance				
Assess Baseline				
Process-based Information	**Energy and Water**	**Information and Communication Technology**	**Facilities**	**Transportation**
Recovery Plans				
Emergency Management Plan				
Cyber Plan				
Continuition of Operations Plan (COOP)				
Memorandum of Understanding (MOU)				
Site Master Plan for Development				
Critical Mission Functions				
Information Sharing				
Communication				
First Responders				
Operational Data	**Energy and Water**	**Information and Communication Technology**	**Facilities**	**Transportation**
Energy Consumption per Building				
Water Consumption pser building				
Fuel Consumption by Mobile Assets				
List of Backup Generators				
Fuel Storage on-site				
Geospatial Data	**Energy and Water**	**Information and Communication Technology**	**Facilities**	**Transportation**
Electrical System Maps				
Natural Gas Maps				
Water and Wasterwater Maps				
Facility Maps				
Communication Network Maps				
Historical Data	**Energy and Water**	**Information and Communication Technology**	**Facilities**	**Transportation**
Grid Outages				
Utility Disruption				
After-Action Plans				
Weather Related Events				

APPENDIX D: SAMPLE AGENCY SCORECARD

Metric Score		
Not Started / No	In progress	Complete / Yes
🔴 1	🟡 2	🟢 3

		Score			
Step	**Metric Category**	**Information Communication Technology**	**Energy and Water**	**Facilities**	**Transportation**
1	Preparedness/Planning				
1.1	Stakeholder Identification	🟢 3	🟢 3	🟢 3	🟢 3
1.2	Critical Mission Identification	🟢 3	🟢 3	🟡 2	🟢 3
1.3	Criticality Assessment	🟢 3	🟢 3	🟡 2	🟢 3
1.4	Risk Assessment	🟢 3	🟢 3	🟢 3	🟢 3
1.5	Cyber Plan	🟢 3	🟢 3	🟢 3	🔴 1
1.6	Information Sharing	🟢 3	🟢 3	🟢 3	🔴 1
1.7	Business Continuity Plan	🟢 3	🟢 3	🟢 3	🟢 3
2	Construction Mitigation Measures				
2.1	Natural hazards	🟢 3	🟢 3	🟢 3	🟢 3
2.2	Standoff distance	🟢 3	🟢 3	🟡 2	🟢 3
3	Alternate Site Mitigation Measures				
3.1	Mitigation with Alternative Sites	🟢 3	🟢 3	🟢 3	🟢 3
4	Resource Mitigation Measures (Redundant Sources)				
4.1	Electric	🟢 3	🟢 3	🟢 3	🟢 3
4.2	Natural Gas	n/a	🟢 3	🟢 3	n/a
4.3	Communications & IT	🔴 1	🟢 3	🟢 3	n/a
4.4	Transportation	n/a	🟢 3	🟢 3	🟡 2
4.5	Water	n/a	🟢 3	🟢 3	n/a
4.6	Wastewater	n/a	🟢 3	🟢 3	n/a
5	Response Capabilities Onsite				
5.1	Incident command capability	🟢 3	🟢 3	🟢 3	🟢 3
6	Response Capabilities Offsite				
6.1	First responders interaction (mutual aid)	🟢 3	🟢 3	🟢 3	🟢 3
7	Recovery Restoration Agreements in Place				
7.1	Agreements	🟢 3	🟢 3	🟢 3	n/a
8	Resource Recovery Plans				
8.1	Recovery Plans	n/a	🟢 3	🟢 3	🟢 3
Total Score		🟢 2.9	🟢 3.0	🟢 2.9	🟢 2.7