



Threat and Hazard Identification and Risk Assessment Guide

Comprehensive Preparedness Guide (CPG) 201
Supplement 1: Toolkit

First Edition
April 2012



Homeland
Security

Table of Contents

Overview	1
Resources and Information.....	1
FEMA Documents.....	1
Presidential Documents	3
Federal Statutes and Regulations.....	3
Human-Caused Incidents.....	4
Technological Incidents.....	5
Data Sources.....	5
THIRA Templates.....	13

This page intentionally left blank.

Overview

This toolkit provides resources and information, data sources, and templates to support the conduct of a Threat and Hazard Identification and Risk Assessment (THIRA) as described in the first edition of the Comprehensive Preparedness Guide 201: Threat and Hazard Identification and Risk Assessment Guide.

Resources and Information

The resources and information in this section will assist jurisdictions in locating information on processes and guidance related to the identification of threats and hazards along with subsequent risk assessment. The list is broken down into research areas to facilitate understanding of the THIRA process as a whole, as well as each individual step of the process. The literature collection, though not exhaustive, is primarily focused on materials published and released directly by the Federal Emergency Management Agency (FEMA) and commonly referenced materials.

All referenced Web sites are active as of April 2012.

FEMA Documents

[National Preparedness Goal, First Edition. Department of Homeland Security. September 2011.](#)

The first edition of the National Preparedness Goal (Goal) sets the vision for preparedness nationwide and identifies the core capabilities and capability targets necessary to achieve that vision across the five mission areas: prevention, protection, mitigation, response, and recovery.

<http://www.fema.gov/pdf/prepared/npg.pdf>

[National Preparedness System. Department of Homeland Security. November 2011.](#)

The National Preparedness System description identifies six components to improve national preparedness for a wide range of threats and hazards, such as acts of terrorism, cyber attacks, pandemics, and catastrophic natural disasters: (1) identifying and assessing risks, (2) estimating capability requirements, (3) building or sustaining capabilities, (4) developing and implementing plans to deliver those capabilities, (5) validating and monitoring progress made toward achieving the Goal, and (6) reviewing and updating efforts to promote continuous improvement.

http://www.fema.gov/pdf/prepared/nps_description.pdf

[Perspective on Preparedness: Taking Stock Since 9/11. Report to Congress of the Local, State, Tribal, and Federal Preparedness Task Force. September 2010.](#)

Recommendations from this report indicate that all levels of government should be able to identify both natural and manmade risks. The report also states that jurisdictions can use existing state hazard mitigation processes as a potential model for the THIRA.

http://www.fema.gov/pdf/preparednesstaskforce/perspective_on_preparedness.pdf

[Comprehensive Preparedness Guide \(CPG\) 101. Federal Emergency Management Agency. November 2010.](#)

CPG 101, which provides guidance on the planning and development of emergency operations plans, places threats alongside hazards as priorities to consider during the planning process. Specifically, one of the components of Step 2 as outlined in this Guide is “Identify Threats and Hazards.”

http://www.fema.gov/pdf/about/divisions/npd/CPG_101_V2.pdf

[Multi-Hazard Identification and Risk Assessment: A Cornerstone of the National Mitigation Strategy. Federal Emergency Management Agency. January 1997.](#)

This reference is available to assist hazard identification, risk assessment, and mitigation specialists in refining the understanding of hazards and effects that hazards have on people and the built environment. This guide is meant to be updated as identification, assessment, and mitigation approaches are refined.

<http://www.fema.gov/library/viewRecord.do?id=2214>

[State and Local Mitigation Planning How-to-Guide: Understanding Your Risks – Identifying Hazards and Estimating Losses \(FEMA 386-2\). Federal Emergency Management Agency. August 2001.](#)

This FEMA how-to guide is designed to provide information that state and local governments need to initiate and maintain a planning process that will result in safer communities and to provide easy-to-understand guidance for field practitioners. The guides are applicable to states and communities of various sizes and varying ranges of financial and technical resources. The how-to guide focuses on identifying hazards and assessing losses to the community.

<http://www.fema.gov/library/viewRecord.do?id=1880>

[State and Local Mitigation Planning How-to Guide: Integrating Manmade Hazards into Mitigation Planning \(FEMA 386-7\). Federal Emergency Management Agency. September 2003.](#)

This FEMA how-to guide is designed to provide information that state and local governments need to initiate and maintain a planning process that will result in safer communities and to provide easy-to-understand guidance for field practitioners. The guides are applicable to states and communities of various sizes and varying ranges of financial and technical resources. This guide is specifically designed to incorporate mitigation considerations for manmade hazards into hazard mitigation planning.

<http://www.fema.gov/library/viewRecord.do?id=1915>

[Using HAZUS-MH for Risk Assessment \(FEMA 433\). Federal Emergency Management Agency. August 2004.](#)

This FEMA how-to guide provides detailed information on using HAZUS-MH to identify and measure risk for hazard mitigation purposes.

<http://www.fema.gov/pdf/plan/prevent/hazus/fema433.pdf>

Presidential Documents

[Presidential Policy Directive \(PPD\) 8—National Preparedness. March 2011.](http://www.dhs.gov/xabout/laws/gc_1215444247124.shtm)

http://www.dhs.gov/xabout/laws/gc_1215444247124.shtm

[Homeland Security Presidential Directive 5—Management of Domestic Incidents. February 2003.](http://www.fas.org/irp/offdocs/nspd/hspd-5.html)

<http://www.fas.org/irp/offdocs/nspd/hspd-5.html>

[Homeland Security Presidential Directive 7—Critical Infrastructure Identification, Prioritization, and Protection. December 2003.](http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm)

http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm

[Homeland Security Presidential Directive 18—Medical Countermeasures against Weapons of Mass Destruction. January 2007.](http://www.fas.org/irp/offdocs/nspd/hspd-18.html)

<http://www.fas.org/irp/offdocs/nspd/hspd-18.html>

[Homeland Security Presidential Directive 19—Combating Terrorist Use of Explosives in the United States. February 2007.](http://www.fas.org/irp/offdocs/nspd/hspd-19.pdf)

<http://www.fas.org/irp/offdocs/nspd/hspd-19.pdf>

[Intelligence Reform and Terrorism Prevention Act of 2004. Public Law 108–458. December 2004.](http://www.nctc.gov/docs/irtpa.pdf)

<http://www.nctc.gov/docs/irtpa.pdf>

[National Strategy for Homeland Security. Executive Office of the President. October 2007.](http://georgewbush-whitehouse.archives.gov/infocus/homeland/nshs/2007/index.html)

<http://georgewbush-whitehouse.archives.gov/infocus/homeland/nshs/2007/index.html>

Federal Statutes and Regulations

[An Act to Authorize Funding for Computer and Network Security Research and Development and Research Fellowship Programs, and for Other Purposes \(Public Law 107-305\). November 2002.](http://www.gpo.gov/fdsys/pkg/PLAW-107publ305/html/PLAW-107publ305.htm)

<http://www.gpo.gov/fdsys/pkg/PLAW-107publ305/html/PLAW-107publ305.htm>

[“Mitigation Planning,” Title 44 Code of Federal Regulations, Chapter 1, Pt. 201, 2009 ed.](http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&rgn=div5&view=text&node=44:1.0.1.4.53&idno=44)

<http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&rgn=div5&view=text&node=44:1.0.1.4.53&idno=44>

[Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended, and Related Authorities as of June 2007. Federal Emergency Management Agency. June 2007.](https://www.fema.gov/library/viewRecord.do?id=3564)

<https://www.fema.gov/library/viewRecord.do?id=3564>

Human-Caused Incidents

[2010 Report on Terrorism. National Counterterrorism Center. April 30, 2011.](#)

This report, furnished by the National Counterterrorism Center (NCTC), contains statistical information about reported attacks that have been classified as terrorism, including details about the location, type, and frequency of each incident. Tracking and analyzing terrorist incidents can help establish an understanding of important characteristics about terrorism, including the geographic distribution of attacks and information about the perpetrators, their victims, and other relevant details.
http://www.nctc.gov/witsbanner/docs/2010_report_on_terrorism.pdf

[Evolving Terrorist Threat: Long-term Trends and Drivers and Their Implications for Emergency Management. Strategic Foresight Initiative. September 2011.](#)

FEMA's Strategic Foresight Initiative (SFI) is a collaborative effort on the part of the emergency management community to examine current trends that may shape the future of emergency management. This paper sets forth a series of research findings on trends relating to the Evolving Terrorist Threat driver, one of nine drivers SFI has identified as being likely to affect the field of emergency management over the next 15 years.
http://www.fema.gov/pdf/about/programs/oppa/evolving_terrorist_threat.pdf

[Smith, B. A Look at Terrorist Behavior: How They Prepare, Where They Strike. National Institute of Justice Journal. Issue 260.](#)

This article investigates a series of projects that the National Institute of Justice launched in an effort to explore patterns of terrorist behavior. The conclusion is that most terrorists "act locally" in some manner. This understanding, coupled with details and findings of the projects described in this article, may be used by agencies to prevent terrorist acts and arrest perpetrators.
<https://www.ncjrs.gov/pdffiles1/nij/222900.pdf>

[Ezell, B. C., et al. Probabilistic Risk Analysis and Terrorism Risk. Risk Analysis. Volume 30, Number 4, pp. 575-589. 2010.](#)

This article describes a number of existing and potential approaches to terrorism risk analysis, with particular attention to the application of probabilistic risk analysis. "Tools for Terrorism Risk Analysis," a section within the article, presents three categories of tools that can be used in probabilistic risk analysis as it applies to terrorism risk. These tools include the use of logic trees; additional methods, including influence diagrams, systems dynamics models, and Bayesian networks; and game theoretic models.
<http://www.dhs.gov/xlibrary/assets/rma-risk-assessment-technical-publication.pdf>

[Strategic Implementation Plan for Empowering Local Partners to Prevention Violent Extremism in the United States. Executive Office of the President. December 2011.](#)

This plan provides a blueprint for how the United States will build community resilience against violent extremism, with priority on preventing violent extremism and terrorism that is inspired by al-Qa'ida and its affiliates and adherents.
<http://www.whitehouse.gov/sites/default/files/sip-final.pdf>

Technological Incidents

[IT Security Essential Body of Knowledge: A Competency and Functional Framework for IT Security Workforce Development. Department of Homeland Security, National Cyber Security Division, Office of Cybersecurity and Communications. September 2008.](#)

This document, developed by the U.S. Department of Homeland Security's (DHS) U.S. Computer Emergency Readiness Team (CERT), helps government and private sector management identify core IT security capabilities. The document is a comprehensive collection of IT security terms, competency areas (e.g., digital forensics, procurement, risk management), roles, key knowledge, and core responsibilities.

<http://www.us-cert.gov/ITSecurityEBK/EBK2008.pdf>

[Comprehensive National Cybersecurity Initiative. Executive Office of the President.](#)

This document provides an overview of the U.S. national cybersecurity priorities. In addition, the document identifies 12 activities underway to help secure the United States in cyberspace.

<http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf>

Data Sources

[ALOHA.](#)

ALOHA (Areal Locations of Hazardous Atmospheres) is a program designed to model chemical releases for emergency responders and planners. It can estimate how a toxic cloud might disperse after a chemical release and also features several fire and explosion scenarios.

<http://response.restoration.noaa.gov/aloha>

[Bureau of Economic Analysis. U.S. Department of Commerce.](#)

The Bureau of Economic Analysis publishes annual estimates of the share of Gross Domestic Product (GDP) contributed by each state (Gross State Product) and territory, except Puerto Rico. The Bureau also produces similar metrics for urban areas and local area personal income summary data for metropolitan areas and counties.

<http://www.bea.gov/regional/index.htm>

[Bureau of Transportation Statistics, Research and Innovative Technology Administration. U.S. Department of Transportation.](#)

The Bureau of Transportation Statistics provides data on a range of transportation topics, including border crossing/entry data, commodity flow, freight data, maritime trade and transportation, ferry operators, national and state bridge data, and transportation system and infrastructure data.

http://www.bts.gov/data_and_statistics/

[Centers for Disease Control. U.S. Department of Health and Human Services.](#)

The Centers for Disease Control provides data and information on a range of health topics, including recent outbreaks and incidents, as well as biological, chemical, and radiological agents.

<http://www.cdc.gov>

[Coastal Resilience Index Critical Facilities Tool. Gulf of Mexico Alliance's Coastal Community Resilience Priority Issue Team, Mississippi-Alabama Sea Grant Consortium, Louisiana Sea Grant College Program, National Oceanic and Atmospheric Administration.](#)

This tool was developed by the Gulf of Mexico Alliance's Coastal Community Resilience Priority Issue Team, the Mississippi-Alabama Sea Grant Consortium, and the Louisiana Sea Grant College Program in collaboration with 18 communities along the Gulf Coast from Texas to Florida. It is a self-assessment tool and provides communities with a method of predicting if an acceptable level of functionality may be maintained after a disaster.

<http://www.csc.noaa.gov/criticalfacilities/>

[Computer Security Resource Center. National Institute of Standards and Technology. Computer Security Division.](#)

This resource center offers many publications and security bulletins on issues relating to information technology security.

<http://csrc.nist.gov/index.html>

[Data.gov.](#)

The purpose of Data.gov is to increase public access to high value, machine readable datasets generated by the Executive Branch of the Federal Government. As a priority Open Government Initiative for President Obama's administration, Data.gov increases the ability of the public to easily find, download, and use datasets that are generated and held by the Federal Government. Data.gov provides descriptions of the Federal datasets (metadata), information about how to access the datasets, and tools that leverage government datasets. The data catalogs will continue to grow as datasets are added. Federal, Executive Branch data are included in the first version of Data.gov.

<http://www.data.gov>

[DHS OneView. Department of Homeland Security.](#)

This site requires the generation of an account and is a geospatial visualization tool designed for the use of homeland security partners in protecting the Nation's critical infrastructure and key resources. This tool may NOT be used to overlay and/or visualize datasets containing personally identifiable information.

<https://gii.dhs.gov/OneView/Login/Login.aspx?ReturnUrl=%2foneview>

[Environmental Protection Agency.](#)

This site provides maps and general information on human health and environmental impacts.

<http://www.epa.gov/>

[FEMA Disasters and Maps.](#)

FEMA provides information and maps relating to hurricanes, floods, earthquakes, and dam failures. In addition, FEMA provides information on disaster and emergency declarations.

<http://www.fema.gov/hazard/index.shtm>

[FEMA Map Service Center](#)

The FEMA Map Service Center is the official government distribution center for digital flood hazard mapping products created by FEMA in support of the National Flood Insurance Program. The Map Service Center provides all current flood maps (Flood Insurance Rate Maps) for the entire United States and its territories.

<https://msc.fema.gov>

[Full-Spectrum Risk Knowledgebase.](#)

The Full-Spectrum Risk Knowledgebase is a FEMA initiative designed to support government officials in considering their risks and to enhance risk-informed decisionmaking. This secure Web site serves as a resource for stakeholders and provides reference material, information, and guidance aimed at helping users further develop and refine their own knowledge of all-hazards risks. Among other information, the Knowledgebase includes descriptions of various threats and hazards, visual depictions of how hazards relate to one another (cause and consequence), information on mitigation strategies and countermeasures, examples of various incidents for added context, and information on the application of different structured analytic techniques to aid in analyses. All site content is kept very general and it is up to users to apply their knowledge and experience to tailor the information to their respective area(s) of responsibility as needed.

<https://riskknowledge.fema.gov>

[HAZUS-MH. Federal Emergency Management Agency.](#)

This site has a tool that estimates loss, impact on physical damage, social impacts, shelter requirements, etc. for floods, earthquakes, and hurricanes.

<http://www.fema.gov/plan/prevent/hazus/>

[Homeland Security Digital Library.](#)

The Homeland Security Digital Library (HSDL) is the Nation's premier research collection of open-source resources related to homeland security policy, strategy, and organizational management. The HSDL is sponsored by the Naval Postgraduate School Center for Homeland Defense and Security and DHS's National Preparedness Directorate, FEMA.

<http://www.hsdl.org>

[HURREVAC.](#)

HURREVAC is a computer program used by government emergency managers to track hurricanes and assist in decisionmaking for their communities. <http://www.hurrevac.com/>

[LandScan USA. Oak Ridge National Laboratory.](#)

This is a population distribution model that produces the finest resolution population distribution data.

<http://www.ornl.gov/sci/landscan/>

[Maritime Administration. United States Department of Transportation.](#)

The Maritime Administration provides a count of the annual number of passengers that embark on a cruise ship from a port.

http://www.marad.dot.gov/library_landing_page/data_and_statistics/Data_and_Statistics.htm

[Lessons Learned Information Sharing.](#)

Lessons Learned Information Sharing (LLIS) is a DHS/FEMA program. LLIS.gov serves as the national, online network of lessons learned, best practices, and innovative ideas for the emergency management and homeland security communities. This information and collaboration resource helps emergency response providers and homeland security officials to prevent, protect against, respond to, and recover from terrorist attacks, natural disasters, and other emergencies. LLIS.gov provides Federal, state, and local responders and emergency managers with a wealth of information and front-line expertise on effective planning, training, and operational practices across homeland security functional areas.

<https://www.llis.dhs.gov/>

[National Vulnerability Database. Department of Homeland Security, National Cyber Security Division.](#)

This Web site is a tool for government and private-sector IT departments to use for identifying and correcting technical and cyber vulnerabilities. This Web site, which functions as the Federal Government's repository of information relating to these vulnerabilities, contains links to information about vulnerabilities, alerts, and publicly available security checklists that provide guidance on the security configuration of common operating systems and applications.

<http://nvd.nist.gov/>

[Naval Vessel Register. U.S. Navy.](#)

The Naval Vessel Register contains information, including location, on ships and service craft that comprise the official inventory of the U.S. Navy from the time of vessel authorization through its life cycle and disposal. It also includes ships that have been stricken but not disposed.

<http://www.nvr.navy.mil/>

[National Oceanic and Atmospheric Administration \(NOAA\) – National Hurricane Center](#)

This site provides a plethora of information on hurricanes. It includes forecasts of hurricane season, as well as tracking of low pressure systems that have the potential of developing into a hurricane. The site has a large amount of information on historical hurricanes that can be applied to the THIRA process.

<http://www.nhc.noaa.gov/>

[NOAA – National Weather Service.](#)

This site provides weather forecasting all over the United States. This includes normal weather as well as severe weather incidents.

<http://weather.gov/>

[NOAA – River Forecast Centers.](#)

This site provides information on rivers across the United States. The site divides the United States into regions. It provides real-time data on rivers that includes their current heights and forecasts of potential droughts and overflow.

<http://water.weather.gov/ahps/rfc/rfc.php>

[Nuclear Regulatory Commission.](#)

This site provides the locations of nuclear facilities.

<http://www.nrc.gov/info-finder.html>

[Office of Highway Policy Information. U.S. Department of Transportation.](#)

This site provides data on highway statistics, such as drivers, vehicles and travel.

<https://www.fhwa.dot.gov/policyinformation/>

[Pipeline and Hazardous Materials Safety Administration. U.S. Department of Transportation.](#)

This site provides information on the Nation's pipeline transportation system and hazardous materials. It includes data and statistics on pipeline accidents and incidents as well as hazardous materials incidents.

<http://www.phmsa.dot.gov/home>

[Roadmap for Adapting to Coastal Risk. NOAA Coastal Services Center.](#)

The Roadmap for Adapting to Coastal Risk is a participatory process that assesses a community's vulnerability to hazards. The process incorporates relevant data and information about hazards and the climate into ongoing local planning and decisionmaking. Various training opportunities for the Roadmap assessment methodology exist, including a three-hour virtual training and a recorded webinar. Additional information can be found on the Training tab of the Roadmap page or the Tools tab of the Coastal Services Center page.

<http://www.csc.noaa.gov/digitalcoast/training/roadmap/index.html>

[Sea, Lake, and Overland Surges from Hurricanes \(SLOSH\).](#)

SLOSH is a computerized model developed by FEMA, the U.S. Army Corps of Engineers (USACE), and the National Weather Service to estimate storm surge depths resulting from historical, hypothetical, or predicted hurricanes by taking into account a storm's pressure, size, forward speed, forecast track, wind speeds, and topographical data.

http://www.fema.gov/plan/prevent/nhp/slosh_link.shtm

[Sea Level Rise and Coastal Flooding Impacts Viewer.](#)

Being able to visualize potential impacts from sea level rise is a powerful teaching and planning tool; the Sea Level Rise Viewer brings this capability to coastal communities. A slider bar is used to show how various levels of sea level rise will impact coastal communities. The initial project areas include Mississippi, Alabama, and parts of Texas and Florida, with additional coastal counties to be added in the near future. Visuals and the accompanying data and information cover sea level rise inundation, uncertainty, flood frequency, marsh impacts, and socioeconomics.

<http://csc.noaa.gov/digitalcoast/tools/slrviewer/>

[U.S. Army Corps of Engineers Debris Model.](#)

This tool estimates the amounts of debris from hurricanes making landfall along the Gulf and East Coasts.

<https://eportal.usace.army.mil/sites/ENGLink/DisasterImpactModels/ModelDescription/default.aspx>

[U.S. Army Corps of Engineers Waterborne Commerce Statistics Center.](#)

The Waterborne Commerce Statistics Center provides statistics on the commercial movement of foreign and domestic cargo, including trips and tonnage data by ports and waterways.

<http://www.ndc.iwr.usace.army.mil/wcsc/wcsc.htm#2009> Waterborne Commerce of the United States (WCUS)

[U.S. Census Bureau. U.S. Department of Commerce.](#)

The Census Bureau provides data about the Nation's people and economy at various levels of detail. It can be used to determine how many people may be affected by a threat or hazard and the characteristics of that population, including daily commuters, nighttime population, jurisdictional land area, and international waters and borders.

<http://www.census.gov/>

[U.S. Department of Defense. Base Structure Report.](#)

The Base Structure Report is a consolidated summary of the department's real property inventory, including the number of personnel at U.S. military bases.

<http://www.acq.osd.mil/ie/>

[U.S. Geological Survey.](#)

This site provides a great deal of information on environmental threats and hazards. Topics covered include avian influenza to floods and wildfires to remote sensing systems. It includes real-time data on multiple topics.
<http://www.usgs.gov/>

[United States Computer Emergency Readiness Team. Department of Homeland Security, National Cyber Security Division.](#)

This Web site is maintained by DHS's CERT and is intended for users at varied levels of technical expertise. The Web site provides links to various security publications, cyber security alerts, and tools that can be used to report vulnerabilities or incidents.
<http://www.us-cert.gov>

[USA Trade Online. Foreign Trade Division, Census Bureau, U.S. Department of Commerce.](#)

USA Trade Online provides import and export vessel cargo value data at the district, port, and state levels.
<https://www.usatradeonline.gov/> (paid registration required)

[Vulnerability and Capacity Assessment \(VCA\). International Federation of Red Cross and Red Crescent Societies.](#)

The purpose of this tool is to determine people's exposure to and ability to resist natural hazards. VCA allows for local priorities to be identified and appropriate action to be taken to reduce disaster risk and assist in the design and development of programs for those that are directly affected. The VCA has the following goals: assess risks and hazards facing communities and the capacities they have to deal with them; involve communities, local authorities, and humanitarian and development organizations in the assessment; draw up action plans to prepare for and respond to identified risks; and identify risk-reduction activities to prevent or lessen the effects of hazards, risks, and vulnerabilities.
<http://www.ifrc.org/en/what-we-do/disaster-management/preparing-for-disaster/disaster-preparedness-tools/disaster-preparedness-tools/>

[Worldwide Incidents Tracking System. National Counterterrorism Center.](#)

Maintained by the NCTC, this database includes information on terrorist attack events that occurred between January 1, 2004, and April 30, 2010, details of which have been compiled from open source data. Users can filter and sort incident data by a broad range of characteristics, browse attack records, and derive statistics on terrorism around the world.
<https://wits.nctc.gov/FederalDiscoverWITS/index.do?N=0>

This page intentionally left blank.

THIRA Templates

The templates in this document mirror Tables 3–6 in CPG 201. Jurisdictions can use these tables to develop descriptions of possible threats and hazards, capture or establish desired outcomes, and estimate the impacts to the community through the lens of the core capabilities.

Step Two of the THIRA process involves giving threats and hazards context for how they might unfold in a community. The template for a Threat and Hazard Description Statement table allows a jurisdiction to develop description statements that briefly explain the conditions under which a threat or hazard might occur. The statements should take into account the following, as well as factors such as demographics, climate, and the built environment:

- When might a threat or hazard occur? What time of day? What season?
- Where might the threat or hazard occur? Populated areas? Coastal zones? Industrial or residential areas?

Multiple descriptions statements may be needed if varying conditions make a significant difference in how a threat or hazard affects the community. Examples of description statements for each threat and hazard group—natural, technological, and human-caused—are included in the template for reference. The number of rows of included threat and hazard group and description statements are for illustration only and do not convey requirements.

Table 1: Threat and Hazard Description Statements

Threat/Hazard Group	Threat/Hazard Type
Natural	<i>Tornado</i>
<p>Description 1: <i>Example: An F3 tornado strikes the business district on a Saturday afternoon in spring</i></p> <p>Description 2: <i>Example: An F4 strikes a residential community on a Thursday morning in winter</i></p> <p>Description 3: <i>Other description statements as needed</i></p>	
Technological	<i>Dam Failure</i>
<p>Description 1: <i>Example: A major power-generating dam has a catastrophic failure resulting in the downstream flooding of three towns</i></p> <p>Description 2: <i>Example: A small earthen dam that retains a recreational lake that feeds a community's water supply fails, resulting in downstream flooding and a loss of potable water for an extended period</i></p> <p>Description 3: <i>Other description statements as needed</i></p>	
Human-caused	<i>Chemical Attack</i>
<p>Description 1: <i>Example: An unknown terrorist group delivers a chemical nerve agent attack at a large outdoor public gathering during the summer</i></p> <p>Description 2: <i>Example: An unknown terrorist group delivers a chemical nerve agent attack on a mass transit system on a work day during rush hour</i></p>	

Threat/Hazard Group	Threat/Hazard Type
Natural	
Description 1: Description 2: Description 3:	
Technological	
Description 1: Description 2: Description 3:	
Human-caused	
Description 1: Description 2: Description 3:	

Step Three of the THIRA process involves using the threat and hazard context to identify impacts to the community through the lens of the core capabilities described in the Goal. First, a jurisdiction should develop desired outcomes—what the jurisdiction wants to achieve for each core capability. These outcomes should be informed by the Goal and should be developed with the whole community. The template for a Desired Outcomes table allows a jurisdiction to list the desired outcomes for all 31 core capabilities. These outcomes statements will assist the jurisdiction in setting capability targets. Examples of desired outcomes included in the template are for illustration purposes.

Table 2: Desired Outcomes

	Core Capability	Desired Outcome
Common	Planning	<i>Mitigation Example: All hazard mitigation plans that address all relevant threats/hazards in accordance with the results of their risk assessment</i>
	Public Warning and Information	
	Operational Coordination	
Prevention	Forensics and Attribution	<i>Example: Physical evidence collection and analysis is prioritized to assist in preventing initial or follow-on terrorist acts</i>

	Core Capability	Desired Outcome
Prevention and Protection	Intelligence and Information Sharing	
	Interdiction and Disruption	
	Screening, Search, and Detection	<i>Prevention Example: Screen 100% of targeted cargo, conveyances, mail, baggage, and people associated with an imminent terrorist threat or act using technical, non-technical, intrusive, or non-intrusive means</i>
Protection	Access Control and Identity Verification	<i>Example: Ensure 100% verification of identity to authorize, grant, or deny physical and cyber access to specific locations, information, and networks</i>
	Cybersecurity	
	Physical Protective Measures	
	Risk Management for Protection Programs and Activities	
	Supply Chain Integrity and Security	
Mitigation	Community Resilience	
	Long-term Vulnerability Reduction	<i>Example: Achieve a measurable decrease in the long-term vulnerability of critical infrastructure and systems</i>
	Risk and Disaster Resilience Assessment	
	Threats and Hazard Identification	

	Core Capability	Desired Outcome
Response	Critical Transportation	
	Environmental Response/Health Safety	
	Fatality Management Services	<i>Example: During the first 72 hours of an incident, conduct operations to recover fatalities</i>
	Mass Care Services	
	Mass Search and Rescue Operations	
	On-Scene Security and Protection	
	Operational Communications	
	Public and Private Services and Resources	
	Public Health and Medical Services	
	Situational Assessment	
Response and Recovery	Infrastructure Systems	<i>Recovery Example: Within 15 days of an incident, restore and sustain essential services (public and private) to maintain community functionality</i>
Recovery	Economic Recovery	<i>Example: Within 60 days of an incident, conduct a preliminary assessment of economic issues and identify potential inhibitors to fostering stabilization of the affected communities</i>
	Health and Social Services	
	Housing	
	Natural and Cultural Resources	

Step Three of the THIRA process also involves estimating the impacts of threats and hazards on a community. Those impacts should, at a minimum, span the core capabilities described in the Goal. Displaced households, fatalities, injuries/illnesses, direct economic impacts to the jurisdiction, indirect economic impacts from supply chain system disruption, and disruption to infrastructure are some, but not all of the impacts that should be considered. The template for an

Estimated Impacts table allows a jurisdiction to estimate the impacts to the community of its threats and hazards statements across the 31 core capabilities and all mission areas—Prevention, Protection, Mitigation, Response, and Recovery. Examples of impacts are included in Table 5 of CPG 201.

Table 3: Example Estimated Impacts

Threat/Hazard Description	Common			Prevention	Prevention and Protection			Protection				
	Planning	Public Information and Warning	Operational Coordination	Forensics and Attribution	Intelligence and Information Sharing	Interdiction and Disruption	Screening, Search, and Detection	Access Control and Identity Verification	Cybersecurity	Physical Protective Measures	Risk Management for Protection Programs and Activities	Supply Chain Integrity and Security
Threat/Hazard Description	Mitigation				Response							
	Community Resilience	Long-term Vulnerability Reduction	Risk and Disaster Resilience and Assessment	Threats and Hazard Identification	Critical Transportation	Environmental Response/Health and Safety	Fatality Management Services	Mass Care Services	Mass Search and Rescue Operations	On-scene Security and Protection	Operational Communications	Public and Private Services and Resources
Threat/Hazard Description	Response		Response and Recovery	Recovery								
	Public Health and Medical Services	Situational Assessment	Infrastructure Systems	Economic Recovery	Health and Social Services	Housing	Natural and Cultural Resources					

Step Four of the THIRA process looks across the estimated impacts to the community, in the context of each core capability, and couples that information with a jurisdiction’s desired outcomes to set capability targets. The template for capability targets allows a jurisdiction to list their targets. Examples of capability targets are included in the template for illustration.

Table 4: Example Core Capabilities Targets

	Core Capability	Desired Outcome
Common	Planning	
	Capability Target:	
	Public Warning and Information	
	Capability Target:	
	Operational Coordination	
	Capability Target:	
Prevention	Forensics and Attribution	
	Capability Target:	
Prevention and Protection	Intelligence and Information Sharing	
	Capability Target:	
	Interdiction and Disruption	
	Capability Target:	
	Screening, Search, and Detection	<i>Screen 100% of targeted cargo, conveyances, mail, baggage, and people associated with an imminent terrorist threat or act using technical, non-technical, intrusive, or non-intrusive means</i>
	Capability Target: <i>Example: Screen 67,500 people associated with an imminent terrorist threat or act using technical, non-technical, intrusive, or non-intrusive means</i>	

	Core Capability	Desired Outcome
Protection	Access Control and Identity Verification	<i>Ensure 100% verification of identity to authorize, grant, or deny physical and cyber access to specific locations, information, and networks</i>
	Capability Target: <i>Example: Verify 2,500 identities to authorize, grant, or deny physical and cyber access</i>	
	Cybersecurity	
	Capability Target:	
	Physical Protective Measures	
	Capability Target:	
	Risk Management for Protection Programs and Activities	
	Capability Target:	
	Supply Chain Integrity and Security	
Capability Target:		
Mitigation	Community Resilience	
	Capability Target:	
	Long-term Vulnerability Reduction	<i>Achieve a measurable decrease in the long-term vulnerability of critical infrastructure and systems</i>
	Capability Target: <i>Example: Achieve a measurable decrease in the long-term vulnerability by rerouting 100% of rail containing toxic inhalation chemicals around densely populated areas</i>	
	Risk and Disaster Resilience Assessment	
	Capability Target:	
	Threats and Hazard Identification	
Capability Target:		

		Core Capability	Desired Outcome
Response		Critical Transportation	
		Capability Target:	
		Environmental Response/Health and Safety	
		Capability Target:	
		Fatality Management Services	<i>During the first 72 hours of an incident, conduct operations to recover fatalities</i>
		Capability Target: Example: During the first 72 hours of an incident, conduct operations to recover 375 fatalities	
		Mass Care Services	
		Capability Target:	
		Mass Search and Rescue Operations	
		Capability Target:	
		On-Scene Security and Protection	
		Capability Target:	
		Operational Communications	
		Capability Target:	
		Public and Private Services and Resources	
		Capability Target:	
		Public Health and Medical Services	
		Capability Target:	
	Situational Assessment		
	Capability Target:		

	Core Capability	Desired Outcome
Response and Recovery	Infrastructure Systems	<i>Example: Within 15 days of an incident, restore and sustain essential services (public and private) to maintain community functionality</i>
	Capability Target: <i>Example: Within 15 days of an incident, restore power to 350,000 customers</i>	
Recovery	Economic Recovery	
	Capability Target:	
	Health and Social Services	
	Capability Target:	
	Housing	
	Capability Target:	
	Natural and Cultural Resources	
Capability Target:		