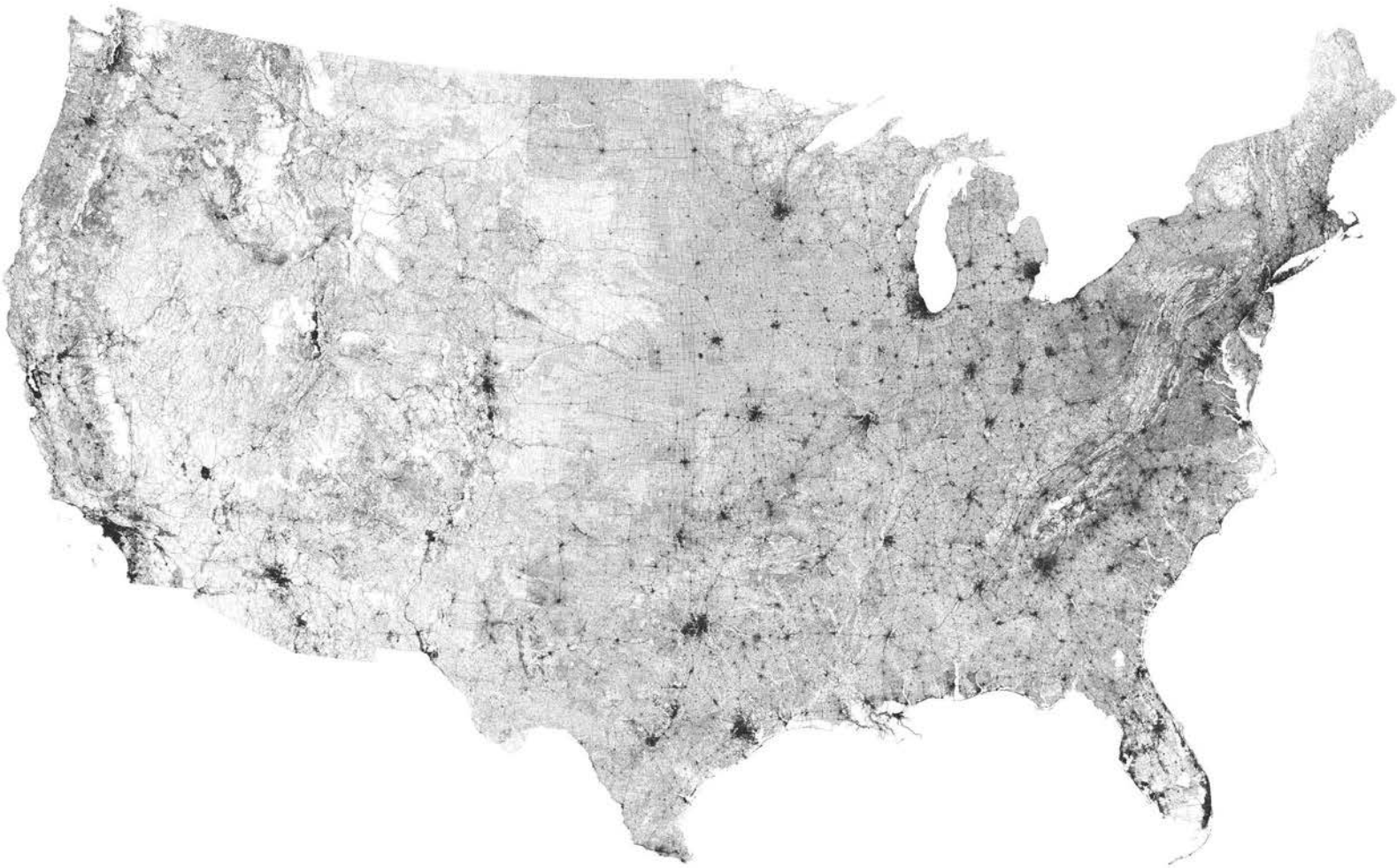

National Protection Framework

Second Edition
June 2016

Homeland Security

Executive Summary

The National Protection Framework describes the way that the whole community safeguards against acts of terrorism, natural disasters, and other threats or hazards. The Protection processes and guiding principles contained in this Framework provide a unifying approach that is adaptable to specific Protection mission requirements, mission activities, jurisdictions, and sectors. The dynamic nature of risks facing the Nation requires a national approach that is adaptable to this changing and increasingly volatile landscape.

This Framework describes the core capabilities, roles and responsibilities, and network of coordinating structures that facilitate the protection of individuals, communities, and the Nation. It is focused on actions to protect against the Nation's greatest risks in a manner that allows American interests, aspirations, and way of life to thrive.

Partnerships at all levels of government, and with the private and nonprofit sectors coordinate the development and delivery of 11 national core capabilities for Protection. This effort is guided by the principles of resilience and scalability, risk-informed culture, and shared responsibility.

The National Protection Framework relies on existing coordinating structures to promote integration, synchronization, and resilience across various jurisdictions and areas of responsibility. The range of coordinating structures that contribute to the Protection mission includes operations centers; law enforcement task forces; critical infrastructure sector, government, and cross-sector coordinating councils; governance boards; regional consortiums; information-sharing mechanisms, such as state and major urban area fusion centers; health surveillance networks; and public-private partnership organizations at all levels.[1] As national doctrine, this Framework provides a unifying approach for aligning the Protection activities across the varied activities and coordination structures of the mission.

These partnerships may span functional, critical infrastructure sector, and geographical boundaries. They allow for the exchange of expertise and information and provide a source of potential resources through mutual aid and assistance agreements. Partners across the whole community can use the National Protection Framework to inform and align relevant planning, training, exercises, and other activities designed to enhance security for individuals, families, communities, organizations, and jurisdictions. Structuring planning, training, exercises, and operations around the Protection core capabilities enhances national preparedness.

The principles outlined in this Framework are designed to provide a common reference for implementing Protection as part of national preparedness. The National Protection Framework promotes a shared understanding of the Protection mission that enables more effective information sharing, interoperability, and effectiveness of Protection activities nationwide.

[1] This Framework is aligned with relevant Presidential policy directives and existing preparedness doctrine. For example, structures outlined in the National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience, which was developed in support of Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience and Executive Order 13636: Improving Critical Infrastructure Cybersecurity, are integral to the Protection mission.

Table of Contents

Introduction

The National Preparedness System outlines an organized process for the whole community to achieve the National Preparedness Goal. The National Preparedness System integrates efforts across the five preparedness mission areas—Prevention, Protection, Mitigation, Response, and Recovery—in order to achieve the goal of a secure and resilient Nation. The National Protection Framework, part of the National Preparedness System, sets the strategy and doctrine for how the whole community builds, sustains, and delivers the Protection core capabilities identified in the National Preparedness Goal in an integrated manner with the other mission areas. This second edition of the National Protection Framework reflects the insights and lessons learned from real-world incidents and the implementation of the National Preparedness System.

Prevention: The capabilities necessary to avoid, prevent, or stop a threatened or actual act of terrorism. Within the context of national preparedness, the term "prevention" refers to preventing imminent threats.

Protection: The capabilities necessary to secure the homeland against acts of terrorism and manmade or natural disasters.

Mitigation: The capabilities necessary to reduce loss of life and property by lessening the impact of disasters.

Response: The capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred.

Recovery: The capabilities necessary to assist communities affected by an incident to recover effectively.

Framework Purpose and Organization

The National Protection Framework describes what the whole community—from community members to senior leaders in government—should do to safeguard against acts of terrorism, natural disasters, and other threats or hazards.[2] To support the National Preparedness Goal, this Framework provides guidance to leaders and practitioners at all levels of government, the private and nonprofit sectors, and individuals by

- Describing the core capabilities needed to conduct the Protection mission and create conditions for a safer, more secure, and more resilient Nation.
- Aligning key roles and responsibilities to deliver Protection capabilities.
- Describing coordinating structures that enable all stakeholders to work together.
- Laying the foundation for operational coordination and planning that aligns Protection efforts within the whole community.

[2] The whole community includes individuals and communities, the private and nonprofit sectors, faith-based organizations, and all levels of government (local, regional/metropolitan, state, tribal, territorial, insular area, and Federal). Whole community is defined in the National Preparedness Goal as "a focus on enabling the participation in national preparedness activities of a wider range of players from the private and nonprofit sectors, including nongovernmental organizations and the general public, in conjunction with the participation of all levels of government in order to foster better coordination and working relationships. Used interchangeably with "all-of-Nation."

- Strengthening the ability of essential Protection functions and services to continue regardless of threat or hazard.

The National Protection Framework is structured as a single document that provides the national model for interdisciplinary coordination of Protection activities. The Protection mission is inherently decentralized. Protection mission activities are conducted across multiple disciplines and jurisdictions, by agencies, organizations, and communities that operate under distinct authorities.

While the National Preparedness System emphasizes the National Incident Management System (NIMS) as the basis for organizing operations during incident management, Protection capabilities are built, sustained, and delivered by a wide range of organizational arrangements.[3] Protection is often delivered across disparate sectors and geographical areas that require decentralized, mutually informed action. This places a particular emphasis on information sharing and the autonomy of individual communities of protection.

The principles outlined in the National Protection Framework describe a common scheme but do not prescribe a national structure for organization. Rather, they outline the means by which the Nation jointly builds capabilities and the structure by which decentralized organizations supporting the Protection mission jointly deliver those capabilities.

The process and policies described in this document will be conducted in accordance with existing laws and regulations.

Intended Audience

Although the National Protection Framework is intended to provide guidance for the whole community, it focuses especially on the needs of those involved in delivering and applying the Protection core capabilities defined in the National Preparedness Goal. This includes senior leaders with direct responsibility for implementing core capabilities within the Protection mission. Such leaders include, but are not limited to, government and corporate executives; law enforcement, security, public health, health systems, fire, emergency medical, and emergency management professionals; critical infrastructure owners and operators; and others with legal or statutory authorities within this mission area.

Protection professionals and communities deliver their capabilities to a variety of other communities and individuals, those in other mission areas, those in other security areas, and other affiliated groups. These communities are the customers for Protection professionals and are a key element for planning and responsibly delivering the Protection capabilities.

Engaging the whole community is critical to success, and individual and community preparedness is a key component. By providing equal access to acquire and use the necessary knowledge and skills, this Framework seeks to enable the whole community to contribute to and benefit from national preparedness. This includes children;[4] older adults; individuals with disabilities and others with access and functional needs;[5] those from religious, racial, and ethnically diverse backgrounds; and

[3] When Protection capabilities and personnel are delivered in support of incident operations, they conform to NIMS and appropriate incident command structures for planning and operations.

[4] Children require a unique set of considerations across the core capabilities contained within this document. Their needs must be taken into consideration as part of any integrated planning effort.

[5] Access and functional needs refers to persons who may have additional needs before, during and after an incident in functional areas, including but not limited to: maintaining health, independence, communication, transportation, support, services, self-determination, and medical care. Individuals in need of additional response assistance may include those who have disabilities; live in institutionalized settings; are older adults; are children; are from diverse cultures; have limited English proficiency or are non-English speaking; or are transportation disadvantaged.

people with limited English proficiency. Their contributions must be integrated into the Nation's efforts, and their needs must be incorporated as the whole community plans and executes the core capabilities.

Scope

Protection core capabilities are a key component of preparedness. In large part, the structures and capabilities needed to achieve the Protection mission end-state build upon existing doctrine, plans, and activities. The Protection mission includes actions to deter threats, reduce vulnerabilities, or minimize the consequences associated with an incident. Effective Protection relies upon the close coordination and alignment of practices across the whole community as well as with international partners and organizations.

The National Protection Framework focuses on Protection core capabilities that are applicable during both steady-state conditions and the escalated decision making and enhanced Protection operations before or during an incident and in response to elevated threat. Steady-state conditions call for routine, normal, day-to-day operations. Enhanced conditions call for augmented operations that take place during temporary periods of elevated threat, heightened alert, or during periods of incident response in support of planned special events in which additional or enhanced protection activities are needed.[6] The National Protection and Prevention Frameworks share three core capabilities, and these mission areas are expected to operate seamlessly when needed. For this reason, the Protection Framework is closely aligned with the Prevention Framework. The Protection Framework addresses core capabilities that contribute to protecting the Nation domestically.

The core capabilities for Protection enable a range of activities that include, but are not limited to, the following:[7]

- **Border Security.** Securing U.S. air, land, sea ports, and borders against the illegal flow of people and goods, while facilitating the flow of lawful travel and commerce.
- **Critical Infrastructure Protection.** Protecting the physical and cyber elements of critical infrastructure. This includes actions to deter the threat, reduce vulnerabilities, or minimize the consequences associated with a terrorist attack, natural disaster, or manmade disaster. Critical Infrastructure Protection is an element of critical infrastructure security and resilience as detailed in Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience.[8]

[6] This includes elevated threat of terrorism as described in the National Terrorism Advisory System, or NTAS, and all-hazards monitoring, as well heightened activity around emergent and persistent risk issues that involve Protection capabilities.

[7] As with all activities supporting the National Preparedness Goal, activities under the Protection mission area must be consistent with all pertinent statutes and policies, particularly those involving privacy and civil and human rights, such as the Americans with Disabilities Act of 1990, the Rehabilitation Act of 1973, and the Civil Rights Act of 1964.

[8] Critical infrastructure, as defined in PPD-21, includes those 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 safety or health; environment; or any combination of these matters, across any jurisdiction. Critical infrastructure security and resilience addresses sectors along common functions that include chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

- **Cybersecurity.** Securing the cyber environment and infrastructure from unauthorized or malicious access, use, or exploitation while protecting privacy, civil rights, and other civil liberties.
- **Defense against Weapon of Mass Destruction (WMD) Threats.** Protecting the Nation from threats associated with WMD and related materials and technologies including their malicious acquisition, movement, and use within the United States.
- **Defense of Agriculture and Food**. Defending agriculture and food networks and systems from all-hazards threats and incidents.[9]
- **Health Security.** Securing the Nation and its people to be prepared for, protected from, and resilient in the face of health threats or incidents with potentially negative health consequences.
- **Immigration Security.** Securing the Nation from illegal immigration through effective and efficient immigration systems and processes that respect human and civil rights.
- **Maritime Security.** Securing U.S. maritime infrastructure, resources, and the Marine Transportation System from terrorism and other threats and hazards and securing the homeland from an attack from the sea, while preserving civil rights, respecting privacy and protected civil liberties, and enabling legitimate travelers and goods to move efficiently without fear of harm or significant disruption.
- **Protection of Key Leadership and Special Events**. Safeguarding key leadership from hostile acts by terrorists and other malicious actors and to ensure security at events of national significance.[10]
- **Transportation Security.** Securing U.S. transportation systems and the air domain against terrorism and other threats and hazards, while preserving civil rights, respecting privacy and protected civil liberties, and enabling legitimate travelers and goods to move without fear of harm or significant disruption.

Guiding Principles

The following principles guide the development and support the delivery of Protection core capabilities:

1. **Resilience and Scalability.** Effective delivery of the core capabilities for Protection minimizes the risks from all threats and hazards through:
    a. **Resilience.** Resilience is the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions.[11] It may be enhanced through the delivery of

[9] Core capabilities for Protection align with policy established in Homeland Security Presidential Directive (HSPD) 9: Defense of United States Agriculture and Food to include identifying and prioritizing sector critical infrastructure; developing awareness and early warning capabilities; mitigating vulnerabilities; and enhancing screening procedures.

[10] Key leaders are defined as current and former Presidents, Vice Presidents, their families, and others granted such protection under Title 18 U.S.C. Sections 3056 and 3056A. Events of national significance fall within two categories: National Special Security Events (NSSE) as defined in Title 18, U.S.C. Section 3056 and further clarified in PPD-22, and events formally assessed under the Special Event Assessment Rating (SEAR) process by the interagency (DHS, FBI, USSS, and FEMA) Special Event Working Group (SEWG) based on input provided by Federal, state, local law enforcement entities.

[11] See White House, PPD-21: Critical Infrastructure Security and Resilience (Washington, DC, White House, 2013).

core capabilities for Protection and involve a wide range of activities, including improving security protocols; hardening facilities; adopting redundancy; incorporating hazard resistance into facility design and maintenance; initiating active or passive countermeasures; installing security systems; leveraging "self-healing" technologies; promoting workforce surety programs; implementing cybersecurity measures; training and exercises; continuity planning and operations; and restoration and recovery actions.[12]

b. **Scalability.** Scalable capabilities are designed to meet unforeseen, unmet, and evolving needs of varying geographic scope, complexity, and intensity. Scalability allows Protection capabilities to function across jurisdictions and sectors, expanding to meet dynamic mission requirements.

2. **Risk-informed Culture.** A risk-informed culture supports Protection capabilities and requires

   a. **Vigilance and situational awareness** through a national system of monitoring emerging threats and hazards and the risk they pose.

   b. **Information sharing and risk-informed decision making** through coordination mechanisms that allow for the delivery of appropriate information to stakeholders who will use it to guide analysis and action.

3. **Shared Responsibility.** Protection is most effective as a shared responsibility through

   a. **Engaged partnerships** to share information; exchange ideas, approaches, and effective practices; facilitate security planning and resource allocation; establish effective coordinating structures among partners; and build public awareness.

   b. **Integrated processes** across all government and with private and nonprofit sectors partners to more effectively achieve the shared vision of a safe and secure Nation.

Risk Basis

Risk is the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.[13] It is assessed based on applicable threats and hazards, vulnerabilities, and consequences. For the Protection mission area, the emphasis on a risk basis both promotes an understanding of what needs to be protected and ensures that security, resilience, and sustainability guide investment decisions.

Results of the Strategic National Risk Assessment (SNRA), contained in the second edition of the National Preparedness Goal, indicate that a wide range of threats and hazards continue to pose a significant risk to the Nation, affirming the need for an all-hazards, capability-based approach to preparedness planning. The results contained in the Goal include:

- Natural hazards, including hurricanes, earthquakes, tornadoes, droughts, wildfires, winter storms, and floods, present a significant and varied risk across the country. Climate change has the potential to cause the consequence of weather-related hazards to become more severe.
- A virulent strain of pandemic influenza could kill hundreds of thousands of Americans, affect millions more, and result in economic loss. Additional human and animal infectious diseases, including those undiscovered, may present significant risks.

[12] The Protection and Mitigation mission areas work together to increase resilience. For an explanation of the differences and similarities between Protection and Mitigation, refer to the Core Capabilities section of this document.

[13] Department of Homeland Security Risk Steering Committee, *DHS Risk Lexicon*, Washington, DC, 2011.

- Technological and accidental hazards, such as transportation system failures, dam failures, chemical spills or releases, have the potential to cause extensive fatalities and severe economic impacts. In addition, these hazards may increase due to aging infrastructure.
- Terrorist organizations or affiliates may seek to acquire, build, and use WMDs. Conventional terrorist attacks, including those by "lone actors" employing physical threats such as explosives and armed attacks, present a continued risk to the Nation.
- Malicious cyber activities can have catastrophic consequences, which in turn, can lead to other hazards, such as power grid failures or financial system failures. These cascading hazards increase the potential impact of cyber incidents. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk.
- Some incidents, such as explosives attacks or earthquakes, generally cause more localized impacts, while other incidents, such as human pandemics, may cause impacts that are dispersed throughout the Nation, thus creating different types of impacts for preparedness planners to consider.

In addition to these findings, climate change has the potential to adversely impact a number of threats and hazards. Rising sea levels, increasingly powerful storms, and heavier downpours are already contributing to an increased risk of flooding. Droughts and wildfires are becoming more frequent and severe in some areas of the country.

The SNRA results contained in the Goal focus on contingency events, which are typically defined by beginning and end points. The results do not explicitly address a range of persistent steady-state risks, such as border and trade violations, illegal immigration, drug trafficking, and intellectual property violations that account for a significant component of the steady-state Protection. Recognition of routine and ongoing Protection responsibilities along with the SNRA results contained in the Goal guided the development of the National Protection Framework and should inform community-based analysis. Additionally, the whole community must be able to conduct essential functions during an actual hazard or incident to ensure delivery of core capabilities for all mission areas.

Roles and Responsibilities

Many individuals, organizations, and entities are engaged in the Protection mission. Protection partners have varying authorities, capacities, and resources that, when aligned in a risk-informed way, provide the basis for national Protection.

Protection takes place across a continuum of conditions. The roles and responsibilities of Protection partners reflect a decentralized model of coordination and independent action that comprises the national approach to Protection.

Individuals, Families, and Households

Communities share responsibility for understanding the threats and hazards in their locales. Individuals, families, and households should take risk-informed protective actions based on this knowledge. Individuals, families, and households acquire an awareness of potential threats and hazards through sources such as news outlets, local emergency management agencies, public information and warning systems, community education campaigns, and information-sharing mechanisms.

Communities

Communities are unified groups that share goals, values, or purposes, and may operate independently of geographic boundaries or jurisdictions. Communities bring individuals together in different ways for different reasons. They have the ability to promote and implement core capabilities within the Protection mission and share information and effective practices. Communities may include faith-based organizations; neighborhood partnerships; individuals with access and functional needs such as people with disabilities; people from diverse religious, racial, and ethnic communities; online communities; hazard-specific or health coalitions; and professional associations. Communities are instrumental in the development and delivery of Protection capabilities, often leading the way in establishing protection standards of practice, mutual aid agreements, and mechanisms for information sharing. For this reason, communities play a central role in the development of Protection plans and in identifying and implementing solutions to Protection challenges. As risks transect geographical and jurisdictional boundaries, communities are essential partners for understanding how to manage complex Protection issues across multiple spheres of responsibility.

Private Sector Entities

Private sector entities include businesses, industries, private schools, and universities. One particular focus for protection is on owners and operators of the Nation's infrastructure. Owners and operators of both private and public sector infrastructure develop and implement risk-based protective programs and resilience strategies for infrastructure as well as the related information and operations under their control.[14] Owners and operators maintain situational awareness, take actions on a continuous basis to build protection capabilities, and make investments in security and resilience as necessary components of prudent day-to-day business and continuity of operations planning. Private sector entities work together and with public sector entities through established sector coordination bodies established under relevant legal authorities to share information and jointly address public risks. Private sector entities are also central to the development of regulatory measures that address and manage risks across infrastructure sectors.

International Partnerships

While the National Protection Framework focuses largely on domestic activities, Protection capabilities are often interconnected globally. For this reason, Protection efforts with foreign nations and regional and international organizations focus on instituting partnerships with international stakeholders, implementing agreements and instruments that affect protection, and addressing cross-sector and global issues. International partnerships are essential to developing and delivering core capabilities for the Protection mission. Protection efforts with international partners require coordination with the Department of State and, as appropriate, other government entities at the local, regional/metropolitan, state, tribal, territorial, insular area,[15] and Federal levels.

Nongovernmental Organizations

NGOs are encouraged to establish or participate in regional and community preparedness partnerships with the whole community to develop a common understanding of risk and how to address it through their protection efforts. Where applicable, NGOs and faith-based organizations

[14] For the purposes of the National Protection Framework, "owners and operators" include owners and operators both of privately owned businesses and infrastructure as well as publicly owned infrastructure (e.g., public works and utilities).

[15] For the purposes of the National Protection Framework, insular areas include Guam, the Commonwealth of the Northern Mariana Islands, American Samoa, and the U.S. Virgin Islands.

also contribute to the Protection mission as advocates for, or assistance providers to, the entire range of community members by helping communities, individuals, and households to receive protection information and resources.

Local Governments

Local governments have unique responsibilities for the public safety, security, health, and welfare of the people in their jurisdictions. Local governments promote the coordination of ongoing protection plans and the implementation of core capabilities, as well as engagement and information sharing with private sector entities, infrastructure owners and operators, and other jurisdictions and regional entities. Local governments also address unique geographical protection issues, including transborder concerns, dependencies and interdependencies among agencies and enterprises, and, as necessary, the establishment of agreements for cross-jurisdictional and public-private coordination. Local governments are also responsible for ensuring all citizens receive timely information in a variety of accessible formats.

State, Tribal, Territorial, and Insular Area Governments

State, tribal, territorial, and insular area governments are responsible for implementing the Protection mission, protecting public welfare, and ensuring the provision of uninterrupted essential services and information to protect public health and security to communities and infrastructure within their jurisdictions. They address transborder issues and organizational interdependencies and establish coordination agreements. These governments serve an integral role as a conduit for coordination between Federal agencies and local governments.

Federal Government

The President leads the Federal Government protection efforts to prepare the Nation for all hazards, including natural disasters, acts of terrorism, and other emergencies. The Federal Government provides leadership, coordination, and integration for the development and delivery of Protection capabilities. Federal departments and agencies execute national policy directives and implement statutory and regulatory responsibilities for a wide array of protective programs and provide assistance in a number of areas, including funding, acquisition, research, coordination, continuity operations and planning, oversight, implementation, and enforcement.

To deliver the Protection mission, all Federal departments and agencies cooperate with one another, and with local, regional/metropolitan, state, tribal, territorial, insular area, and Federal governments, community members, private and nonprofit sector. The Federal Government, working with all of these partners, contributes to the development and delivery of the core capabilities by implementing national laws, and establishing regulations, guidelines, and standards designed to protect the public while ensuring the free flow of commerce and the protection of privacy, civil rights, and civil liberties. The Federal Government provides integrated public safety and security capabilities and resources for potential or actual incidents requiring a coordinated Federal response.

Federal departments and agencies have differing responsibilities regarding protection. The Protection Federal Interagency Operational Plan (FIOP) provides a detailed description of how the following Federal departments and agencies engage and contribute to the delivery of core capabilities.[16]

- Department of Homeland Security[17]
- Department of Agriculture
- Department of Commerce
- Department of Defense
- Department of Energy
- Department of Health and Human Services[18]
- Department of the Interior

[16] The FIOPs are a required component of the National Preparedness System. Their intent is to provide guidance across the Federal Government to successfully implement the frameworks. The Protection FIOP is discussed further in the Operational Planning section of this document.

[17] By directive of the President, the Secretary of Homeland Security is the principal Federal official for domestic incident management. Pursuant to the Homeland Security Act of 2002, the Secretary is the focal point regarding natural and manmade crises and emergency planning. The primary DHS missions include preventing terrorist attacks within the United States; reducing the vulnerability of the United States to terrorism; minimizing the damage, and assisting in the recovery from terrorist attacks that do occur within the United States; and carrying out all functions of entities transferred to the Department, including by acting as a focal point regarding natural and manmade crises and emergency planning. In order to protect against, mitigate, and, when appropriate, prevent terrorist attacks, major disasters, and other emergencies, the Secretary is responsible for identifying strategic priorities and coordinating domestic all-hazards preparedness efforts of Executive Branch departments and agencies, in consultation with local, state, tribal, and territorial governments, NGOs, private sector partners, and the general public (except for those activities that may interfere with the authority of the Attorney General or the FBI Director). The National Operations Center is the principal operations center for DHS.

[18] The Pandemic and All-Hazards Preparedness Act directs the Secretary of Health and Human Services to develop a National Health Security Strategy with a focus on human health. In addition to the departments and agencies listed here for their unique roles in human, animal, and environmental health, the National Health Security Strategy is supported by the Departments of Homeland Security, Defense, Education, Justice, Labor, State, and Transportation; the Federal Communications Commission; the Office of Personnel Management; and the Executive Office of the President.

- Department of Justice[19]
- Department of State[20]
- Department of Transportation
- Department of the Treasury
- Environmental Protection Agency
- General Services Administration
- Office of the Director of National Intelligence.[21]

The authority for the Protection mission is established in local, regional/metropolitan, state, tribal, territorial, insular area, and Federal laws, regulations, ordinances, and other directives with the force and effect of law. National policy directives and regulations direct Federal agencies to conduct protection activities within and across several critical infrastructure sectors. The National Protection Framework does not change or replace any existing responsibilities and authorities as specified by law, directive, or policy. Federal departments and agencies are required by law to ensure accessible communication, physical access, and programmatic access to ensure all citizens have equal access and equal opportunity.

[19] The Attorney General has lead responsibility for criminal investigations of terrorist acts or terrorist threats by individuals or groups inside the United States, or directed at United States citizens or institutions abroad, where such acts are within the Federal criminal jurisdiction of the United States, as well as for related intelligence collection activities within the United States, subject to the National Security Act of 1947 (as amended) and other applicable law, Executive Order 12333 (as amended), and Attorney General-approved procedures issued pursuant to that Executive Order. Generally acting through the FBI Director, the Attorney General also has primary responsibility for finding and neutralizing WMD within the United States. The Attorney General, generally acting through the FBI Director, leads and coordinates the operational law enforcement response, on-scene law enforcement, and related investigative and appropriate intelligence activities related to terrorist threats and incidents within the U.S., its territories, territorial waters, or on U.S. flagged vessels. This includes the coordination of the law enforcement activities to detect, prevent, preempt, and disrupt terrorist threats. During an imminent threat, the FBI leads and coordinates the operational law enforcement response and on-scene law enforcement and investigative activities through an FBI On-Scene Commander (OSC). Following a terrorist threat or an actual incident that falls within the criminal jurisdiction of the United States, the full capabilities of the United States shall be dedicated, consistent with U.S. law and with activities of other Federal departments and agencies to protect national security, to assist the Attorney General to identify the perpetrators and bring them to justice. The FBI OSC retains the authority to take appropriate law-enforcement actions at all times during the response, to include hostage-rescue, tactical response, render safe, and bomb management operations, and to conduct, direct, and oversee crime scenes, including those involving WMD, their security, and evidence management through all phases of the response. The FBI manages prevention response and counterterrorism operations through the Strategic Information Operations Center and the 56 FBI field offices Joint Operations Centers. For further information, see the Prevention Framework or Prevention FIOP.

[20] As part of the day-to-day diplomatic activities on behalf of the U.S. Government, the Department of State is responsible for establishing and maintaining international partnerships, which are essential to developing and delivering core capabilities for the Protection mission area.

[21] The Director of National Intelligence serves as the head of the Intelligence Community, acts as the principal advisor to the President for intelligence matters relating to national security, and oversees and directs implementation of the National Intelligence Program. The Intelligence Community, comprising elements across the Federal Government, functions consistent with law, executive order, regulations, and policy to support the national security-related missions of the U.S. Government. In addition to Intelligence Community elements with specific homeland security missions, the Office of the Director of National Intelligence maintains a number of mission and support centers that provide unique capabilities, which together support the delivery of all the core capabilities for Protection.

Core Capabilities

The National Preparedness Goal identifies the core capabilities and targets for each of the five mission areas. Table 1 provides a list of the core capabilities by mission area and highlights the relationship of the Protection capabilities to the whole of national preparedness. Many of these core capabilities exist and are used every day for steady-state protection activities. The approach to further developing and delivering these core capabilities will differ according to and across the mission areas.

Table 1: Core Capabilities by Mission Area[22]

<table>
<tr><th>Prevention</th><th>Protection</th><th>Mitigation</th><th>Response</th><th>Recovery</th></tr>
<tr><td colspan="5">Planning</td></tr>
<tr><td colspan="5">Public Information and Warning</td></tr>
<tr><td colspan="5">Operational Coordination</td></tr>
<tr><td colspan="2">Intelligence and Information Sharing</td><td rowspan="4">Community Resilience
Long-term Vulnerability Reduction
Risk and Disaster Resilience Assessment
Threats and Hazards Identification</td><td colspan="2">Infrastructure Systems</td></tr>
<tr><td colspan="2">Interdiction and Disruption</td><td rowspan="3">Critical Transportation
Environmental Response/Health and Safety
Fatality Management Services
Fire Management and Suppression
Logistics and Supply Chain Management
Mass Care Services
Mass Search and Rescue Operations
On-scene Security, Protection, and Law Enforcement
Operational Communications
Public Health, Healthcare, and Emergency Medical Services
Situational Assessment</td><td rowspan="3">Economic Recovery
Health and Social Services
Housing
Natural and Cultural Resources</td></tr>
<tr><td colspan="2">Screening, Search, and Detection</td></tr>
<tr><td>Forensics and Attribution</td><td>Access Control and Identity Verification
Cybersecurity
Physical Protective Measures
Risk Management for Protection Programs and Activities
Supply Chain Integrity and Security</td></tr>
</table>

[22] The National Preparedness Goal outlines the core capabilities for each mission area.

The National Preparedness Goal identifies 11 core capabilities for the Protection mission. Three of these core capabilities (Planning, Public Information and Warning, and Operational Coordination) span all of the mission areas. In addition, the Protection and Prevention mission areas share three core capabilities: Intelligence and Information Sharing; Interdiction and Disruption; and Screening, Search, and Detection. The cross-cutting core capabilities between mission areas provide opportunities for integration and joint capability development. The Prevention mission area focuses on those intelligence, law enforcement, and homeland security activities that prevent an adversary from carrying out a terrorist attack within the United States. Protection and Prevention share a number of common elements and rely on many of the same core capabilities. Many Protection and Prevention processes described in these frameworks are designed to operate simultaneously and to complement each other. Protection and Mitigation share capabilities directly related to risk management. For Protection, the capability is Risk Management for Protection Programs and Activities. For Mitigation, risk management is informed by Long-Term Vulnerability Reduction; Risk and Disaster Resilience Assessment; and Threat and Hazard Identification. The Protection and Mitigation mission areas coordinate through the risk management process as they identify threats and hazards and work to reduce vulnerabilities. Figure 1 is a simplified graphic that conceptually illustrates the interconnectedness of all of the mission areas. The figure calls specific attention to the connections and shared or related core capabilities that align efforts in the context of Protection and Prevention, as well as Protection and Mitigation. Additionally, Protection is linked to Response and Recovery through various core capabilities such as those pertaining to Infrastructure Systems and relevant coordinating structures.

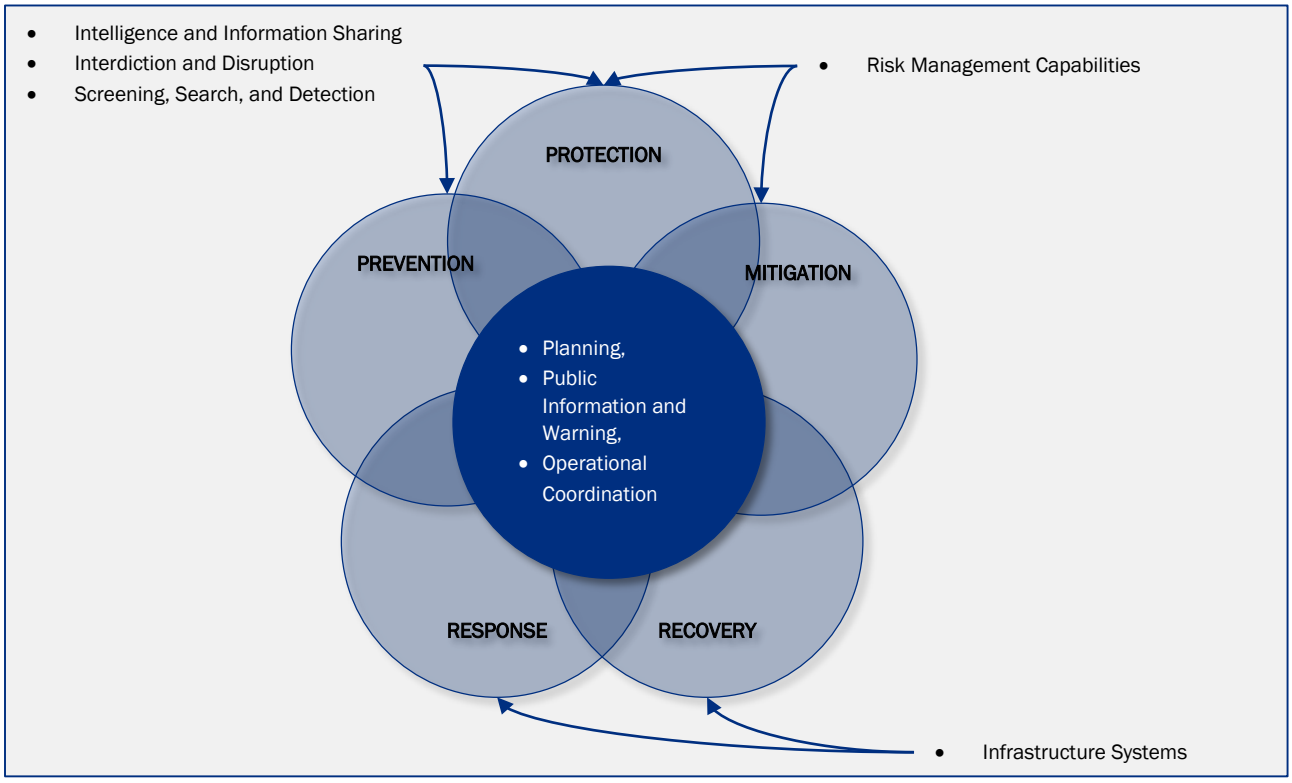

Figure 1: Core Capability Connections

Collectively, the core capabilities for the Protection mission provide the foundation for a secure and resilient Nation that is protected from terrorism and other hazards in a manner that allows American interests, aspirations, and way of life to thrive.

The National Preparedness Goal establishes targets for each of the Protection mission core capabilities. The targets from the Goal were used to identify critical tasks, listed on the following pages. The critical tasks are specific to Protection and can be used to identify tailored goals and objectives.

The critical tasks associated with the Protection core capabilities are ambitious. They are not tasks for any single jurisdiction or agency; rather, achieving them requires a national effort involving the whole community.

Cross-cutting Core Capabilities

The following three core capabilities span all five mission areas: Planning, Public Information and Warning, and Operational Coordination.

Planning

Description: Conduct a systematic process engaging the whole community, as appropriate, in the development of executable strategic, operational, and/or tactical-level approaches to meet defined objectives. Planning includes the development exercise and maintenance of multidisciplinary plans that provide joint guidance across Protection mission activities.

Critical Tasks

- Initiate a flexible planning process that builds on existing plans as part of the National Planning System.
- Establish partnerships that facilitate coordinated information sharing between partners to support the protection of critical infrastructure within single and across multiple jurisdictions and sectors.
- Identify and prioritize critical infrastructure and determine risk management priorities.
- Conduct vulnerability assessments, perform risk analyses, identify capability gaps, and coordinate protective measures on an ongoing basis in conjunction with the private and nonprofit sectors and local, regional/metropolitan, state, tribal, territorial, insular area, and Federal organizations and agencies.
- Establish joint Protection objectives within and across mission area activities.
- Implement security, protection, resilience, and continuity plans and programs, and training and exercises, and take corrective actions.
- Integrate Protection planning for the whole community and those with animals (including household pets and service and assistance animals); develop and document continuity plans and supporting procedures so that, when implemented, the plans and procedures provide for the continued performance of essential functions under all circumstances.
- Ensure that Protection planning and activities mutually support, and do not conflict with or adversely affect, other mission area plans and activities, especially with analytic and risk management products, and complementary concepts of operation. .

Public Information and Warning

Description: Deliver coordinated, prompt, reliable, and actionable information to the whole community through the use of clear, consistent, accessible, and culturally and linguistically appropriate methods to effectively relay information regarding any threat or hazard and, as appropriate, the actions being taken and the assistance made available.

Public Information and Warning uses effective and accessible indications and warning systems to communicate significant threats and hazards to involved operators, security officials, and the public (including alerts, detection capabilities, and other necessary and appropriate assets).[23]

Critical Tasks

- Execute public awareness campaigns to enhance vigilance.
- Determine requirements for Protection stakeholder information and information sharing.
- Determine information sharing requirements and processes to address the communication needs of the whole community.
- Establish accessible mechanisms and provide the full spectrum of support necessary for appropriate and ongoing information sharing among all levels of government, the private sector, faith-based organizations, NGOs, and the public.
- Promptly share actionable information with the public and among all levels of government, the private and nonprofit sector.
- Leverage all appropriate communication means, such as the Integrated Public Alert and Warning System, National Terrorism Advisory System, and social media sites and technology.
- Counter violent extremist messages via social media and other forms of public information.

Operational Coordination

Description: Establish and maintain a unified and coordinated operational structure and process that appropriately integrates all critical stakeholders and supports the execution of core capabilities.

Operational Coordination supports networking, planning, and coordination between protection partners.

Critical Tasks

- Establish joint concepts of operation for delivering Protection capabilities.
- Collaborate with all relevant protection partners.
- Determine jurisdictional priorities, objectives, strategies, and resource allocations.
- Establish clear lines and modes of communication among participating organizations and jurisdictions.
- Define and communicate clear roles and responsibilities relative to courses of action.
- Integrate and synchronize the actions of participating organizations and jurisdictions to ensure unity of effort.
- Coordinate across and among all levels of government and with critical private and nonprofit sector to protect against potential threats, conduct law enforcement investigations, or engage in enforcement and protective activities based on jurisdictional authorities.
- Build mechanisms to enable interoperable communications to enhance coordination around protection mission.

[23] Public Information and Warning systems must provide effective communication to individuals with disabilities, such as audio and video captioning for multimedia and use-accessible Web sites. Public Information and Warning should also be communicated using various languages and culturally diverse media outlets.

- Coordinate across mission areas to deliver Protection capabilities in support of national preparedness.

Protection and Prevention Core Capabilities

The following core capabilities span the Protection and Prevention mission areas: Intelligence and Information Sharing; Interdiction and Disruption; and Screening, Search, and Detection. These capabilities are addressed here in a Protection context. For a description of these capabilities in a Prevention context, see the Prevention Framework.

Intelligence and Information Sharing

Description: Intelligence sharing is providing timely, accurate, and actionable information resulting from the planning direction, collection, exploitation, processing, analysis, production, dissemination, evaluation, and feedback of available information concerning threats to the United States, its people, property, or interests; the development, proliferation, or use of WMD; or any other matter bearing on U.S. national or homeland security by local, state, tribal, territorial, Federal, and other stakeholders.[24]

Information sharing is the ability to exchange intelligence, information, data, or knowledge among government or private sector entities, as appropriate.

Intelligence and information are essential to guide the strategic development of other Protection capabilities and to inform Protection actions. All actions in the National Protection Framework rely on the monitoring, gathering, and analysis of intelligence and information. Intelligence and information sharing as a capability requires the cultivation of analytic capacity, and the development and use of networks, procedures, and formats for the distribution of analytic products.

In the context of Protection, Intelligence and Information Sharing capabilities involve the effective execution of the intelligence cycle and other information collection and sharing processes by local, regional/metropolitan, state, tribal, territorial, insular area, and Federal, the private and nonprofit sector, and the public to develop situational awareness of potential threats and hazards within the United States.

Lawful sharing of information through robust and collaborative partnerships, coupled with coordinated interactions that increase situational awareness, strengthen the Protection mission. The U.S. Government promotes an information sharing culture, deploys new technologies, and refines its policies and procedures in support of its commitment to share timely, relevant, and actionable intelligence and other information to the widest appropriate audience.

Critical Tasks

- Monitor, analyze, and assess the positive and negative impacts of changes in the operating environment as it pertains to threats and hazards to public safety, health, and security. Share analysis results through
  - Participation in public, local, regional, state, tribal, territorial, and national education and awareness programs; and
  - Participation in the routine exchange of security information—including threat assessments, alerts, attack indications and warnings, and advisories—among partners.

[24] Intelligence cycle processes include the following steps: planning; direction; the collection, exploitation, processing, and analysis of available information; production; dissemination; evaluation; and feedback.

- Determine intelligence and information sharing requirements for protection stakeholder intelligence, information, and information sharing.
- Develop or identify and provide access to mechanisms and procedures for intelligence and information sharing between the public, private sector, faith-based, and government protection partners.[25]
- Use intelligence processes to produce and deliver relevant, timely, accessible, and actionable intelligence and information products to others as applicable, to include partners in the other mission areas.
- Adhere to appropriate mechanisms for safeguarding sensitive and classified information and protecting privacy, civil rights, and civil liberties.

Interdiction and Disruption

Description: Delay, divert, intercept, halt, apprehend, or secure threats and/or hazards. These threats and hazards include people, materials, or activities that pose a threat to the Nation, including domestic and transnational criminal and terrorist activities and the malicious movement and acquisition/transfer of chemical, biological, radiological, nuclear, and explosive (CBRNE) materials and related technologies.

In the context of Protection, this capability includes those interdiction and disruption activities undertaken in response to elevated threats, or focusing capabilities during special events.

Interdiction and disruption activities conducted by law enforcement and public and private sector security personnel during the course of their routine duties include the enforcement of border authorities at and between ports of entry into the United States.

Critical Tasks

- Deter movement and operation of terrorists into or within the United States and its territories.
- Ensure the capacity to detect CBRNE devices or resolve CBRNE threats.
- Interdict conveyances, cargo, and persons associated with a potential threat or act.
- Implement public health measures to mitigate the spread of disease threats abroad and prevent disease threats from crossing national borders.
- Disrupt terrorist financing or conduct counter-acquisition activities to prevent weapons, precursors, related technology, or other material support from reaching its target.
- Enhance the visible presence of law enforcement to deter or disrupt threats from reaching potential target(s).
- Intervene to protect against the spread of violent extremism within U.S. communities.

[25] Information sharing must provide effective communication to individuals with access and functional needs including people with limited English proficiency and people with disabilities, including people who are deaf or hard-of-hearing and people who are blind or have low vision. Effective communication with individuals with access and functional needs includes use of appropriate auxiliary aids and services, such as sign language and other interpreters, captioning of audio and video materials and user-accessible Web sites, communication in various languages, and use of culturally diverse media outlets.

- Employ wide-area search and detection assets in targeted areas in concert with local, regional/metropolitan, state, tribal, territorial, insular area, and Federal personnel or other Federal agencies (depending on the threat).

Screening, Search, and Detection

Description: Identify, discover, or locate threats and/or hazards through active and passive surveillance and search procedures. These activities may include the use of systematic examinations and assessments, biosurveillance, sensor technologies, or physical investigation and intelligence.

In the context of Protection, this capability includes the screening of cargo, conveyances, mail, baggage, and people, as well as the detection of WMD, traditional and emerging threats, and hazards of concern.

Screening, search, and detection actions safeguard residents, visitors, and critical assets, systems, and networks against the most dangerous threats to the Nation without unduly hampering commerce.

Critical Tasks

- Identify potential threats resulting from persons or networks.
- Develop and engage an observant Nation (individuals, families, communities, and local, state, tribal, and territorial government and private sector partners).
- Screen persons, baggage, mail, cargo, and conveyances using technical, non-technical, intrusive, and non-intrusive means without unduly hampering the flow of legitimate commerce. Consider additional measures for high-risk persons, conveyances, or items:
  - Conduct CBRNE search and detection operations.
  - Conduct passive and active detection of CBRNE agents.
  - Operate safely in a hazardous environment.
  - Consider the deployment of Federal teams and capabilities to enhance local, regional/metropolitan, state, tribal, territorial, insular area, and Federal, including the use of incident assessment and awareness assets.
- Conduct biosurveillance of data relating to human health, animal, plant, food, water, and environmental domains.

Core Capabilities Unique to Protection

The remaining core capabilities are unique to Protection: Access Control and Identity Verification; Cybersecurity; Physical Protective Measures; Risk Management for Protection Programs and Activities; and Supply Chain Integrity and Security.

Access Control and Identity Verification

Description: Apply and support necessary physical, technological, and cyber measures to control admittance to critical locations and systems.

This capability relies on the implementation and maintenance of protocols to verify identity and authorize, grant, or deny physical and cyber access to specific locations, information, and networks.

Critical Tasks

- Verify identity to authorize, grant, or deny physical and cyber access to physical and cyber assets, networks, applications, and systems that could be exploited to do harm.
- Control and limit access to critical locations and systems to authorized individuals carrying out legitimate activities.

Cybersecurity

Description: Protect (and, if needed, restore) electronic communications systems, information, and services from damage, unauthorized use, and exploitation.

Cybersecurity activities ensure the security, reliability, integrity, and availability of critical information, records, and communications systems and services through collaborative cybersecurity initiatives and efforts.

Critical Tasks

- Implement countermeasures, technologies, and policies to protect physical and cyber assets, networks, applications, and systems that could be exploited to do harm.
- Secure, to the extent possible, public and private networks and critical infrastructure (e.g., communication, financial, power grid, water, and transportation systems), based on vulnerability results from risk assessment, mitigation, and incident response capabilities.
- Formalize partnerships with governmental and private sector cyber incident or emergency response teams to accept, triage, and collaboratively respond to incidents in an efficient manner.
- Formalize partnerships between communities and disciplines responsible for cybersecurity and physical systems dependent on cybersecurity.
- Formalize relationships between information communications technology and information system vendors and their customers for ongoing product cyber security, business planning, and transition to response and recovery when necessary.
- Share actionable cyber threat information with the domestic and international government, and private sectors to promote shared situational awareness.
- Implement risk-informed standards to ensure the security, reliability, integrity, and availability of critical information, records, and communications systems and services through collaborative cybersecurity initiatives and efforts.
- Detect and analyze malicious activity and support mitigation activities.
- Collaborate with partners to develop plans and processes to facilitate coordinated incident response activities.
- Leverage law enforcement and intelligence assets to identify, track, investigate, disrupt, and prosecute malicious actors threatening the security of the Nation’s public and private information systems.
- Create resilient cyber systems that allow for the uninterrupted continuation of essential functions.

Physical Protective Measures

Description: Implement and maintain risk-informed countermeasures, and policies protecting people, borders, structures, materials, products, and systems associated with key operational activities and critical infrastructure sectors.

This capability includes reducing or mitigating risks, including actions targeted at threats, vulnerabilities, and/or consequences, by controlling movement and protecting borders, critical infrastructure, and the homeland.

Critical Tasks

- Identify and prioritize assets, systems, networks, and functions that need to be protected.
- Identify necessary physical protections, countermeasures (including medical and non-pharmaceutical countermeasures), and policies through a risk assessment of key operational activities and infrastructure.
- Protect critical lifeline functions, which include energy, communications, transportation, and water and wastewater management.
- Develop and implement security plans, including business continuity plans, that address identified security risks.
- Develop and implement risk-based physical security measures, countermeasures, policies, and procedures.
- Implement security training for workers focused on awareness and response.
- Develop and implement biosecurity and biosafety programs and practices.
- Leverage Federal acquisition programs, as appropriate, to ensure maximum cost efficiency, security, and interoperability of procurements.

Risk Management for Protection Programs and Activities

Description: Identify, assess, and prioritize risks to inform Protection activities, countermeasures, and investments. This goal is accomplished by implementing and maintaining risk assessment processes to identify and prioritize assets, systems, networks, and functions, as well as implementing and maintaining appropriate tools to identify and assess threats, vulnerabilities, and consequences.

Risk management is a systemic and analytical process to consider the likelihood that a threat will endanger an asset, individual, or function and to identify actions to reduce the risk and mitigate the consequences. Threat assessments are a decision support tool that can assist in security program planning. Threat assessments identify and provide an evaluation of threats based on various factors, including capability and intentions, as well as the potential lethality and other consequences of an incident.

Critical Tasks

- Gather required data in a timely and accurate manner to effectively identify risks.
- Develop and use appropriate tools to identify and assess threats, vulnerabilities, and consequences.
- Build the capability within communities to analyze and assess risk and resilience.
- Identify, implement, and monitor risk management plans.

- Update risk assessments to reassess risk based on changes in the following areas: the physical environment (including climate change impacts), aging infrastructure, new development, new mitigation projects and initiatives, post-event verification/validation, new technologies or improved methodologies, and better or more up-to-date data.
- Validate, calibrate, and enhance risk assessments by relying on experience, lessons learned, and knowledge beyond raw data or models.
- Use risk assessments to design exercises and determine the feasibility of mitigation projects and initiatives.
- Develop a unified approach to make investments in secure and resilient infrastructure in order to enable communities to withstand the effects of a disaster, respond effectively, recover quickly, adapt to changing conditions, and manage future disaster risk.

Supply Chain Integrity and Security

Description: Strengthen the security and resilience of the supply chain. This capability relies on securing and making resilient key nodes, methods of transport between nodes, and materials in transit between a supplier and consumer.

The expansive nature of the global supply chain renders it vulnerable to disruption from intentional or naturally occurring causes. The multimodal, international nature of the global supply chain system requires a broad effort that includes input from stakeholders from the public and private sectors, both international and domestic. Protection relies on a layered, risk-based, and balanced approach in which necessary security measures and resiliency planning are integrated into supply chains.

Critical Tasks

- Integrate security processes into supply chain operations to identify items of concern and resolve them as early in the process as possible.
- Analyze key dependencies and interdependencies related to supply chain operations.[26]
- Use risk management principles to identify, mitigate vulnerabilities of, and protect key assets, infrastructure, and support systems.
- Implement physical protections, countermeasures, and policies to secure and make resilient key nodes, methods of transport between nodes, and materials in transit.
- Use verification and detection capabilities to identify goods that are not what they are represented to be, are contaminated, are not declared, or are prohibited; and to prevent cargo from being compromised or misdirected as it moves through the system.
- Use layers of defense to protect against a diverse range of traditional and asymmetric threats. These layers include intelligence and information analysis; appropriate use of technology; effective laws, regulations, and policies; properly trained and equipped personnel; and effective partnerships.

[26] Dependency is a one-directional reliance on input, interaction, or another source in order to function properly. Interdependency is a mutually reliant relationship between objects, individuals, or groups. The degree of interdependency does not need to be equal in both directions.

Coordinating Structures and Integration

Coordinating structures are the mechanisms that sustain and deliver core capabilities. The National Protection Framework relies on a wide array of existing coordinating structures across the whole community, and identifies a unified approach that aligns various jurisdictions, mission activities, and areas of responsibility, to address complex and interdisciplinary Protection issues. Coordinating structures support steady state Protection mission activities and strengthen the Nation's ability to increase its protective posture during periods of heightened alert, periods of incident response, or in support of planned special events. These structures are used to conduct planning, implement training and exercise programs, promote information sharing, shape research and development priorities and technical requirements, address common vulnerabilities, align resources, and promote the delivery of Protection capabilities. The range of coordinating structures that contribute to the Protection mission includes operations centers, law enforcement task forces, critical infrastructure partnerships, governance boards, regional consortiums, information-sharing mechanisms such as state and major urban area fusion centers, health surveillance networks, and public-private partnership organizations at all levels.

This section outlines broad national categories of coordinating structures and provides a unified approach for how those structures work together to deliver the Protection mission.

- Community, Local, Tribal, State, and Regional Coordinating Structures
  - Partnerships
  - Operational Coordination
  - Coordination Through Established Systems and Principles
- Federal Coordinating Structures
  - National Security Council
  - Federal Departments and Agencies
  - Interagency Coordination
- Working Across Coordinating Structures

Community, Local, Tribal, State, and Regional Coordinating Structures

Coordination through Partnerships

Protection mission capabilities are coordinated through existing partnerships at all levels of government and with the private and nonprofit sector. There are numerous examples of existing protection partnerships or coalitions, ranging from neighborhood-based programs to regional public-private councils, joint task forces, healthcare coalitions, and infrastructure protection coordinating councils. Many established community and regional groups promote actions to support protection and preparedness. These partnerships may cross critical infrastructure sectors and geographical boundaries. They allow for the exchange of expertise and information and provide a source of potential resources through mutual aid and assistance agreements.

The National Infrastructure Protection Plan (NIPP), for example, promotes the shared responsibility for critical infrastructure security and resilience efforts among all levels of government and critical infrastructure owners and operators. While not the only public-private partnership in the U.S.

Government, this partnership focuses on the security and resilience of critical infrastructure. Sector-specific agencies (SSA) provide expertise and day-to-day engagement for critical infrastructure security and resilience activities in specified sectors.[27] Each sector has built partnerships with sector stakeholders, including facility owners and operators; local, regional/metropolitan, state, tribal, territorial, insular area, and Federal agencies; the law enforcement community; trade associations; and state homeland security advisors. The established sector, government, and cross-sector councils and information sharing mechanisms, such as Information Sharing and Analysis Organizations, are among the foundational structures for protection planning, risk management, and the implementation of protective programs for better physical and cybersecurity. SSAs are responsible for working with both public and private partners to develop security and resilience programs and strategies.

Because of the specific challenges and interdependencies facing individual regions and the broad range and diversity of public and private and nonprofit sector, regional efforts are often complex. Examples of regional partnerships formed to consider regional issues range from the Pacific NorthWest Economic Region (PNWER) partnership,[28] whose working groups look at such issues as border security, agriculture, and energy, to regional partnerships that focus primarily on a single infrastructure sector, such as the Multi-state Partnership for Security in Agriculture.[29]

Voluntary public/private collaboration and information sharing between public and private sector and nonprofit sector is essential to meeting critical objectives for core capabilities within the Protection mission and sustaining programs.

Operational Coordination

In most jurisdictions, the coordinated delivery of core capabilities for Protection occurs through the decentralized coordination of the whole community. State and major urban fusion centers support and inform operational coordination by serving as focal points within the local, tribal, and state environments for the receipt, analysis, gathering, and sharing of threat-related information between government, private and nonprofit sector. Likewise, local, tribal, and state operations centers serve to align and adjudicate resources in support of Protection partners. DHS coordinates critical infrastructure security and resilience activities through the National Infrastructure Coordinating Center and the National Cybersecurity and Communications Integration Center, but equally supports ongoing operational coordination through the sector coordination structures that orient the national effort to coordinate between public and private sector partners. Joint Terrorism Task Forces are FBI-led multijurisdictional task forces established to conduct terrorism-related investigations and are based in over 100 cities nationwide. FBI Joint Terrorism Task Forces focus primarily on terrorism-related issues, with specific regard to terrorism investigations with local, regional, national, and international implications. Coordination among these Centers and Task Forces and information sharing with operations and fusion centers help inform Prevention, Protection, Response, and Recovery activities. These centers also contribute insights and lessons learned to shape Mitigation planning efforts.

[27] The SSAs that provide expertise and day-to-day engagement for critical infrastructure security and resilience for specified sectors are identified in PPD-21: Critical Infrastructure Security and Resilience. PPD-21 also provides that, in addition to the responsibilities given to the SSAs, other Federal departments and agencies have special functions relating to critical infrastructure security and resilience.

[28] Founded in 1991, PNWER is a statutory, bi-national, public/private partnership. PNWER facilitates working groups of public and private leaders to address issues impacting the Pacific Northwest regional economy.

[29] Founded in 2004, the Multi-State Partnership for Security in Agriculture is a 14-state consortium that recognizes that agricultural disasters could have regional, national, and global effects.

Coordination through Established Systems and Principles

The National Protection Framework promotes the use of principles, such as those contained in the NIMS to coordinate core capabilities within the Protection mission across all levels of government, the private and nonprofit sector. The NIMS, for example, provides guidelines to enable organizations with different legal, geographic, and functional responsibilities to coordinate, plan, and interact effectively. Each participating organization maintains its authority, responsibility, and accountability. The NIMS components, concepts, and principles support the transition of organizations with active roles in multiple mission areas.

Federal Coordinating Structures

At the Federal level, an array of coordinating structures exist to facilitate partnerships, planning, information sharing, and resource and operational synchronization across all aspects of the Protection mission. This section focuses on the policy-level coordination conducted through White House leadership, public-private partnerships, and those structures in place or to be established to ensure a coordinated approach to protection across the whole community.

National Security Council

The National Security Council is the principal policy body for consideration of national security policy issues requiring Presidential determination. The National Security Council advises and assists the President in integrating all aspects of national security policy as it affects the United States—domestic, foreign, military, intelligence, and economic (in conjunction with the National Economic Council). Along with its subordinate committees, the National Security Council is the President's principal means for coordinating Executive Branch departments and agencies in the development and implementation of national security policy.

Federal Departments and Agencies

In addition to the Secretary of Homeland Security's statutory and other responsibilities, the Secretary of Homeland Security is responsible for coordinating the domestic all-hazards preparedness efforts of all Executive Branch departments and agencies, in consultation with local, state, tribal, and territorial governments, private and nonprofit sector, and the general public.[30] The heads of all Executive Branch departments and agencies with a role in Protection are responsible for national preparedness efforts consistent with their statutory roles and responsibilities.[31]

The Federal Government promotes coordination within the Protection mission through a wide range of coordinating structures. Under the National Protection Framework, various Federal departments or agencies assume primary coordinating roles based on their authorities and the nature of the threat or hazard. These Federal departments and agencies provide the basis for the ongoing coordination and collaboration that will be required to promote implementation and ensure the ongoing management and maintenance of the National Protection Framework and other Protection preparedness efforts.

The Secretary of Homeland Security will convene, as appropriate, a meeting or meetings among Federal department and agency representatives to discuss and consider the coordination of core capabilities within the Protection mission, focusing on the following:

[30] Except for those activities that may interfere with the authority of the Attorney General or the FBI Director.
[31] Specific statutory and other responsibilities of Federal departments and agencies are identified in the Roles and Responsibilities section.

- Preparedness planning and coordination in accordance with the National Protection Framework and other National Preparedness System implementation efforts.
- Information sharing pertinent to protection activities.
- Collaboration across the whole community.
- Common concerns and recommended courses of action.
- Integration with Prevention, Mitigation, Response, and Recovery by coordinating with similar groups within those mission areas.

Interagency Coordination

In response to increased risk, or the requirement for heightened activity around Protection Mission issues, the Secretary of Homeland Security may notify Departments and Agencies of the need to support the escalated decision process outlined in this framework. Alternately, leadership within Departments and Agencies may notify the Secretary of Homeland Security of such a need. Federal Department and Agency leadership may convene through existing DHS or interagency coordination forums to support interagency Protection planning for the management and resolution of exigent or pressing Protection issues. Such escalated coordination does not have a fixed function or set of responsibilities, but convenes based on the nature and requirements of emergent Protection issues. During steady-state operations, standing interagency coordination groups within the ten Protection coordinating activities convene to coordinate planning and information sharing efforts across the federal government.

Working across Coordinating Structures

Protection activities and missions are coordinated within a series of overlapping spheres of authority, capability, and function. The laws that provide authority to government entities, and the professional arrangements that govern the conduct of Protection mission activities also provide the model by which Protection activity is coordinated to secure the Nation against complex threats and hazards. In the same sense that threats and hazards impact multiple disciplines and cut across the boundaries of sectors and jurisdictions, the arrangements within the Protection mission are unified by establishing connections across existing coordination structures.

Coordination structures are integrated by the joint development of national capabilities, and the cultivation of joint plans, analytic products, and conduits for information sharing that span national preparedness mission areas.

Protection Actions to Deliver Core Capabilities

Steady-state Protection Process

This section summarizes the process to identify the measures necessary to protect against threats and hazards under steady-state conditions. The responsibility for steady-state Protection is shared by the protection community, including individuals and their households, all levels of government, private and nonprofit sector.

All entities that are responsible for Protection—including governments at all levels, critical infrastructure owners and operators, and businesses—are encouraged to use the steady-state coordinating process to identify the core capabilities needed to accomplish the Protection mission. Figure 2 depicts the steady-state Protection process.

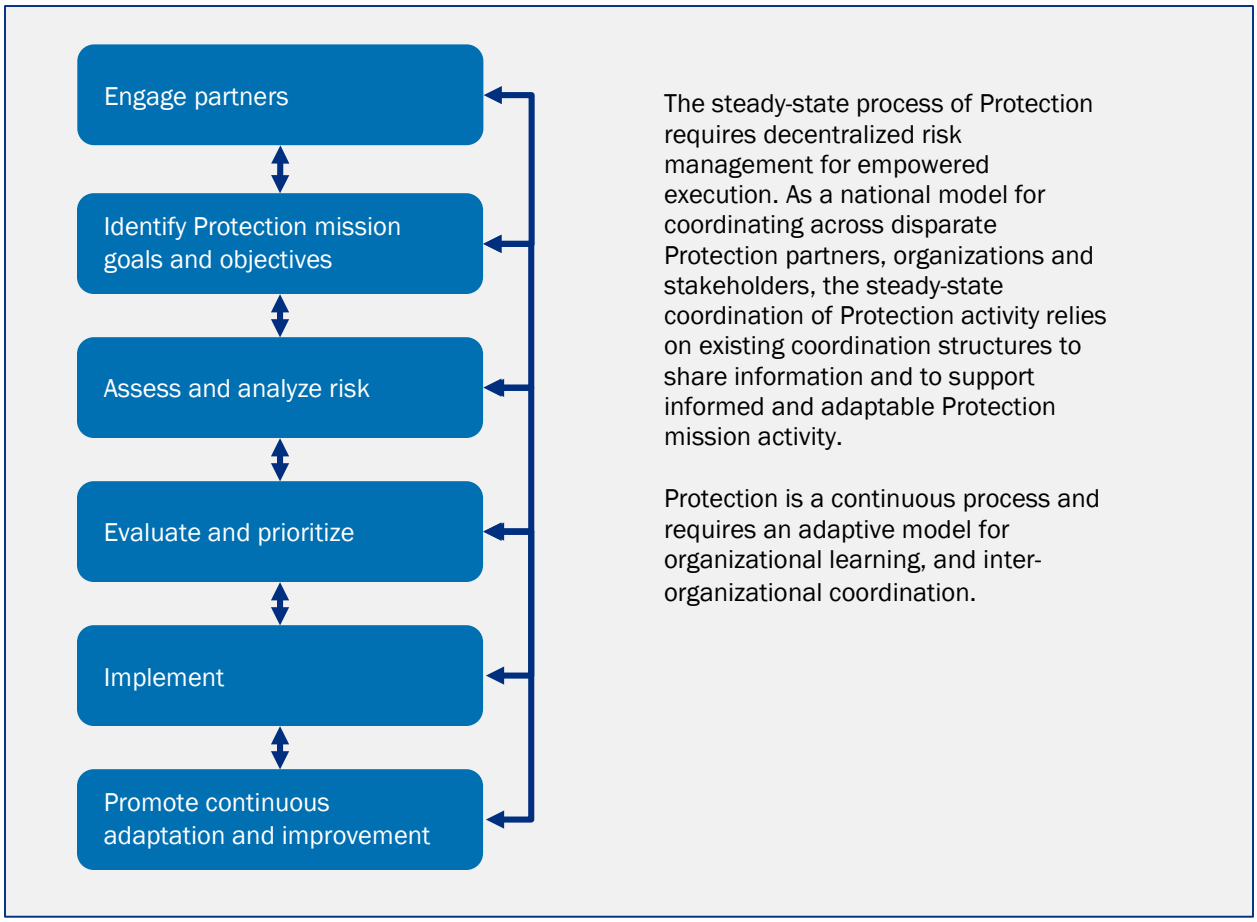

Figure 2: Steady-state Protection Process

1. **Engage partners.** This step of the Protection cycle determines the size and scope of the community or jurisdiction's local coordinating structures by identifying additional protection partners. Protection partners will identify the core capabilities needed based on the Protection mission and delineate the roles and responsibilities for each protection partner.

2. **Identify Protection mission goals and objectives.** The second step of the process is to identify exactly what the community or jurisdiction is trying to protect. Desired goals and objectives may vary across and within jurisdictions or areas of responsibility, depending on the risk landscape and operating environment. Goals and objectives that are collaboratively derived help establish a common vision of the desired long-term security posture and recovery criteria and should reflect the broad protection goals of the full range of partners. Protection partners also can draw on these goals during risk management to best determine which specific Protection core capabilities and risk-reduction and protective strategies most significantly enhance security in the area. Steps in the Protection process should include identifying opportunities to build resilience into planning and implementation efforts.

3. **Assess and analyze risk.** During this step, Protection partners assess and analyze risks to obtain a common risk picture. A specific methodology for the risk assessment is not prescribed.[32] Whatever the method used, it is important to assess potential threats, hazards, vulnerabilities, and consequences in a way that allows them to be compared and prioritized. During this step, Protection partners gather data concerning potential threats and hazards from international and domestic terrorism, manmade and natural disasters, climate change, and infrastructure failures. Data gathering identifies potential issues, challenges, or vulnerabilities that may be associated with the specific activity or the size and scope of the Protection mission. The process involves research of current and historical information. Historical information is useful in assessing the likelihood of occurrence and consequences of potential threats and hazards. This information will be used to inform the risk assessment and other requirements.
4. **Evaluate and prioritize.** In this step, Protection partners use risk analysis results to evaluate their Protection activities for potential risks. Partners also prioritize their Protection capability needs and efforts, taking into account mission goals and objectives.
5. **Informed, Decentralized, and Empowered Action.** In this step, Protection partners take action to achieve the identified Protection goals and objectives. They implement protective activities to address the priorities established earlier in the process under distinct authorities and in coordination with other mission partners.
6. **Promote continuous adaptation and improvement.** This step includes actions that ensure continuous improvement, such as training and exercises, identifying lessons learned, and reviewing evaluation results. Adaptability to changing risks occurs alongside improved efficiency. This process may lead the community or jurisdiction to revisit any of the previous steps in the process.

Protection Escalation Decision Process

Interagency coordination may be compressed during periods of elevated threat or impending disasters. In this instance, communities move quickly to coordinate multiple jurisdictional protection activities (e.g., information sharing; interagency course of action development; communications planning/coordination; assessments, analysis, and modeling; alert and deployment of resources; and other activities required) in consultation and coordination with Federal departments and agencies and the affected jurisdiction(s). Figure 3 depicts this protection escalation decision process.

[32] Comprehensive Preparedness Guide 201, Second Edition provides communities additional guidance for conducting a Threat and Hazard Identification and Risk Assessment (THIRA). For critical infrastructure security and resilience, the National Infrastructure Protection Plan provides criteria that need to be met for risk assessment methodologies. For additional information, refer to the National Infrastructure Protection Plan.

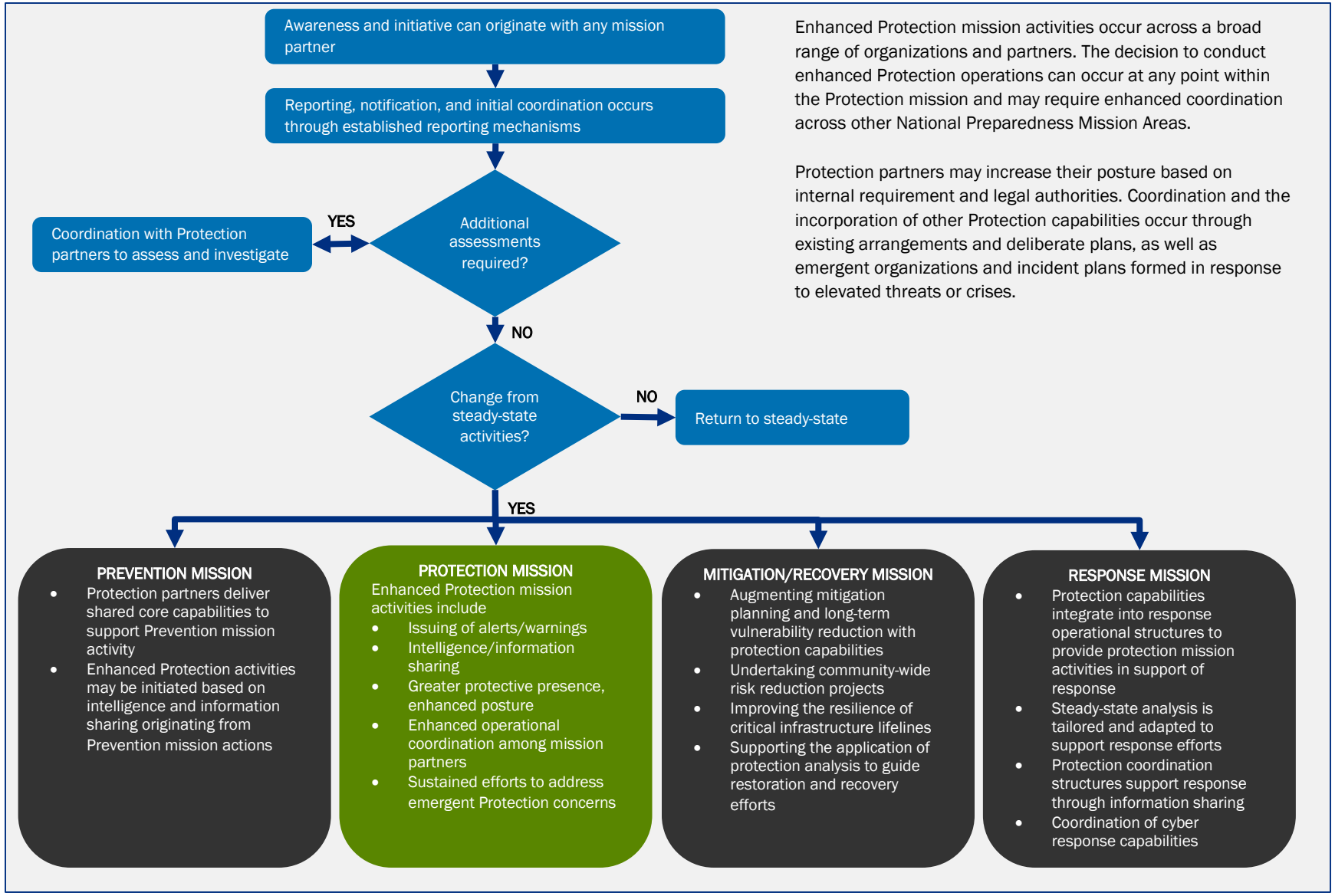

Figure 3: Protection Escalation Decision Process

- **Awareness and initiative**. The need to escalate Protection activities and coordinate across multiple partners can occur anywhere within the scope of Protection mission activities. The decision to initiate actions that result in a heightened level of Protection activity and involve other partners are the result of leadership on the part of Protection partners and coordination across the whole community.
- **Reporting and notifications.** The whole community shares information about potential threats and hazards using established communications and reporting channels. Depending on the type of threat or hazard, governmental, private and nonprofit sector are either required or encouraged to report the potential threat and hazard information using existing mechanisms and legal requirements. Examples include law enforcement, health, and established partnership communications and reporting channels.
- **Assessments.** Governments at all levels maintain emergency operations, watch, and response centers to maintain situational awareness and analyze potential threats and consequences. An assessment of the emerging threat as credible and of the threat as exigent would signal a change from steady-state activities and require action in accordance with the National Response Framework, along with enhanced steady-state Protection and Mitigation activities. An assessment of the emerging threat as a potential terrorist threat may require action in accordance with the National Prevention Framework.
- **Response and enhanced steady-state protection activities.** Following an assessment of the situation, the situation may require the initiation of Prevention, Mitigation, Response, or Recovery activities that require Protection mission support. Emerging issues may also require a change from protection steady-state to enhanced steady-state activities. The importance of existing partnership structures and information sharing channels increases with the need for enhanced steady-state activities. The following are examples of Protection activities taken during enhanced steady-state:
    - Sharing of threat information including the issuances of watches, warnings, and other emergency bulletins. For example, the National Weather Service issues weather-related notices to warn the public of impending storms and severe weather. A number of health surveillance systems are used routinely at the local, state, tribal, and national levels to monitor health risks. The National Terrorism Advisory System communicates information about terrorist threats to the whole community.
    - Sharing of cyber threat information and warning between the Federal government and private sector partners.
    - Supporting Response activities by making sure that communities and responders have adequate protection during the crisis.
    - Coordinating with Prevention, Mitigation, Response, and Recovery activities through the implementation of appropriate authorities and the provision of resources.
- **Return to steady-state protection activities.** When an enhanced Protection situation has abated, there is a return to steady-state activities.

Relationship to Other Mission Areas

This section describes the relationship between Protection and the other mission areas. The National Protection Framework addresses steady-state and enhanced steady-state actions that require coordination and, for the most part, are carried out concurrently with those processes identified in the frameworks for Prevention, Mitigation, Response, and Recovery.

Prevention Mission Area

The **Prevention** and Protection missions are closely aligned and integrated. Prevention includes the capabilities necessary to avoid, prevent, or stop a threatened or actual act of terrorism. For the purposes of the National Planning Frameworks, the term "prevention" refers to preventing imminent threats from terrorism. The Prevention mission area focuses on those intelligence, technical, and law enforcement actions that prevent an adversary from carrying out an attack within the United States when the threat is imminent in order to thwart an initial or follow-on terrorist attack. Protection activities, on the other hand, focus on government, private sector, and citizen measures that detect, deter, and/or disrupt terrorist surveillance, planning, and/or execution activities or deter and disrupt other threats and hazards and, like mitigation, focus on minimizing the consequences of significant events. In some cases, the same capabilities that are used for Protection functions are also used in Prevention operations. However, while the National Prevention Framework addresses imminent acts of terrorism, the National Protection Framework addresses all hazards and the ongoing security of potential terrorist targets. Many other activities traditionally considered preventative, such as disease prevention and cybersecurity, fall under the Protection mission based on the distinction between Prevention and Protection in the National Preparedness Goal. Further, following an attack, it is likely that mission area operations will be executed concurrently, and that decisions made in one mission area can have impacts across others. As a result, decisions should be uniformly informed through information sharing and operational coordination through situational assessment.

The National Protection and Prevention Frameworks share three of the same core capabilities. Processes described in these frameworks are designed to operate simultaneously and to provide for seamless integration when needed. For example, during a period of imminent terrorist threat, Prevention activities may focus on information sharing, law enforcement operations, and other activities to prevent, deter, and preempt terrorism. Protection may assess the increased risks and coordinates the information sharing and other actions needed to enhance specific protective measures.

Mitigation Mission Area

Mitigation refers to the capabilities necessary to reduce loss of life and property by lessening the impact and likelihood that a particular incident will result in a major disaster. Activities in the Mitigation and Protection missions typically are performed in a steady-state or well before an event. Protection places particular emphasis on security and deterring threats, while mitigation emphasizes achieving resilience by reducing vulnerabilities. Both seek to minimize consequences and have a nexus on critical infrastructure. Addressing the security of that infrastructure falls within the Protection mission, and the resilience of the infrastructure falls within the Mitigation mission area. Risk analysis is necessary to effectively design successful strategies for mitigation and protection. Integration of risk information, planning activities, and coordinating structures reduces duplication of effort and streamlines risk management actions in both mission areas.

Response Mission Area

The **Response** mission area includes the capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred. Natural disasters and incidents can increase vulnerabilities that require the implementation during response activities of actions developed through the National Protection Framework. Efforts to protect people and communities as well as vital facilities, systems, and resources, are inextricably linked to response efforts. Responders support the Protection mission and rely on protection organizations before, during, and after incidents. Protection resources and capabilities required to support response operations will be coordinated through the structures identified in the National Response Framework. The National Protection Framework provides the structure to assess and address increased vulnerabilities and risks beyond the specific disaster area and ensure that the protective posture is not compromised.

Protection capabilities deployed to support response efforts conform to and integrate into response organizational structures including the Incident Command System and the Emergency Support Function structures.

Analytic products developed in support of Protection activities during steady-state conditions are also designed to support Response planning efforts and provide the basis for operational planning during incident response.

Assessments of infrastructure impacts and prioritization efforts during response also rely on the structures and relationships developed within the Protection mission.

Recovery Mission Area

The **Recovery** mission area encompasses the capabilities necessary to assist communities affected by an incident to recover effectively. The systematic evaluation of the threats and hazards affecting the whole community and the executable strategies derived from that evaluation of the community's threats and hazards through risk-based planning are foundational to the actions taken during recovery. Coordination with the pre- and post-disaster recovery plans will ensure a resilient recovery process that takes protection into account. Protection and Mitigation focus on a sustainable economy and community resilience and not just the swift restoration of infrastructure, buildings, and services.

Establishing recovery priorities, and ensuring that resilience and risk management are central to the recovery effort requires the Protection mission to structure its activities in a way that supports Recovery efforts.

Operational Planning

The National Planning Frameworks explain the role of each mission area in national preparedness and provide the overarching doctrine for how the whole community builds, sustains, and delivers the core capabilities. The concepts in the frameworks are used to guide operational planning, which provides further information regarding roles and responsibilities, identifies the critical tasks an entity will take in executing core capabilities, and identifies resourcing, personnel, and sourcing requirements. Operational planning is conducted across the whole community. At the Federal level, each framework is supported by a mission area-specific FIOP. Comprehensive Preparedness Guide 101 provides further information on the various types of plans and guidance on the fundamentals of planning.

The following sections outline how operational planning is applied within the Protection mission at the Federal level.

Protection Operational Planning

Planning across the full range of Protection activities is an inherent responsibility of every level of government, private and nonprofit sector. A plan is a continuous, evolving instrument of anticipated or ongoing activities that maximizes opportunities and guides protection operations. Operational planning is conducted across the whole community. Its purpose is to determine jurisdictional priorities, objectives, strategies, and resource acquisitions and allocations needed to protect against potential threats, conduct law enforcement investigations, or engage in enforcement and protective activities based on jurisdictional authorities. From the Federal perspective, integrated planning helps explain how Federal departments and agencies and other national-level whole community partners provide the right resources at the right time to support local, regional/metropolitan, state, tribal, territorial, insular area, and Federal operations.

Department-level Operational Plans

To maintain the National Preparedness System, each executive department and agency develops and maintains deliberate department-level operational plans where needed, to deliver Protection core capabilities to fulfill the organization's responsibilities described in the FIOPs.

Departments and agencies may use existing plans, protocols, or standard operating procedures or guides for the development of such plans. Each department or agency determines its own planning requirements and decides whether its components or agencies need to develop subordinate operational plans.

Department-level operational plans identify specific critical tasks and responsibilities, including how to meet resource requirements and other specific provisions addressed in the FIOPs. Department-level operational plans also utilize the integrating factors for Protection—addressing risk, planning and exercising coordination and communication procedures, and sharing resources—and Protection core capabilities.

Protection Federal Interagency Operational Plan

The Protection FIOP will describe how Federal departments and agencies work together to deliver the Protection core capabilities. Government, private and nonprofit sector will be able to use the Protection FIOP to inform ongoing protection planning, training, and exercises within their jurisdictions or organizations. The Protection FIOP will be developed through a collaborative process that ensures integration among all of the mission areas, with specific focus on Prevention and Mitigation. The information about Federal capabilities will enable government, private and nonprofit sector to more accurately focus on local, regional/metropolitan, state, tribal, territorial, and insular area resource and capability requirements. Private and nonprofit sector, local, regional/metropolitan, state, tribal, territorial, insular area, and Federal government planning efforts supporting the National Protection Framework should address the following:

- Collaboration with all relevant stakeholders, including advocacy organization for individuals with access and functional needs including people with disabilities, people with limited English proficiency, and people from racially and ethnically diverse communities.
- A detailed concept of operations that explains how protection operations are coordinated and executed in a collaborative fashion.[33]

[33] A concept of operations is a statement that explains in broad terms what an organization (or group of organizations) intends to accomplish. It should describe how the organization or group will accomplish a set of objectives in order to reach a desired end-state.

- A description of critical tasks.
- A description of roles and responsibilities.
- Resource and personnel requirements.
- Specific provisions for the rapid integration of resources and personnel for enhanced steady-state operations.
- How Protection plans may be executed simultaneously with other plans.
- How the plan provides for multiple, geographically dispersed threats and hazards.
- How the plan addresses the needs of people with acute medical conditions.
- How the plan addresses the continuation of the essential functions that are necessary for the core capabilities that support the mission areas.
- Compliance with provisions regarding the rights of individuals protected by civil rights laws, including individuals with disabilities, racial and ethnic minorities, and individuals with limited English proficiency.

The Secretary of Homeland Security coordinates the development of the Protection FIOP in collaboration with all Federal departments and agencies that play a role in the implementation of the core capabilities within the Protection mission. The Roles and Responsibilities section identifies the Federal departments and agencies with predominant authorities or responsibilities within the Protection mission. The departments and agencies identified have primary responsibility for engaging in the National Preparedness planning processes and engaging other Federal departments and agencies and others with relevant responsibilities. The Secretary of Homeland Security is responsible for the ongoing management and maintenance of the Protection FIOP. The Secretary will lead a process to review and update the Plan at least every three years or following major exercises, real-world events, or revisions to relevant authorities or doctrine.

Planning Assumptions

The following assumptions will guide the development of the operational plans:

- Capabilities of the whole community play a critical role in protection.
- Activities within the Protection mission occur continuously and may be implemented concurrently with Prevention, Mitigation, Response, and Recovery capabilities.
- The National Protection Framework focuses on steady-state and enhanced steady-state.
- Protection resources are acquired, allocated, and assigned through normal budget and program processes.
- Protection responsibilities are decentralized and command and control capabilities are distributed among the whole community of Protection individuals, organizations, departments and agencies.

Framework Application

Government, private and nonprofit sector partners can use the National Protection Framework to inform and align relevant planning, training, exercises, and other activities designed to enhance security for the whole community. The Protection processes and guiding principles contained in this Framework provide a structured and unifying approach that is flexible and adaptable to specific

Protection mission requirements. Focusing planning, training, and exercises on the Protection core capabilities enhances preparedness.

Integration

Integration across the five mission areas results in synchronization and interoperability across the whole community. Integration is accomplished across and within the mission areas through planning and operational coordination processes, using the coordinating structures described in the respective frameworks and associated plans.

Planning. Protection entities coordinate planning activities across the whole community to ensure that required resources are and will be available when needed, particularly if those resources can be used to avert a threat or hazard. Protection partners should consider the following during planning:

- Estimating available resources from the whole community maximizes unity of effort and effectiveness, and reduces costs and time of delivery. Many jurisdictions, private and nonprofit sector organizations enter into mutual aid agreements to identify shared resources.
- Coordinating and analyzing requirements using common planning assumptions, risk assessments, or scenarios supports identifying which investments in capabilities most effectively address the threat or hazard and use resources most efficiently.
- Taking into consideration resource depletion rates incurred in previous or multiple events identifies potential gaps in resources over time.

Operational Coordination. The establishment and maintenance of unified operational structures and processes provides the architecture to appropriately integrate activities when required for the concurrent delivery of core capabilities for Prevention, Protection, Mitigation, Response, and Recovery. Joint training and exercises promote integration and supports unity of effort by allowing Protection and other mission area partners to align coordination and communication structures.

Networked Integration

Networked integration is the coordination and implementation of core capabilities within the Protection mission among the various sectors of the whole community. In contrast to a hierarchic or command and control model for implementing mission activity, the overlapping and decentralized nature of jurisdictions requires a networked model of coordination. For example, states integrate their activities with local, tribal, territorial, and insular areas, as well as with the Federal departments that support them in protection operations. In the same way, Federal departments and agencies operating under their own authorities exercise distinct jurisdictions for Protection activity, but also endeavor to coordinate across partnerships and capabilities. Pertinent regional organizations are also included as essential elements of networked integration; they can provide a bridge between the national and local levels.[34] In addition, all levels of government participate in joint protection exercises to ensure integration of their activities.

Protection partners integrate operations in the following ways:

- **Integration through partnerships and information sharing.** Protection core capabilities are coordinated across functional areas within a jurisdiction, such as police, fire, emergency medical services, public health, health systems, public works, and animal/agriculture entities. Core

[34] Examples of regional organizations include the PNWER Partnership, mentioned previously and the All Hazards Consortium. The All Hazards Consortium facilitates regional integration among governments and private sector infrastructure owners and operators, primarily in the mid-Atlantic region of the United States.

capabilities are also coordinated regionally with nearby jurisdictions that may share a common risk profile, resources, or information and support each other in delivering Protection core capabilities. Such integration occurs between and among government entities and the private sector elements, community groups, faith-based organizations, and NGOs at all levels through partnerships and information sharing.

- **Integration through the frameworks and plans.** At the Federal level, horizontal integration is achieved across the five mission areas through the development of the frameworks, FIOPs, and department-level operational plans. Specifically, all mission areas coordinate their frameworks with each other, focusing on integrating factors such as the core capabilities and the timing of overlapping activities. These factors are also applied in the development and maintenance of the FIOPs and Federal department-level operational plans. Using these integrating factors enables protection partners to understand the relationships, such as interdependencies and capabilities, among the five mission areas.

Integrating Science and Technology

Science and technology (S&T) capabilities and investments are essential for enabling the delivery and continuous improvement of National Preparedness. The whole community should design, conduct, and improve operations based on the best, most rigorous scientific data, methods, and science-based understandings available. Commitments and investments that ensure global leadership in science and technology will yield leading-edge technology and scientific understanding to guide National Preparedness actions. In addition, coordination across the whole community, including scientific researchers, will ensure that scientific efforts are relevant to National Preparedness.

Multiple core capabilities under the protection mission area rely upon sound, science-based vulnerability assessments, risk-informed standards, and advanced tools to detect and identify potential threats. Critical infrastructure protection, cybersecurity, defense of agriculture and food, health security, maritime security, and transportation security all benefit significantly from advances in science and technology. For example, S&T investments to advance the understanding of natural hazard phenomena support improvements in infrastructure standards and maritime security protocols. These S&T investments include research on coastal and riverine flood modeling to more accurately predict the magnitude and location where flooding, high winds, and dangerous maritime conditions occur.

Ensuring long-term S&T investments advance the ability to monitor and protect against emerging vulnerabilities, and sustaining a healthy science and technology workforce, supports the protection mission area core capabilities for years into the future. Coordination between those with protection mission responsibilities and U.S. science and technology communities and institutions will be necessary to ensure that scientific efforts, education, and investments are relevant to protection.

Supporting Resources

An array of resources are in place to support the Protection mission. These resources include training, exercises, and Web-based information—such as CitizenCorps.gov, USA.gov, and Ready.gov—that are available to both government and nongovernmental partners.

In addition, a variety of documents and guidelines exist that support the development of interagency and other operational plans. Examples include, but are not limited to the National Infrastructure Protection Plan and related Sector-Specific Plans; Executive Order 13636: Improving Critical Infrastructure Cybersecurity; Executive Order 13691: Promoting Private Sector Cybersecurity

Information; PPD-21: Critical Infrastructure Security and Resilience; HSPD 9: Defense of United States Agriculture and Food; National Security Presidential Directive 46: The U.S. Policy and Strategy in the War on Terror; HSPD 5: Management of Domestic Incidents; the National Strategy for Global Supply Chain Security; the Federal Interagency Geospatial Concept of Operations; Federal Continuity Directives 1 & 2; Continuity Guidance Circular 1 & 2; PPD-22: National Special Security Events; National Security Presidential Directive 51/Homeland Security Presidential Directive 20: National Continuity Policy; and the Cybersecurity Information Sharing Act of 2015.

Conclusion

The National Protection Framework is designed to promote the coordination of Protection mission activities in the face of increasingly dynamic and volatile risks. The shared responsibility for the Protection mission builds from the individual level and the community level to local jurisdictions; state, tribal, territorial, and insular area governments; and the Federal Government. The decentralization and adaptability of Protection mission activities is attuned to the nature of the risks, and the delivery of national Protection capabilities relies on a network of coordination structures that spans the Nation.

In implementing the National Protection Framework to build national preparedness, partners develop a shared understanding of risk while building future capacity and capability. The unifying principles and doctrine contained in this Framework will be regularly reviewed to evaluate consistency with existing and new policies, evolving conditions, and the experience gained from its use. Subsequent reviews will be conducted in order to evaluate the effectiveness of this Framework on a quadrennial basis.

DHS will coordinate and oversee the review and maintenance process for the National Protection Framework. The revision process includes developing or updating any documents necessary to carry out capabilities. Significant updates to this Framework will be vetted through a Federal senior-level interagency review process. This Framework will be reviewed in order to accomplish the following:

- Assess and update information on the core capabilities in support of protection goals and objectives.
- Ensure that it adequately reflects the organization of responsible entities.
- Ensure that it is consistent with the other four mission areas.
- Update processes based on changes in the national threat/hazard environment.
- Incorporate lessons learned and effective practices from day-to-day operations, exercises, and actual incidents and alerts.
- Reflect progress in the Nation's implementation of core capabilities within the Protection mission, the need to execute new law, executive orders, and Presidential directives, as well as strategic changes to national priorities and guidance, critical tasks, or national capabilities.

America's security and resilience work is ongoing and must evolve and adapt to changing threats and hazards to ensure sustainability. While the Nation is safer, stronger, and better prepared than a decade ago, the commitment to safeguard the Nation against the greatest risks it faces now and for decades to come, remains resolute. By bringing the whole community together now to support the collective and integrated action needed to address the shared future needs, the Nation will continue to improve its preparedness to face whatever challenges unfold.