# National Protection Framework

*[Month Year] 05/01/2012*

Homeland Security

**WORKING DRAFT**
**PRE-DECISIONAL**

# Table of Contents

# Introduction

*Presidential Policy Directive 8 (PPD-8), National Preparedness*, was released in March 2011 with the goal of strengthening the security and resilience of the United States through systematic preparation for the threats that pose the greatest risk to the security of the Nation. PPD-8 defines five mission areas—Prevention, Protection, Mitigation, Response, and Recovery—and mandates the development of a series of policy and planning documents to explain and guide the Nation's approach to ensuring and enhancing national preparedness. This National Protection Framework, part of the National Preparedness System, sets the strategy and doctrine for building, sustaining, and delivering the core capabilities for mitigation identified in the National Preparedness Goal.

**Prevention:** The capabilities necessary to avoid, prevent, or stop a threatened or actual act of terrorism. As defined by PPD-8, the term "prevention" refers to preventing imminent threats.

**Protection:** The capabilities necessary to secure the homeland against acts of terrorism and man-made 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 provides the unifying principles and strategies required to safeguard the Nation against acts of terrorism and man-made or natural disasters. It describes the core capabilities, roles and responsibilities, and coordinating structures that facilitate the protection of individuals, communities, and the Nation as a whole. This Framework is focused on actions to protect against the greatest risks to the Nation in a manner that allows American interests, aspirations, and way of life to thrive.

Protection includes actions to deter threats, mitigate vulnerabilities, or minimize the consequences associated with an incident. Protection can include a wide range of activities, such as improving physical security, building redundancy, incorporating resistance to hazards in facility design, initiating active or passive threat countermeasures, installing security systems, promoting workforce surety, training and exercising, and implementing cybersecurity measures. Effective Protection relies upon the close coordination and alignment of Protection practices across the whole community[1] as well as coordination with international partners and organizations.

This Framework identifies the structures and capabilities needed to achieve the Protection mission area end-state: to "create conditions for a safer, more secure, and more resilient Nation by enhancing

[1] Whole community includes: individuals, families, communities, the private and nonprofit sectors, faith-based organizations, and Federal, state, local, tribal, and territorial governments. 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 Federal, state, and local governmental partners in order to foster better coordination and working relationships." The National Preparedness Goal is located at http://www.fema.gov/ppd8.

Protection through cooperation and collaboration with all sectors of society."[2] In accordance with PPD-8, Protection mission activities[3] include, but are not limited to, the following: Defense Against Weapons of Mass Destruction (WMD)[4] Threats, Defense of Agriculture and Food, Critical Infrastructure Protection,[5] Protection of Key Leadership[6] and Events,[7] Border Security, Maritime Security, Transportation Security, Immigration Security, Cybersecurity, and Health Security.[8] The structures and capabilities needed to achieve the Protection mission area end-state build in large part upon existing doctrine, plans, and activities. While many of the capabilities in the Protection area are provided by Federal departments and agencies, overall success is dependent upon close and continuous coordination between government organizations and the whole community to share the responsibility of promoting national preparedness through integrated planning, training, and exercising. The National Protection Framework provides a roadmap to align Protection efforts and will benefit the whole community by accomplishing the following:

- A unified approach to Protection
- Synchronization and interoperability within the Protection mission area and across the Prevention, Mitigation, Response, and Recovery mission areas
- Collaboration and engagement across the whole community to achieve the objectives of the National Preparedness Goal.

## Intended Audience

This Framework is applicable across government at all levels, non-governmental organizations, and the private sector. The intended audience includes, but is not limited to: government and corporate executives; law enforcement, security, public health, fire, emergency medical and emergency management professionals; critical infrastructure owners and operators; and those with legal and/or statutory authorities within the Protection mission area.

---

[2] The Protection end-state is defined in the National Preparedness Goal. The National Preparedness Goal is located at http://www.fema.gov/ppd8.

[3] The Protection mission activities, as identified in PPD-8, are further described in the Scope section of this Framework.

[4] Weapons of mass destruction include chemical, biological, radiological, nuclear, and explosive munitions with the capacity to kill large numbers of human beings indiscriminately.

[5] Critical infrastructure, as defined in the National Infrastructure Protection Plan (NIPP), 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 protection addresses 18 sectors along common functions: banking and finance; chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; food and agriculture; government facilities; healthcare and public health; information technology; national monuments and icons; nuclear reactors, materials, and waste; postal and shipping; transportation systems; and water. There are close parallels between several of the NIPP critical infrastructure sectors and the Protection mission activities identified in PPD-8, for example: food and agriculture; healthcare and public health; and transportation systems. Other sectors, such as the information technology and postal and shipping sectors, closely parallel Protection mission activities. For more information on critical infrastructure protection and the sectors, see the NIPP at http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

[6] 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.

[7] Events of national significance fall within two categories: National Special Security Events (NSSEs) as defined in Title 18, U.S.C. Section 3056, and events assessed under the Special Events Assessment Rating (SEAR) process by the Department of Homeland Security and the Federal Bureau of Investigation, based on input from Federal, state, and local law enforcement entities.

[8] Health security refers not only to human health; it includes animal and environmental health.

The Protection Framework describes how the whole community contributes to the full spectrum of Protection mission activities and capabilities and what individuals and organizations can do to ensure this Nation is optimally protected from the full spectrum of man-made and natural threats and hazards.

While large portions of the Protection mission area fall under the authority of Federal stakeholders, 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, the Framework enables the whole community to contribute to and benefit from national preparedness. This includes children, individuals with disabilities, and others with access and functional needs; those from religious, racial, and ethnically diverse backgrounds; and people with limited English proficiency. Their contributions must be integrated into preparedness efforts, and their needs must be incorporated during planning and execution of the core capabilities.

## Scope

This Framework focuses on Protection activities that take place during both steady-state and enhanced steady-state conditions immediately before or during an incident.[9] Steady-state activities take place during routine, normal, day-to-day operations. Enhanced steady-state activities are those that take place during temporary periods of heightened alert when a threat is believed to be imminent, during periods of incident response, or in support of planned events in which additional, or enhanced, Protection activities are needed.

**Enhanced Steady-state Condition**

An enhanced steady-state condition is caused by a deliberative decision by appropriate leadership to increase capability for a period of time over a particular area.[10]

This Framework addresses activities that contribute to protecting the Nation domestically, but it does not address all the activities or coordinating structures that may be required to protect U.S. interests overseas. The whole community contributes to the security and resilience of the Nation by developing and sustaining specific core capabilities[11] that directly support accomplishment of the Protection mission activities.

The Protection mission activities can be grouped into three categories (refer to Figure 1): Community and Infrastructure Protection, Transportation and Transborder Security, and Protection of Key Leadership and Events. The whole community shares responsibility across all Protection mission activities to varying degrees, based on jurisdictions and geographic locations. Protecting the Nation's critical infrastructure, for example, is a shared responsibility between critical infrastructure owners and operators from the private sector and the government at all levels. The Federal Government has unique Protection authorities for Border, Maritime, and Immigration Security, as well as for the Protection of Key Leaders and Events. Within these specified mission activities, the Federal Government works collaboratively with local, state, tribal, and territorial governments and the private sector to develop and deliver Protection core capabilities such as Interdiction and Disruption or Screening, Search, and Detection in support of these activities.

[9] The steady-state Protection and pre-incident coordination processes are discussed in detail in the Coordinating Structures and Integration section of this document.

[10] Sources: *Global Nuclear Detection Architecture Annual Report 201; Interagency Domestic Radiological Nuclear Search Operations Plan*

[11] For a more comprehensive explanation of the protection core capabilities, please see the Core Capabilities section of this document.


**Figure 1: Protection Mission Activities**

- Community and Infrastructure Protection Mission Activities
  - Critical Infrastructure Protection.[12] Protecting the physical, cyber, and human elements of critical infrastructure. This includes actions to deter the threat, reduce vulnerabilities, and/or minimize the consequences associated with a terrorist attack, natural disaster, or man-made disaster.
  - Cybersecurity. Securing the cyber environment against or from damage, unauthorized use, or malicious exploitation while protecting infrastructure, civil rights, individual privacy, and other civil liberties.
  - Defense Against 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.
  - 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.
- Transportation and Transborder Security
  - Border Security. Securing our U.S. air, land, and sea borders against the illegal flow of people and goods while facilitating the flow of lawful travel and commerce.
  - Immigration Security. Securing the Nation from illegal immigration through effective, efficient immigration systems and processes that respect human rights.

[12] Refer to the description of critical infrastructure in footnote 5 on page 2 of this document.

- Maritime Security. Securing our 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 enabling legitimate travelers and goods to efficiently move without fear of harm, violation of civil rights, reduction of civil liberties, or disruption of commerce.
- Transportation Security. Securing our transportation systems against terrorism and other threats and hazards while enabling legitimate travelers and goods to move without significant disruption of commerce, undue fear of harm, violation of civil rights, or loss of civil liberties.

▪ Protection of Key Leadership and Events

- Protecting key leadership to safeguard government executive leadership from hostile acts by terrorists and other malicious actors and to ensure security at events of national significance.

▪ International Dimension

- Protection measures do not stop at a facility's fence or at a national border. Because disruptions in global infrastructure and security can have ripple effects around the world, the Protection mission area also considers cross-border critical infrastructure, international vulnerabilities, and global dependencies and interdependencies.

## *Guiding Principles*

Three principles guide the development and support the execution and deployment of Protection mission activities and related core capabilities. These guiding principles are as follows:

1. **Resilience, Scalability, and Sustainability.** Effective Protection capabilities, mission activities, plans, programs, policies, and practices together minimize the risks from all threats and hazards through:
   a. **Increasing resilience** by reducing the impact and/or duration of disruptive events on organizations and communities.[13]
   b. **Executing scalable and sustainable capabilities and activities** to meet unforeseen, unmet, and evolving needs of varying geographic scope, complexity, and intensity, without compromising the ability to address continuing and future needs.
2. **Risk-Informed Culture.** A risk-informed culture supports Protection activities and capabilities and requires:
   a. **Vigilance and situational awareness** through a comprehensive understanding of current, evolving, and emerging threats and hazards and the relative risk they pose.
   b. **Information sharing and risk-informed decisionmaking** through sharing appropriate, accessible, and timely information to allow for the ongoing analysis of risks and assessment of effective practices.

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

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

   a. **Engaged partnerships** to 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 levels of government and with private sector 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. It is assessed based on applicable threats and hazards, vulnerabilities, and consequences.

The National Preparedness System[14] uses a risk-based approach. Its components are based on the Strategic National Risk Assessment (SNRA),[15] which identifies the threats and hazards that pose the greatest risk to the Nation (see Table 1). The core capabilities in the National Preparedness Goal, in turn, are based on the results of the SNRA.

Given the National Preparedness Goal's emphasis on contingency events with defined beginnings and endpoints, the SNRA results enumerated in the table do not explicitly assess persistent steady-state risks like border violations, illegal immigration, drug trafficking, and intellectual property violations. However, these remain important considerations for Protection and are a significant component of the steady-state capabilities provided for by Federal departments and agencies.

[14] The National Preparedness System description was developed as a requirement under PPD-8, which calls for creation of a National Preparedness Goal, a National Preparedness System description, and a National Preparedness Report. The National Preparedness System description explains current preparedness efforts and how the Nation builds on those efforts to build, sustain, and deliver the core capabilities needed to achieve the National Preparedness Goal. The National Preparedness System description is located at http://www.fema.gov/pdf/prepared/nps_description.pdf.

[15] The Secretary of Homeland Security led an interagency effort to conduct a SNRA in support of PPD-8 to help identify the types of incidents that pose the greatest threat to the Nation's homeland security. The SNRA document is located at http://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf.

209 **Table 1: National Threats and Hazards[16]**

| Row | Threat/Hazard Group | Threat/Hazard Type |
|---|---|---|
| 1 | Natural | Animal Disease Outbreak |
| | | Earthquake |
| | | Flood |
| | | Human Pandemic Outbreak |
| | | Hurricane |
| | | Space Weather |
| | | Tsunami |
| | | Volcanic Eruption |
| | | Wildfire |
| 2 | Technological/Accidental | Biological Food Contamination |
| | | Chemical Substance Spill or Release |
| | | Dam Failure |
| | | Radiological Substance Release |
| 3 | Adversarial/Human-Caused | Aircraft as a Weapon |
| | | Armed Assault |
| | | Biological Terrorism Attack (non-food) |
| | | Chemical/Biological Food Contamination Terrorism Attack |
| | | Chemical Terrorism Attack (non-food) |
| | | Cyber Attack against Data |
| | | Cyber Attack against Physical Infrastructure |
| | | Explosives Terrorism Attack |
| | | Nuclear Terrorism Attack |
| | | Radiological Terrorism Attack |

210
211 Planning for and managing the "greatest risks" is a fundamental component of the National
212 Preparedness Goal and a compass for all participants who share responsibilities under the National
213 Protection Framework. The National Protection Framework contributes to a comprehensive
214 improvement in risk management by emphasizing the use of risk-informed decisionmaking for
215 Protection. This is the determination of a course of action based on the assessment of risk, the
216 expected impact of the course of action on that risk, and other relevant factors. It allows
217 decisionmakers to adapt to changing conditions.

[16] Source: SNRA. http://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf.

# Roles and Responsibilities

The whole community shares responsibility for maintaining awareness of threats and hazards and for taking actions to address risk within their own domains. Protection partners have varying authorities, capacities, and resources that, when stitched together in a risk-informed way, provide the basis for the National Protection Framework.

Protection takes place across a continuum of conditions ranging from steady-state activities through crisis response and recovery. Many individuals, organizations, and entities engaged in Protection activities are also key contributors within other mission areas. The Protection Framework is designed to provide a cohesive and ongoing approach to dealing with those risks that can be most effectively reduced, transferred, or avoided through the effective delivery of the Protection mission area activities and core capabilities.

## *Individuals, Families, and Households*

Individuals, families, and households provide the foundation for effective protection by maintaining awareness of threats and hazards and by taking risk-informed protective actions. Awareness of potential threats and hazards is acquired through an array of sources that include, but are not limited to: news outlets, public information and warning systems, and information-sharing mechanisms. Taking protective actions may include the following: installing and using home security systems or computer protection software, completing relevant training programs such as first aid or cardiopulmonary resuscitation (CPR) training, developing a household evacuation plan, reporting suspicious activities to law enforcement, participating in community-based programs such as Citizen Corps[17] or neighborhood watch, or maintaining an emergency kit at home and at work. Individuals support Protection efforts by assisting in the development of objectives for community and local Protection activities.

## *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 Protection activities and share information and effective practices. Communities may include neighborhood partnerships, online communities, hazard-specific coalitions, and professional associations.

## *Non-governmental Organizations*

Non-governmental organizations (NGOs) are encouraged to establish or participate in regional and community preparedness partnerships and activities with the whole community to develop a common understanding of risk and how to address it through their Protection efforts. Where applicable, NGOs also contribute to the Protection mission area 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.

[17] Citizen Corps programs educate people and communities about disaster preparedness for hazards that may impact their area. The Citizen Corps Website is located at: http://www.citizencorps.gov/.

### Private Sector Entities

Private sector entities include businesses, commerce, private universities, and industry. The focus for Protection is on the owners and operators of the vast majority of the Nation's infrastructure. Owners and operators of both private and public sector infrastructure[18] develop and implement risk-based protective programs and resilience strategies for the businesses, infrastructure, information, and operations under their control. Owners and operators maintain situational awareness and take actions on a continuous basis to build Protection capabilities and make investments in security as necessary components of prudent day-to-day business planning and continuity of operations.

## International Partnerships

Protection capabilities often are interconnected globally. International Protection coordination and cooperation is focused on instituting partnerships with international stakeholders, implementing current agreements and instruments that affect protection, and addressing cross-sector and global issues such as cybersecurity and foreign investment.

International protection activities require coordination with the Department of State and appropriate government entities at the state, tribal, territorial, and Federal levels.

### Local Governments

Governments at all levels contribute to the Protection mission by taking a leadership role in developing, delivering, reviewing, and assessing the core capability critical objectives. Many of these core capabilities already exist and are used every day for steady-state Protection activities.

Local governments are responsible for the public safety, security, health, and welfare of the people who live in their jurisdictions. Local governments promote the coordination of ongoing Protection plans and activities as well as engagement and sharing information 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, establish agreements for cross-jurisdictional and public-private coordination..

### State, Tribal, Territorial, and Insular Area Governments

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

### Federal Government

The Federal Government provides a leadership, coordination, and integration role in the development and delivery of Protection capabilities. Federal departments and agencies implement statutory and regulatory responsibilities for a wide array of protective programs and provide assistance in a number

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

of areas, including funding, acquisition, research, coordination, oversight, implementation, and enforcement.

The Federal Government, in coordination with state and local partners and the private sector, contributes to the development and delivery of the core capability targets by establishing and implementing national laws, regulations, guidelines, and standards designed to protect public health and security while ensuring the free flow of commerce, the protection of civil rights, and the preservation of civil liberties. The Federal Government provides integrated Federal public safety and security capabilities and resources for potential or actual incidents requiring a coordinated Federal response.

A range of Federal departments and agencies, including the Department of Homeland Security and the Department of Defense, have differing responsibilities regarding Protection. These departments and agencies may contribute to the Protection mission in primary, coordinating, and/or supporting roles based on their authorities and the nature of the threat or hazard. Table 2 provides a list of the Federal departments and agencies that have predominant responsibility for the specified mission activities. The Protection Federal Interagency Operations Plan (FIOP)[19] will provide a detailed description of how the full range of Federal departments and agencies engage in Protection mission activities.

**Table 2: Coordinating Departments and Agencies by Protection Mission Activity**

| Row | Protection Mission Activity | Coordinating Departments and Agencies |
|---|---|---|
| 4 | Defense Against WMD Threats | Department of Agriculture<br>Department of Defense<br>Department of Energy<br>Department of Health and Human Services<br>Department of Homeland Security<br>Department of Justice |
| 5 | Defense of Agriculture and Food | Department of Agriculture<br>Department of Health and Human Services<br>Department of Homeland Security |
| 6 | Critical Infrastructure Protection | Department of Homeland Security<br>Department of Agriculture<br>Department of Defense<br>Department of Energy<br>Department of Health and Human Services<br>Department of the Interior<br>Department of the Treasury<br>Environmental Protection Agency |
| 7 | Protection of Key Leadership and Events | Department of Homeland Security<br>Department of Justice |

[19] The FIOPs are a required component of the National Preparedness System directed under PPD-8. Their intent is to provide guidance across the Federal Government to successfully implement the Frameworks. The Protection FIOP is discussed further in the Coordinating Structures and Integration section of this document.

| Row | Protection Mission Activity | Coordinating Departments and Agencies |
|---|---|---|
| 8 | Border Security | Department of Homeland Security<br>Department of State |
| 9 | Maritime Security | Department of Homeland Security<br>Department of Defense |
| 10 | Immigration Security | Department of Homeland Security |
| 11 | Transportation Security | Department of Homeland Security<br>Department of Transportation |
| 12 | Cybersecurity | Department of Homeland Security<br>Department of Justice<br>Department of Defense |
| 13 | Health Security | Department of Health and Human Services<br>Department of Agriculture<br>Department of the Interior<br>Environmental Protection Agency |

The authority for the Protection mission is established in local, state, tribal, territorial, and Federal laws, regulations, ordinances, and other directives with the force and effect of law. This Framework does not change or replace any existing authorities.

Federal statutes, executive orders, and regulations empower a number of Federal agencies to oversee and assist in aspects of the Protection activities within and across several critical infrastructure sectors. Table 2 identifies the Federal departments that have responsibility for the specified mission activities.

The planning and execution of Framework activities will support deconfliction with the authorities and responsibilities of those agencies and their requirements within the respective sector. Organizations having responsibility for planning and execution at all levels will incorporate consultation and coordination with those agencies into their actions to assure compatibility with the agencies' work as an aspect of sector protection.

## Core Capabilities

The National Preparedness Goal identified the core capabilities and targets for each of the five mission areas. See Table 3for a list of the core capabilities by mission area. 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.

328 **Table 3: Core Capabilities by Mission Area[20]**

| Row | Prevention | Protection | Mitigation | Response | Recovery |
|---|---|---|---|---|---|
| 14 | Planning | | | | |
| 15 | Public Information and Warning | | | | |
| 16 | Operational Coordination | | | | |
| 17 | Intelligence and Information Sharing<br>Interdiction and Disruption<br>Screening, Search, and Detection<br>Forensics and Attribution | **Intelligence and Information Sharing**<br>**Interdiction and Disruption**<br>**Screening, Search, and Detection**<br>**Access Control and Identity Verification**<br>**Cybersecurity**<br>**Physical Protective Measures**<br>**Risk Management for Protection Programs and Activities**<br>**Supply Chain Integrity and Security** | Community Resilience<br>Long-Term Vulnerability Reduction<br>Risk and Disaster Resilience Assessment<br>Threat and Hazard Identification | Critical Transportation<br>Environmental Response/ Health and Safety<br>Fatality Management Services<br>Infrastructure Systems<br>Mass Care Services<br>Mass Search and Rescue Operations<br>On-Scene Security and Protection<br>Operational Communications<br>Public and Private Services and Resources<br>Public Health and Medical Services<br>Situational Assessment | Economic Recovery<br>Health and Social Services<br>Housing<br>Infrastructure Systems<br>Natural and Cultural Resources |

329
330 The National Preparedness Goal identifies 11 core capabilities for the Protection mission area. Three
331 of these core capabilities—Planning, Public Information and Warning, and Operational
332 Coordination—cross-cut all of the mission areas. In addition, the Protection and Prevention mission
333 areas share three core capabilities: Intelligence and Information Sharing; Interdiction and Disruption;
334 and Screening, Search, and Detection. The cross-cutting core capabilities between mission areas
335 provide opportunities for integration. For example, Prevention and Protection use many of the same
336 coordinating structures for delivering Intelligence and Information Sharing capabilities. Protection
337 and Mitigation share capabilities directly related to risk management. For Protection, the capability is

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

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 2 displays the relationships between core capabilities and the mission areas, including the overlap in risk management capabilities between Protection and Mitigation.


**Figure 2: Preparedness Mission Areas and Core Capabilities**

Collectively, the core capabilities for the Protection mission area provide the foundation for achieving the Protection mission activities (see Figure 3) and the overarching critical objective for Protection: a homeland 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 established preliminary targets for each of the Protection mission core capabilities, which were used to identify critical tasks.[21] The critical tasks (see Table 4 and Table 5) to achieve the targets are specific to Protection and can be used by jurisdictions at all levels and by other Protection partners to identify tailored goals and objectives using the steady-state Protection process described in the Framework.

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

[21] The Protection mission area capabilities and preliminary targets are identified in the National Preparedness Goal, which is located at http://www.fema.gov/pdf/prepared/npg.pdf.

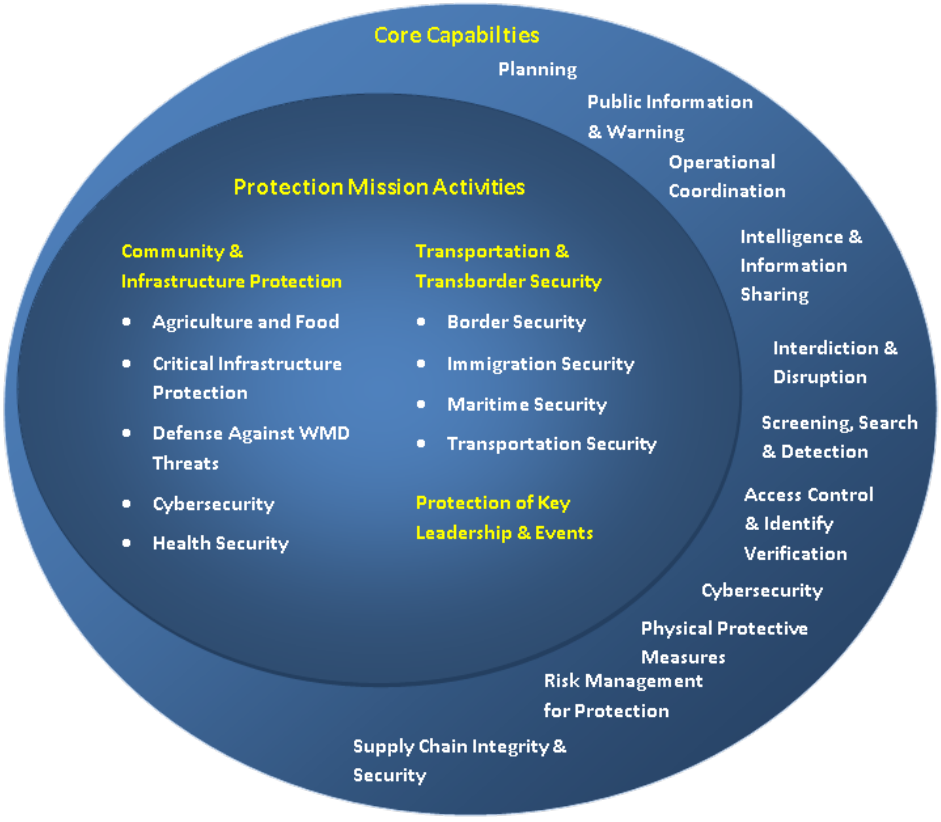


**Figure 3: Protection Core Capabilities and Mission Activities**

## Cross-cutting Core Capabilities

The following three core capabilities span all five mission areas: Planning, Public Information and Warning, and Operational Coordination (refer to Table 4).

362 **Table 4: Overview of Cross-cutting Core Capabilities**

| Row | Cross-cutting Core Capabilities | |
|---|---|---|
| 18 | **1. Planning**<br>*(Cross-cutting with all mission areas)* | **Description:** Conducting a systematic process that engages the whole community, as appropriate, in the development of executable strategic, operational, or community-based approaches to meet defined Protection objectives.<br>Planning includes the development of multidisciplinary plans; their implementation, exercising, and maintenance; and the promotion of planning initiatives. |
| 19 | **Critical Tasks:**<br>▪ Initiate a flexible planning process that builds on existing plans.<br>▪ Establish partnerships, facilitate coordinated information sharing between partners, and enable planning and protection of critical infrastructure within the jurisdiction.<br>▪ Implement measures to identify and prioritize critical infrastructure and determine risk.<br>▪ Conduct vulnerability assessments, perform risk analyses, identify capability gaps, and coordinate protective measures on an ongoing basis in conjunction with the private sector and local, state, tribal, territorial, and Federal organizations and agencies.<br>▪ Implement protection, resilience, and continuity plans and programs, train and exercise, and take corrective actions.<br>▪ Develop and implement progress measures and communicate adjustments and improvements to applicable stakeholders and authorities. | |
| 20 | **2. Public Information and Warning**<br>*(Cross-cutting with all mission areas)* | **Description:** Delivering coordinated, prompt, reliable, and actionable information to the whole community through the use of clear, consistent, accessible, and culturally and linguistically appropriate methods. These efforts will be implemented to effectively relay information regarding any threat or hazard and, as appropriate, the actions being taken and the assistance made available.<br>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). |
| 21 | **Critical Tasks:**<br>▪ Establish mechanisms and provide the full spectrum of support necessary for appropriate and ongoing information sharing among all levels of government, the private sector, non-governmental organizations, and the public.<br>▪ Promptly share actionable measures with the public and among all levels of government, the private sector, and non-governmental organizations.<br>▪ Leverage all appropriate communication means, such as the Integrated Public Alert and Warning System (IPAWS), National Terrorism Advisory System (NTAS), and social media sites and technology. | |

| Row | Cross-cutting Core Capabilities | |
|---|---|---|
| 22 | **3. Operational Coordination** *(Cross-cutting with all mission areas)* | **Description:** Establishing and maintaining unified and coordinated operational structures and processes that appropriately integrate all critical stakeholders and support the execution of core capabilities.<br>Operational coordination supports networking, planning, and coordination between Protection partners. |
| 23 | **Critical Tasks:**<br>▪ Collaborate with all relevant Protection partners.<br>▪ Establish clear lines and modes of communication among participating organizations and jurisdictions.<br>▪ Define and communicate clear roles and responsibilities relative to courses of action.<br>▪ Integrate and synchronize actions of participating organizations and jurisdictions to ensure unity of effort.<br>▪ Determine jurisdictional priorities, objectives, strategies, and resource allocations.<br>▪ Coordinate across and among all levels of government and with critical non-governmental and private sector partners to protect against potential threats, conduct law enforcement investigations, and/or engage in enforcement and protective activities based on jurisdictional authorities.<br>▪ Coordinate with appropriate partners in other mission areas. | |

## Protection Core Capabilities

The remaining Protection core capabilities are the following: Intelligence and Information Sharing; Interdiction and Disruption; Screening, Search, and Detection; Access Control and Identity Verification; Cybersecurity; Physical Protective Measures; Risk Management for Protection Programs and Activities; and Supply Chain Integrity and Security (refer to Table 5).

368 **Table 5: Protection Core Capabilities**

| Row | Protection and Prevention Core Capabilities | |
|---|---|---|
| 24 | **4. Intelligence and Information Sharing**<br>*(Shared with Prevention)* | **Description: Intelligence sharing** is providing timely, accurate, and actionable information resulting from intelligence processes[22] of available information concerning threats to the United States, its people, property, or interests; the development, proliferation, or use of WMDs; or any other matter bearing on U.S. national or homeland security by local, state, tribal, territorial, Federal, and other stakeholders. **Information sharing** is the capability to exchange intelligence, information, data, or knowledge among local, state, tribal, territorial, Federal, or private sector entities as appropriate.<br>All actions within the Protection Framework begin with the monitoring, gathering, and analysis of intelligence and information. Intelligence and information sharing may use pre-defined networks, procedures, and formats.<br>In the context of Protection and Prevention, Intelligence and Information Sharing capabilities involve the effective implementation of the intelligence cycle and information fusion processes by local, state, tribal, territorial, and Federal intelligence entities, the private sector, and the public to develop situational awareness of potential threats and hazards within the United States.<br>Lawful sharing of information with 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 to the widest appropriate audience. |
| 25 | **Critical Tasks:**<br>▪ Monitor, detect, and analyze threats and hazards to public safety, health, and security, which includes:<br>• Participation in local, state, tribal, territorial, regional, and national education and awareness programs.<br>• Participation in the routine exchange of security information—including threat assessments, alerts, attack indications and warnings, and advisories—among partners.<br>▪ Develop or identify and provide access to mechanisms and procedures for intelligence and information sharing between the public, private sector, and government Protection partners.<br>▪ Using intelligence processes, produce and deliver relevant, timely, accessible, and actionable intelligence and information products to others as applicable, to include partners in the other mission areas.<br>▪ Adhere to appropriate mechanisms for safeguarding sensitive and classified information. | |

[22] Intelligence processes, referred to collectively in the intelligence and law enforcement communities as the intelligence cycle, include the following: planning, direction, collection, exploitation, processing, analysis, production, dissemination, evaluation, and feedback.

| Row | Protection and Prevention Core Capabilities | |
|---|---|---|
| 26 | **5. Interdiction and Disruption**<br>*(Shared with Prevention)* | **Description:** Delaying, diverting, intercepting, halting, apprehending, or securing threats and/or hazards.<br>These 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 CBRNE materials and related technologies.<br>In the context of Protection and Prevention, this capability includes those interdiction and disruption activities undertaken in response to specific, actionable intelligence that indicates the location of a suspected weapon and/or threat actor or material. It might also include urgent activities required when an imminent threat is encountered unexpectedly.<br>This capability also includes interdiction and disruption activities conducted by law enforcement and public and private sector security personnel during the course of their routine duties, including the enforcement of border authorities at and between ports of entry into the United States. |
| 27 | **Critical Tasks:**<br>▪ Interdict conveyances, cargo, and persons associated with an imminent threat or act.<br>▪ Prevent movement and operation of terrorists into or within the United States and its territories.<br>▪ Render safe chemical, biological, radiological, nuclear and explosive (CBRNE) threats.<br>▪ Implement public health measures to mitigate the spread of disease threats abroad and prevent disease threats from crossing national borders.<br>▪ Disrupt terrorist financing or conduct counter-acquisition activities to prevent weapons, precursors, related technology, or other material support from reaching its target.<br>▪ Enhance visible presence of law enforcement to deter or disrupt threats from reaching potential target(s).<br>▪ Employ wide-area search and detection assets in targeted areas in concert with local, state, tribal, and territorial personnel or other Federal agencies (depending on threat). | |
| 28 | **6. Screening, Search, and Detection**<br>*(Shared with Prevention)* | **Description:** Identifying, discovering, or locating threats and/or hazards through active and passive surveillance and search procedures. These activities may include the use of systematic examinations and assessments, sensor technologies, disease surveillance, laboratory testing, or physical investigation and intelligence.<br>In the context of Protection and Prevention, 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.<br>Screening, search, and detection actions safeguard citizens, residents, visitors, and critical assets, systems, and networks against the most dangerous threats to the Nation. |

| Row | Protection and Prevention Core Capabilities | |
|---|---|---|
| 29 | **Critical Tasks:**<br>▪ Locate persons and criminal/terrorist networks associated with a potential threat.<br>▪ Develop and engage an observant Nation (individuals, families, communities, and local, state, tribal, and territorial government and private sector partners).<br>▪ Screen persons, baggage, mail, cargo, and conveyances using technical, non-technical, intrusive, and non-intrusive means. Consider additional measures for high-risk persons, conveyances, or items.<br>▪ Conduct physical searches.<br>▪ Conduct CBRNE search and detection operations.<br>• Conduct ambient and active detection of CBRNE agents.<br>• Operate safely in a hazardous environment.<br>• Conduct technical search and detection operations.<br>• Consider deployment of Federal teams and capabilities to enhance local, state, tribal, and territorial efforts, including use of incident assessment and awareness assets.<br>▪ Conduct biosurveillance of medical threats and hazards. | |
| | **Protection Core Capabilities** | |
| 30 | **7. Access Control and Identity Verification** | **Description:** Applying a broad range of physical, technological, and cyber measures to control admittance to critical locations and systems, limiting access to authorized individuals to carry out legitimate activities.<br>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. |
| 31 | **Critical Tasks:**<br>▪ 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.<br>▪ Control and limit access to critical locations and systems to authorized individuals carrying out legitimate activities. | |

369

| | Protection Core Capabilities | |
|---|---|---|
| 32 | **8. Cybersecurity** | **Description:** Protecting against damage to, unauthorized use of, and/or malicious exploitation of (and, if needed, the restoration of) electronic communications systems and services (and the information contained therein).<br>Cybersecurity activities ensure the security, reliability, integrity, and availability of critical information, records, and communications systems and services through collaborative cybersecurity initiatives and efforts. These activities also include procedures to detect malicious activity and to conduct technical and investigative-based countermeasures, mitigation activities, and operations against malicious actors to counter existing and emerging cyber-based threats, consistent with established protocols. |
| 33 | **Critical Tasks:**<br>▪ Implement physical protections, countermeasures, and policies to protect physical and cyber assets, networks, applications, and systems that could be exploited to do harm.<br>▪ Secure, to the extent possible, unclassified Federal Government networks and critical infrastructure (e.g., financial systems, power grid systems, water systems, transportation networks), through risk assessment, mitigation, and incident response capabilities.<br>▪ Share actionable cyber threat information with domestic and international, government and private sector partners, before a cyber incident occurs.<br>▪ Implement risk-informed guidelines, regulations, and standards to ensure the security, reliability, integrity, and availability of critical information, records, and communications systems and services through collaborative cybersecurity initiatives and efforts.<br>▪ Detect malicious activity and conduct technical and investigative-based countermeasures, mitigation activities, and operations against malicious actors to counter existing and emerging cyber-based threats. | |
| 34 | **9. Physical Protective Measures** | **Description:** Reducing or mitigating risks, including actions targeted at threats, vulnerabilities, and/or consequences, by controlling movement and protecting borders, critical infrastructure, and the homeland.<br>This capability includes the development, implementation, and maintenance of risk-informed physical protections, countermeasures, and policies protecting people, structures, materials, products, and systems associated with key operational activities and critical infrastructure sectors. |

| | Protection Core Capabilities | |
|---|---|---|
| 35 | **Critical Tasks:**<br>▪ Identify and prioritize assets, systems, networks, and functions that need to be protected.<br>▪ Identify needed physical protections, countermeasures, and policies through a risk assessment of key operational activities and infrastructure.<br>▪ Develop and implement security plans, including business continuity plans, that address identified security risks.<br>▪ Develop and implement risk-based physical security measures, countermeasures, policies, and procedures.<br>▪ Implement security training for workers, focused on awareness and response.<br>▪ Develop and implement biosecurity and biosafety programs and practices.<br>▪ Leverage Federal acquisition programs, as appropriate, to ensure maximum cost efficiency, security, and interoperability of procurements. | |
| 36 | **10. Risk Management for Protection Programs and Activities**<br>*(Aligned with Mitigation)* | **Description:** Identifying, assessing, and prioritizing risks to inform Protection activities and investments.<br>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.<br>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 of an attack. |
| 37 | **Critical Tasks:**<br>▪ Gather required data in a timely and accurate manner to effectively identify risks.<br>▪ Obtain and use appropriate threat, vulnerability, and consequence tools to identify and assess threats, vulnerabilities, and consequences.<br>▪ Conduct vulnerability assessments and risk analyses of appropriate assets, systems, networks, functions, and their interdependencies and shared vulnerabilities.<br>▪ Build the capability within communities to analyze and assess risk and resilience.<br>▪ Identify, implement, and monitor risk management plans.<br>▪ Update risk assessments to reassess risk based on changes in the following areas: the physical environment, 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.<br>▪ Validate, calibrate, and enhance risk assessments by relying on experience, lessons learned, and knowledge beyond raw data or models.<br>▪ Use risk assessments to design exercises for Protection activities and to determine the feasibility of Mitigation projects and initiatives.<br>▪ Engage in a peer-to-peer mentoring structure that promotes effective practices. | |

| | Protection Core Capabilities | |
|---|---|---|
| 38 | **11. Supply Chain Integrity and Security** | **Description:** Strengthening the security and resilience of the supply chain.<br>This capability relies on securing and making resilient key nodes, methods of transport between nodes, and materials in transit between a supplier and consumer.<br>The expansive nature of the global supply chain renders it vulnerable to disruption from man-made 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. |
| 39 | **Critical Tasks:**<br>▪ Integrate security processes into supply chain operations to identify items of concern and resolve them as early in the process as possible.<br>▪ Use risk management principles to identify, mitigate vulnerabilities of, and protect key assets, infrastructure, and support systems.<br>▪ Implement physical protections, countermeasures, and policies to secure and make resilient key nodes, methods of transport between nodes, and materials in transit.<br>▪ 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.<br>▪ 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. | |

## Coordinating Structures and Integration

Coordinating structures provide the mechanisms to develop and deliver core capabilities at all levels of government, non-governmental organizations, and the private sector across the full range of Protection mission activities. The reliance on the full range of coordinating structures provides for the flexible, scalable, and adaptable approach to the delivery of core capabilities identified in PPD-8. This Framework recognizes, values, and leverages the robust array of existing coordinating structures, and identifies a Protection cycle and guiding principles that promote integration and synchronization across the various jurisdictions and areas of responsibility.

In the context of the Protection Framework, coordinating structures support steady-state Protection program implementation and strengthens the Nation's ability to increase the protective posture and enhanced steady-state Protection resources deployed during periods of heightened alert, terrorist threats, or times of increased vulnerability due to impending or actual disasters. 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.

Coordinating structures identified for this Framework are organized to enhance the effectiveness of the specified mission activities.

The range of coordinating structures that contribute to the Protection mission area includes, but is not limited to, the following: operations centers; state and major urban area fusion centers; critical infrastructure government councils; sector and cross-sector coordinating councils; governance boards; regional consortiums; information-sharing mechanisms; health surveillance networks; and public-private partnership organizations at all levels.

## *Community, Local, State, and Regional Coordinating Structures*

### Coordination through Partnerships

Protection mission activities and capabilities are coordinated through existing partnerships at all levels of government and with the private sector and non-governmental organizations. There are numerous examples of existing Protection partnerships ranging from neighborhood-based programs to regional public-private councils, joint task forces, and infrastructure protection coordinating councils. Many established community and regional groups promote actions to support Protection and preparedness. These partnerships may cross 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.

The National Infrastructure Protection Plan (NIPP), for example, promotes the use of a sector partnership model as the primary organizational structure for coordinating infrastructure protection efforts and activities. Sector-specific agencies (SSAs)[23] are responsible for critical infrastructure protection activities in specified sectors. Each sector has built partnerships with sector stakeholders, including facility owners and operators; local, state, tribal, territorial, and Federal Government agencies; the law enforcement community; trade associations; and state homeland security advisors. SSAs are responsible for working with both public and private partners to develop protective programs and resilience strategies. The NIPP model provides the structure that is used by all mission areas for effective coordination between government at all levels and the owners and operators of critical infrastructure.

Because of the specific challenges and interdependencies facing individual regions and the broad range and diversity of public and private sector Protection partners, regional efforts are often complex. Examples of regional partnerships formed to consider regional issues range from the Pacific NorthWest Economic Region (PNWER) partnership,[24] whose working groups look at such issues as border security, agriculture, and energy, to regional partnerships that focus on a single infrastructure sector, such as the Multi-State Partnership for Security in Agriculture.[25]

Voluntary public-private collaboration and information sharing between public and private sector partners is essential to meeting critical objectives for the Protection mission activities and sustaining Protection programs.

[23] The SSAs responsible for critical infrastructure protection for specified sectors are identified in Homeland Security Presidential Directive 7 (HSPD-7), Critical Infrastructure Identification, Prioritization, and Protection.
[24] 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. For additional information, refer to http://www.pnwer.org/.
[25] 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. For more information, refer to http://www.multistatepartnership.org/.

### National-level Partnership Councils

For many of these mission activities—Defense of Agriculture and Food, Critical Infrastructure Protection, Maritime Security, Transportation Security, Cybersecurity, and Health Security—the established sector, government, and cross-sector coordination councils and information-sharing mechanisms such as Information Sharing and Analysis Centers (ISACs) provide the foundation for Protection planning, risk management, and the implementation of protective programs. The NIPP sector partnership model mentioned above encourages formation of Sector Coordinating Councils (SCCs) and Government Coordinating Councils (GCCs). Together, SCCs and corresponding GCCs create a coordinated national structure for infrastructure protection and resilience within and across sectors. Additional information on the coordinating councils can be found in the NIPP.[26]

### Operational Coordination

In most jurisdictions, local operations centers are the focal point for coordinating the delivery of Protection capabilities to the whole community. In addition, state and major urban fusion centers support and inform operational coordination by serving as focal points within the state and local environments for the receipt, analysis, gathering, and sharing of threat-related information between government and private sector partners, while Joint Terrorism Task Forces (JTTFs) focus on terrorism-related investigations. Coordination with JTTFs 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.

### Coordination through Established Systems and Principles

This Framework promotes the use of principles such as those contained in the National Incident Management System (NIMS) to coordinate Protection activities across all levels of government, the private sector, and non-governmental organizations. NIMS 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. NIMS components, concepts, and principles support the transition of organizations that have 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 area. This section focuses on the policy-level coordination conducted through White House leadership, public-private partnerships, and those structures that are in place or need to be established to ensure a coordinated approach to Protection across the whole community.

### National Security Council

The President leads the Federal Government's Protection efforts to ensure that the necessary coordinating structures, leadership, and resources are applied quickly and efficiently to deliver the Protection core capabilities. The National Security Council, which brings together Cabinet officers and other department or agency heads as necessary, provides national strategic and policy advice to the President on a range of Protection issues.

[26] The NIPP is located at http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

## Federal Departments and Agencies

According to PPD-8, "The Secretary of Homeland Security is responsible for coordinating the domestic all-hazards preparedness efforts of all executive departments and agencies, in consultation with local, state, tribal, and territorial governments, non-governmental organizations, private sector partners, and the general public." Further, the Secretary of Homeland Security has been assigned specific responsibilities that include coordinating "the development and implementation of capabilities related to protection (except for defense activities which are the responsibility of the Secretary of Defense), and the development of the National Protection Framework and associated interagency operations plans."

The Federal Government promotes coordination within and across the Protection mission area through a wide range of coordinating structures. Under the Protection Framework, various Federal departments or agencies assume primary coordinating roles based on their authorities, the specific mission activities, and the nature of the threat or hazard (refer to Table 2). 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 Protection Framework and other Protection preparedness requirements established through PPD-8.

## Federal Interagency Protection Working Group

A Federal Interagency Protection Working Group (FIPWG) will be formed to enhance communication and coordination across the Protection mission area.[27] The Department of Homeland Security will lead the working group, which will be comprised of representatives from designated SSAs and/or Federal departments and agencies with delegated statutory and/or regulatory authority in one or more of the Protection mission activities.

FIPWG activities include the following:

- Facilitating preparedness planning and coordination in accordance with ongoing Protection and PPD-8 implementation efforts
- Sharing information pertinent to the Protection mission area
- Providing a forum for discussion of current issues and events, effective practices, and lessons learned
- Providing subject-matter expertise to collaboratively review, analyze, and make recommendations regarding the Protection mission area, National Protection Framework, and FIOP for Protection
- Promoting collaboration across the whole community
- Meeting semi-annually (or more frequently as needed) to:
  - Promote interagency coordination for the ongoing implementation and maintenance of the National Protection Framework and FIOP for Protection
  - Coordinate efforts for interagency Protection planning
  - Address common concerns and discuss recommended courses of action
  - Provide a forum for integration with Prevention, Mitigation, Response, and Recovery by coordinating with similar groups within those mission areas.

[27] The actions and recommendations of the FIPWG are not intended to interfere with or impede the normal course of Protection activities of its membership.

The FIPWG will be convened within 90 days of the issuance of the Protection Framework and will produce an agreed-upon charter within 180 days. The charter will describe working group membership, roles and responsibilities, rules of engagement, and relationships to existing coordinating structures that facilitate the full range of Protection mission activities.

## Steady-state Protection Process

This section summarizes the process to identify the measures necessary to protect against threats and hazards under steady-state conditions, i.e., within an organization's or jurisdiction's charter or mission, conducted on a routine basis (e.g., day-to-day), and within an anticipated level of effort. The responsibility for steady-state protection is shared by the Protection community, including individuals and their households, all levels of government, and the private sector.

Protection actions are taken at the borders, along the coastline, at international points of entry, and across every critical infrastructure sector. Protection actions take place primarily at the community and facility levels.

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 mission activities and core capabilities needed to accomplish the Protection mission.

Figure 4 depicts the steady-state Protection process.


**Figure 4: Steady-state Protection Process**

1. **Identify Protection mission goals and objectives.** The first 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.

2. **Engage coordination partners.** This step of the Protection cycle determines the size and scope of the community's/jurisdiction's local coordinating structures by identifying key Protection partners.[28] Protection partners will identify the core capabilities needed based on the Protection mission. During engagement, the roles and responsibilities for each Protection partner should be delineated.

3. **Gather data.** During this step, Protection partners gather data concerning potential threats and hazards from international and domestic terrorism, other human-caused incidents, natural disasters, 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 possible likelihood of occurrence and consequences of potential threats and hazards. This information will be used to inform the risk assessment and other requirements.

4. **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.[29] Whatever the method used, it is important to assess all potential threats, hazards, vulnerabilities, and consequences in a way that allows them to be compared and prioritized.

5. **Evaluate and prioritize.** In this step, Protection partners evaluate their preparedness for potential risks and prioritize Protection capability needs and efforts.

6. **Implement protective activities.** In this step, Protection partners identify the Protection activities, core capabilities, and resources needed to achieve the identified Protection goals and objectives. They implement protective activities to address the priorities established earlier in the process.

7. **Promote continuous improvement.** This step includes actions that ensure continuous improvement, such as training and exercising, identifying lessons learned, and reviewing evaluation results. This process may lead the community or jurisdiction to revisit any of the previous steps in the process.

[28] Potential partners were described earlier in the Coordination through Partnerships subsection.

[29] For critical infrastructure protection, the NIPP provides criteria that need to be met for risk assessment methodologies. For additional information, refer to the NIPP, Section 3.3.1. The NIPP is located at: http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

## Pre-incident Coordination Process

Pre-incident 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 5 depicts this pre-incident coordination process.

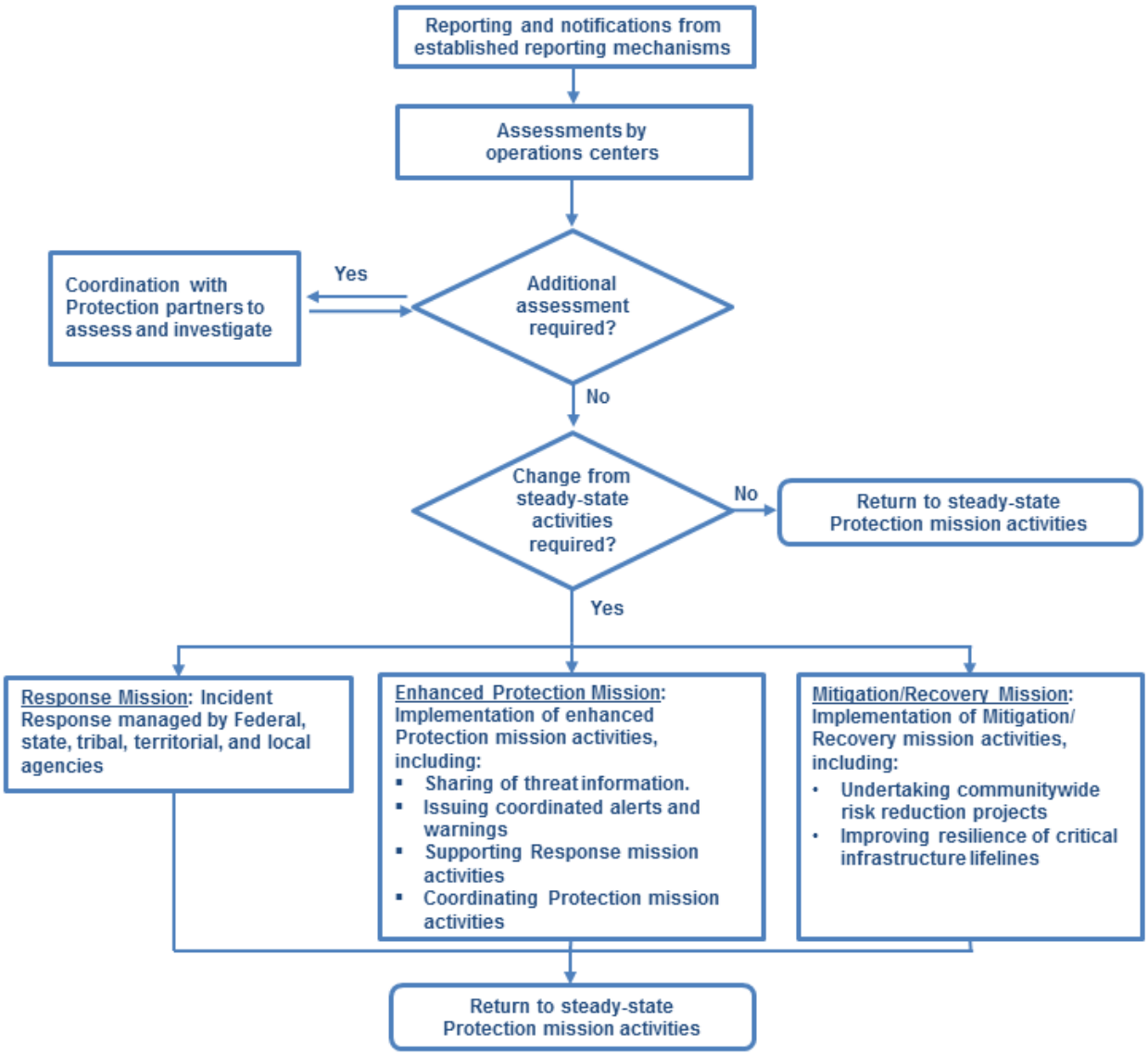


**Figure 5: Pre-incident Coordination Process**

- **Reporting and notifications.** Local, state, tribal, territorial, and Federal agencies, private sector, and non-governmental organizations share information about potential threats and hazards using established communications and reporting channels. Depending on the type of threat or hazard, government and private sector organizations either are 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. 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 Response Framework, along with enhanced steady-state Protection and Mitigation activities. Assessment of the emerging threat as a potential terrorist threat may require action in accordance with the Prevention Framework.
- **Response and enhanced steady-state protection activities.** Following assessment of the situation, the situation may require the initiation of Response mission activities and 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. Examples of enhanced steady-state Protection mission activities may include the following:
  - 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 national, state, and local levels to monitor health risks. The Department of Homeland Security uses the National Terrorism Advisory System to communicate information about terrorist threats to the public, government agencies, first responders, airports and other transportation hubs, and the private sector. Activation of the National Terrorism Advisory System delivers core capabilities for both Prevention and Protection.
  - Supporting Response mission activities by making sure that communities and responders have adequate protection during the crisis.
  - Coordinating enhanced Protection mission activities with Mitigation, Response, and Recovery mission activities through implementation of appropriate authorities and provision of resources.
- **Return to steady-state protection activities.** When enhanced steady-state Protection actions are no longer needed, there is a return to steady-state Protection mission activities.

## *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. Emphasis should be placed on innovative and non-governmental solutions. Many jurisdictions and private sector organizations enter into mutual aid agreements to identify shared resources.
- Coordinating and analyzing requirements using common planning assumptions, risk assessments, and/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 within each mission area provides the architecture to appropriately integrate mission activities when required for the concurrent delivery of core capabilities for Prevention, Protection, Mitigation, Response, and Recovery. Joint training and exercising promotes integration and supports unity of effort by allowing Protection and other mission area partners to align coordination and communication structures.

## Horizontal Integration

Protection partners integrate operations horizontally at the local, state, tribal, territorial, and Federal levels and across private sector organizations in the following ways:

- **Horizontal integration through partnerships and information sharing.** Protection activities are coordinated across functional areas within a jurisdiction, such as police, fire, emergency medical services, public health, and public works entities. Activities also are coordinated regionally with nearby jurisdictions that may share a common risk profile, resources, or information and support each other in delivering Protection core capabilities. Horizontal integration occurs between and among government entities and the private sector elements, community groups, and non-governmental organizations at all levels through partnerships and information sharing. Refer to Figure 6 for examples of horizontal integration.


**Figure 6: Horizontal Integration through Partnerships and Information Sharing**

- **Horizontal 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, the FIOPs[30], and the department-level operational plans. Specifically, all mission areas coordinate their frameworks with each other, focusing on integrating factors. These factors also are applied in the development and maintenance of FIOPs and the 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. The FIPWG provides a platform for horizontal integration across the Federal departments and agencies with responsibilities for Protection as well as between the mission areas.

### Vertical Integration

Vertical integration is a function of coordinating protection activities, by mission area, among all levels of government and the private sector. For example, states integrate their Protection activities both with local, tribal, and territorial jurisdictions, as well as with the Federal departments that support them in Protection operations. Pertinent regional organizations[31] also are included as essential elements of vertical integration; they can provide a bridge between the National and local levels. In addition, all levels of government participate in joint protection exercises to ensure integration of their Protection activities.

## Relationship to Other Mission Areas

This section describes the relationship between the Protection and the other mission areas. The Protection Framework addresses steady-state and enhanced steady-state actions that require coordination for the delivery of core capabilities needed to implement mission activities. The mission activities continue through steady-state and enhanced steady-state conditions 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**[32] and Protection mission areas are closely aligned. The Prevention mission area focuses on intelligence, regulatory, and law enforcement actions that seek out terrorists, their funding sources, and their weapons in order to prevent an attack. Protection activities, on the other hand, focus on government and private sector measures that deter or disrupt terrorist actions at the intended target and, like Mitigation, on minimizing the consequences of significant events. While Prevention activities focus specifically on imminent acts of terrorism, Protection efforts address the ongoing security of potential targets. Many activities traditionally considered preventative, such as disease prevention and cybersecurity, fall under the Protection mission area based on the definitions of Prevention and Protection in PPD-8.

Protection and Prevention share three of the same core capabilities. Processes described in these frameworks are designed to operate simultaneously and to provide for seamless transitions when

[30] The FIOPs are a required component of the National Preparedness System directed under PPD-8. Their intent is to provide guidance across the Federal Government to successfully implement the Frameworks.
[31] Examples of regional organizations include the PNWER Partnership, mentioned previously, and the All Hazards Consortium. The All Hazards Consortium facilitates regional integration between governments and private sector infrastructure owners and operators, primarily in the mid-Atlantic region of the United States. For additional information, see the All Hazards Consortium Website at http://www.ahcusa.org/.
[32] Prevention includes the capabilities necessary to avoid, prevent, or stop a threatened or actual act of terrorism. As defined by PPD-8, the term "prevention" refers to preventing imminent threats from terrorism.

needed to address specific threats. For example, during a period of imminent terrorist threat, Prevention focuses on information sharing and counterterrorism operations to prevent, deter, and preempt terrorism. Protection assesses 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 of disasters. Activities in the Mitigation and Protection mission areas 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 shared focus on critical infrastructure. Addressing the security of that infrastructure falls within the Protection mission area and the resilience of the infrastructure falls within the Mitigation mission area. Threat and hazard risk information and analysis are 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 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 area 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 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.

### 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.

## Operational Planning

The National Planning Frameworks explain the role of each mission area in national preparedness and provide the overarching strategy and doctrine for how the whole community builds, sustains, and deliveries 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, including the private and non-profit sectors and all levels of government. At the Federal level, each

framework is supported by a mission area-specific FIOP. Comprehensive Preparedness Guide (CPG) 101 provides further information on the various types of plans and guidance on the fundamentals of planning.

## Protection Operational Planning

Planning across the full range of Protection activities is an inherent responsibility of every level of government and the private 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, including the private and non-profit sectors and all levels of government to determine jurisdictional priorities, objectives, strategies, and resource acquisitions and allocations to protect against potential threats, conduct law enforcement investigations, and/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, state, tribal, territorial, and insular area operations.

### Department-level Operational Plans

Each executive department and agency will develop and maintain deliberate department-level operational plans where needed, as determined by the respective department or agency, 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 and/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.

### Federal Interagency Operational Plan for Protection

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

- Collaboration with all relevant stakeholders

- A detailed concept of operations[33] that explains how Protection operations are coordinated and executed in a collaborative fashion
- 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 the plan provides for multiple, geographically dispersed threats and hazards
- How Protection plans may be executed simultaneously with other plans.

In accordance with PPD-8, the Secretary of Homeland Security will coordinate the development of the Protection FIOP in collaboration with all Federal departments and agencies that play a role in the implementation of the Protection mission activities. Table 2 identified the Federal departments and agencies with predominant authorities or responsibilities for each of the Protection mission activities. The departments and agencies identified in the table have primary responsibility for engaging in the PPD-8 planning processes and engaging other Federal departments and agencies and others with relevant responsibilities related to the specific mission activity. The Protection FIOP will be reviewed and approved by the Transborder Security Interagency Policy Committee or a successor entity. The Secretary of the Department of Homeland Security is responsible for 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.

- The capabilities of individuals and households, communities and community organizations, private and non-profit entities, and local, state, tribal, and territorial governments play a critical role in Protection.
- Protection activities take place continuously and may be implemented concurrently with Prevention, Mitigation, Response, and Recovery capabilities.
- The Protection Framework focuses on steady-state, enhanced steady-state, or other situations that are directly related to the delivery of core capabilities for the specified mission activities.
- Protection resources are acquired, allocated, and assigned through the normal Federal budget and program processes.
- Protection responsibilities are decentralized and command and control capabilities are distributed among Federal departments and agencies, depending on the mission activity.

[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.

### Framework Application

Government and private sector partners can use the National Protection Framework to inform and align relevant planning, training, exercising, and other activities designed to enhance security for individuals, families, communities, organizations, and jurisdictions. The Protection processes and guiding principles contained in the 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 over the long term.

## Supporting Resources

A wide array of supporting resources is in place to support the various elements of the Protection mission area. These include Web-based information, training, and exercise programs that are available to both government and non-governmental partners. These resources include training programs for critical infrastructure protection, maritime and border security, and individual and personal security. Web-based information services include CitizenCorps.gov, FirstGov.gov, Ready.gov, and USAonWatch.org.

In addition, the following documents and guidelines support the development of interagency and other operational plans.

- The **NIPP** provides a unifying framework that integrates a range of efforts designed to enhance the safety of the Nation's critical infrastructure. It provides the coordinated approach that is used to establish national priorities, goals, and requirements for critical infrastructure protection so that Federal resources are applied in the most effective and efficient manner to reduce vulnerability, deter threats, and minimize the consequences of attacks and other incidents. The NIPP establishes the overarching concepts relevant to all critical infrastructure sectors identified under the authority of Homeland Security Presidential Directive 7, and addresses the physical, cyber, and human considerations required for effective implementation of protective programs and resilience strategies. The NIPP is located at: http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.
- The **SSPs** detail the application of the NIPP risk management framework to the unique characteristics and risk landscape of each of the NIPP critical infrastructure sectors and provide the means by which the NIPP is implemented within the sectors. The sector-specific plans are available at: http://www.dhs.gov/files/programs/gc_1179866197607.shtm#2.
- The **Comprehensive National Cybersecurity Initiative (CNCI)** consists of a number of mutually reinforcing initiatives designed to help secure the United States in cyberspace. The goals of the CNCI are to ensure an organized and unified response to future cyber incidents; strengthen public/private partnerships to find technology solutions that ensure U.S. security and prosperity; invest in the cutting-edge research and development necessary for the innovation and discovery to meet the digital challenges of our time; and begin a campaign to promote cybersecurity awareness and digital literacy from our boardrooms to our classrooms and begin to build the digital workforce of the 21st century. For more information on the CNCI, refer to: http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.
- The **National Strategy for Global Supply Chain Security** is focused on the worldwide network of transportation, postal, and shipping pathways, assets, and infrastructures (including communications and information infrastructures). It provides strategic guidance to departments and agencies within the U.S. Government and identifies priorities to collaboration stakeholders. The goals of the Strategy are twofold: to promote the efficient and secure movement of goods

and to foster a global supply chain system that is prepared for and can withstand evolving threats and hazards and rapidly recovery from disruptions. The document is available at: http://www.whitehouse.gov/sites/default/files/national_strategy_for_global_supply_chain_security.pdf.

- Other resources include existing department-level operational plans and concepts of operations related to applicable programs used in carrying out Protection mission activities, as well as charters for Protection-related councils.

## Conclusion

The shared responsibility for the Protection mission area builds from the individual level and the community level to local jurisdictions, state, tribal, and territorial governments, and the Federal Government. This Framework assists the whole community in protecting against the greatest risks to our Nation from all hazards in a manner that allows our interests, aspirations, and way of life to thrive.

This Framework provides individual, community, non-governmental organization, private sector, and governmental decisionmakers with an understanding of the full spectrum of Protection mission activities and what they can do to ensure our Nation is optimally protected from man-made and natural disasters. Initiatives based on Protection mission activities and core capabilities help guide a community to create conditions for a safer, more secure, and more resilient Nation by enhancing Protection through cooperation and collaboration.

America's security and resilience work is never finished. While we are safer, stronger, and better prepared than a decade ago, we remain resolute in our commitment to safeguard the Nation against the greatest risks it faces, now and for decades to come. This means that this Framework is a living document, and it will be regularly reviewed to evaluate consistency with existing and new policies, evolving conditions, and the experience gained from its use. The first review will be completed no later than 18 months after the release of the Framework. Subsequent reviews will be conducted in order to evaluate the effectiveness of the Framework on a quadrennial basis.