

Protection Federal Interagency Operational Plan

First Edition

August 2016



Homeland
Security

Table of Contents

INTRODUCTION	1
PURPOSE	2
AUDIENCE	3
SCOPE	3
OBJECTIVES	4
PLAN APPLICATION	4
SITUATION	5
MISSION	6
ORGANIZATION	6
PLANNING ASSUMPTIONS	7
CRITICAL CONSIDERATIONS	7
CONCEPT OF OPERATIONS	9
STEADY STATE PROTECTION	11
ESCALATED OPERATIONS	11
CORE CAPABILITIES	15
COORDINATING ACTIVITIES	16
COORDINATION MECHANISMS	17
COORDINATION AND SUPPORT	24
OVERSIGHT, PLAN DEVELOPMENT, AND MAINTENANCE	26
ANNEX A: ALIGNMENT	A-1
INTEGRATION WITH EXISTING PLANS, STRATEGIES, AND DOCTRINE	A-1
RELATIONSHIP WITH NATIONAL PREPAREDNESS PLANNING FRAMEWORKS AND FIOPs	A-1
ANNEX B: PROTECTION CORE CAPABILITY PLANNING	B-1
PROTECTION CRITICAL TASKS BY CORE CAPABILITY	B-1
APPENDIX 1 TO ANNEX B: COMMON CORE CAPABILITIES (PLANNING, PUBLIC INFORMATION AND WARNING, AND OPERATIONAL COORDINATION)	B.1-1
APPENDIX 2 TO ANNEX B: ACCESS CONTROL AND IDENTITY VERIFICATION	B.2-1
APPENDIX 3 TO ANNEX B: INTELLIGENCE AND INFORMATION SHARING	B.3-1
APPENDIX 4 TO ANNEX B: INTERDICTION AND DISRUPTION	B.4-1
APPENDIX 5 TO ANNEX B: SCREENING, SEARCH, AND DETECTION	B.5-1
APPENDIX 6 TO ANNEX B: PHYSICAL PROTECTIVE MEASURES	B.6-1
APPENDIX 7 TO ANNEX B: RISK MANAGEMENT FOR PROTECTION PROGRAMS AND ACTIVITIES	B.7-1

APPENDIX 8 TO ANNEX B: CYBERSECURITY..... B.8-1
APPENDIX 9 TO ANNEX B: SUPPLY CHAIN INTEGRITY AND SECURITY B.9-1
ANNEX C: COORDINATING ACTIVITIES C-1
APPENDIX 1 TO ANNEX C: BORDER SECURITY..... C.1-1
APPENDIX 2 TO ANNEX C: CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE C.2-1
APPENDIX 3 TO ANNEX C: DEFENSE AGAINST WMD THREATS..... C.3-1
APPENDIX 4 TO ANNEX C: HEALTH SECURITY..... C.4-1
APPENDIX 5 TO ANNEX C: IMMIGRATION SECURITY C.5-1
APPENDIX 6 OF ANNEX C: MARITIME SECURITY C.6-1
**(U//FOUO) APPENDIX 7 TO ANNEX C: PROTECTION OF KEY LEADERSHIP AND SPECIAL
EVENTS C.7-1**
APPENDIX 8 TO ANNEX C: TRANSPORTATION SECURITY..... C.8-1
ANNEX D: SELECTED GLOSSARY D-1
ANNEX E: LIST OF ACRONYMS E-1

Introduction

The National Preparedness System outlines an organized process for the whole community¹ to achieve the National Preparedness Goal. The National Preparedness System integrates efforts across the five preparedness mission areas—Prevention, Protection, Mitigation, Response, and Recovery—to achieve the goal of a secure and resilient Nation. One component of the National Preparedness System is a Federal Interagency Operational Plan (FIOP) for each mission area that provides a detailed description of roles and responsibilities, specifies the critical tasks, and identifies Federal resourcing requirements for delivering national preparedness core capabilities.²

Protection comprises the capabilities necessary to secure the homeland against acts of terrorism and manmade or natural disasters. The Protection FIOP builds upon the National Protection Framework, which sets the strategy and doctrine for how the whole community builds, sustains, and delivers the Protection core capabilities. Federal departments and agencies maximize the effectiveness of Protection core capabilities through a range of *coordinating activities*. *Coordinating activities* are the primary, but not exclusive, Federal coordinating mechanisms for building, sustaining, and delivering the Protection core capabilities. Because the *coordinating activities* are autonomous as well as interdependent, this FIOP focuses on how existing Federal capabilities support local, state, tribal, and territorial partners and how those capabilities support each other. The concepts of operations contained in the Protection FIOP are scalable, flexible, and adaptable, allowing the FIOP to be used across the range of Protection *coordinating activities*. Critical tasks are defined actions that are executed by organizations to deliver the Protection core capabilities. Concepts of operations and/or tasks may be modified, added, or deleted depending upon the risk, mission activity, or threat.

Additional National Preparedness System requirements:

- Where needed, each Federal department and agency will develop and maintain deliberate department-level operational plans to deliver capabilities to fulfill responsibilities under the frameworks and FIOPs.
- Departments and agencies may use existing plans, protocols, standard operating procedures (SOP), or guides for the development of such plans; these should be updated as needed.
- Individuals with disabilities and other people who have access and functional needs must be included in all whole community planning activities and must have equal access to and equal participation in all Protection functions.³

¹ The whole community includes individuals and communities, the private and nonprofit sectors, faith-based organizations, and all levels of government (local, regional/metropolitan, state, tribal, territorial, insular area, and Federal). Whole community is defined in the National Preparedness Goal as “a focus on enabling the participation in national preparedness activities of a wider range of players from the private and nonprofit sectors, including nongovernmental organizations and the general public, in conjunction with the participation of all levels of government in order to foster better coordination and working relationships. Used interchangeably with ‘all-of-Nation.’”

² Core capabilities are defined as “distinct critical elements necessary to achieve the National Preparedness Goal.”

³ Participation in all phases of exercise planning and execution at local levels is a critical part of disability inclusion. The Department of Homeland Security (DHS) defines “access and functional needs” as “circumstances that are met for providing physical, programmatic, and effective communication access to the whole community by accommodating individual requirements through universal accessibility and/or specific actions or modifications.

Purpose

This FIOP describes how the Federal departments and agencies work together to deliver Protection core capabilities through eight *coordinating activities*. Protection *coordinating activities* enable the Federal Government to:

- Deliver the core capabilities for the mission area and
- Execute the critical tasks associated with each core capability.

These activities support and integrate Protection efforts during steady state (day-to-day activities) and escalated activities that flow from emergent threats and elevated risks.⁴ The Protection mission, as defined in the National Preparedness Goal, requires Federal departments and agencies to coordinate activity organized under an array of existing authorities, policy directives, operational plans, and relationships. The Protection FIOP does not supersede or direct planning conducted under applicable legal authorities, but serves as the National Preparedness System plan for aligning and synchronizing the *coordinating activities*. Each appendix in Annex C of this FIOP describes key authorities, policies, plans, and coordinating structures as well as how individual *coordinating activities* support other *coordinating activities*.

The scope of the Protection mission area is expansive, covering topics from border security to health security to critical infrastructure security and resilience. In addition, Federal departments and agencies deliver Protection capabilities through distinct authorities and decentralized activities. Therefore, it is critical that the *coordinating activities* in the Protection mission enable information sharing, shared situational awareness, and synchronization of Federal activities. The concept of operations for Protection comes from the principles and concepts in the National Protection Framework and serves as a common reference for the development of contingency or coordinating activity-specific Protection plans. The concept of operations described in this FIOP provides the necessary Federal structure for managing these protection concerns.

Synchronization between the Protection *coordinating activities* expands and contracts based on the active monitoring of information, needs, and threats. Protection *coordinating activities* mainly take place through the day-to-day conduct of Protection activities and the delivery of the Protection core capabilities—i.e., in steady state. But protective actions are also delivered during times of elevated risk, requiring Federal departments and agencies to coordinate, adapt, and align activities. This FIOP provides operational guidance for alignment of Protection *coordinating activities* during steady state and escalated operations. Table 1 summarizes the purpose of the Protection FIOP.

This includes assistance, accommodation, or modification for mobility, communication, transportation, safety, health maintenance, need for assistance, accommodation or modification due to any situation (temporary or permanent) that limits an individual’s ability to take action in an emergency.”

⁴ See Figure 3: Decision Making for Enhanced Protection Activity for a detailed description of the Protection decision making process.

Table 1: FIOP Summary

THE PROTECTION FIOP:	THE PROTECTION FIOP IS NOT/DOES NOT:
Is a document that provides guidance and a concept of operations to facilitate the development of departmental and agency operational plans.	A contingency or implementation plan based on threat(s) or scenario(s).
<ul style="list-style-type: none"> ▪ Describes a Federal approach that departments and agencies can apply to align and integrate the Protection mission. ▪ Addresses Federal department/agency protection roles and responsibilities. ▪ Informs local, state, tribal, territorial, and private sector partners about the ways that departments and agencies deliver Federal capabilities. ▪ Includes security measures taken in response to emergent threats or elevated risks. 	<ul style="list-style-type: none"> ▪ Establish requirements on how Federal departments/agencies will coordinate their Protection requirements. ▪ Address local, state, tribal, territorial, private sector, and individual roles and responsibilities. ▪ Supersede or direct planning conducted under applicable legal authorities.

Audience

While the National Protection Framework provides guidance for the whole community, the Protection FIOP is directed toward Federal departments and agencies. Departments, agencies, Federal coordinating structures, and interagency partnerships should use this FIOP as a guide for Protection operations. Federal departments and agencies will develop and maintain department-level operational plans, as necessary, to deliver capabilities outlined within the National Protection Framework and the Protection FIOP. Local, state, tribal, and territorial partners are encouraged to work with Federal departments and agencies’ coordinating structures and use this FIOP to align planning efforts across all levels of government.

Scope

This document is written for and is applicable across all Federal departments and agencies involved in protecting people, property, critical assets, systems, and networks against the greatest risks to the Nation.⁵ Additionally, it serves as a guide to how the Federal Government builds Protection core capabilities with local, state, tribal, and territorial governments; the private sector; nongovernmental organizations (NGO); and individuals. The scope of the Protection FIOP is summarized in [Table 2](#).

⁵ The Nation includes the U.S. states, territories, and possessions defined as “the United States” in the Homeland Security Act of 2002 § 2(17) (A), as amended.

Table 2: Protection FIOP Scope

	Description
Purpose	Describes how the Federal Government will deliver Protection core capabilities.
Audience	Federal departments/agencies involved in protecting people, critical assets, systems, and networks against the greatest risks to the Nation. Additionally, the “Whole of Community” involved in Protection and Protection-related activities.
Concept of Operations	Federal departments/agencies coordinate decentralized Protection activities conducted under applicable legal authorities and through existing plans and coordinating structures.
Core Capabilities	Distinct critical elements necessary to achieve the National Preparedness Goal.
Coordinating Activities	Protection covers multiple spheres of operations. These stem from statutory authorities and existing Federal coordination structures that are led, coordinated, and integrated by the Federal Government to secure the homeland against acts of terrorism and manmade or natural disasters.

Objectives

The Protection FIOP will accomplish the following:

- Provide a concept of operations for integrating existing Federal capabilities to secure the homeland against natural, technological, and adversarial hazards;
- Describe the Protection *coordinating activities* and illustrate how these *coordinating activities* support each other during steady state and escalated operations;
- Provide an overview of Federal Protection core capability resources;
- Describe Federal operational coordination mechanisms that integrate resources and personnel;
- Explain how Protection integrates with other mission areas in creating conditions for a safer, more secure, and more resilient Nation;
- Lay the foundation for further Federal department or agency Protection planning, including integration among *coordinating activities*;
- Increase routine engagement across the Protection mission space, so that emerging issues can be more readily shared across mission areas;
- Formalize the coordination and decision making process, which supports operational activities during periods when enhanced protective measures are warranted; and
- Identify shared activities where multiple members of the protection mission space can benefit from shared lessons learned or increased collaborative activities.

Plan Application

The Protection mission occurs continuously and is implemented concurrently with Prevention, Mitigation, Response, and Recovery capabilities; therefore, the Protection FIOP is in effect at all times. As such, there are situations where the Protection FIOP overlaps with FIOPs for other mission areas. Annex A of this FIOP describes Protection’s relationship with each mission area and explains how Protection *coordinating activities* support other mission areas before, during, and after an incident.

Nothing in this FIOP is intended to interfere with the execution of the existing roles, responsibilities, and authorities of individual departments and agencies.

Situation

Strategic Environment

Protection stakeholders exist in a strategic environment that includes threats and hazards from three categories: natural disasters, technological/accidental incidents, and adversarial/human-caused incidents, such as terrorism. Issues including globalization, technological innovation, demographic shifts, increasing population in vulnerable areas, escalating resource demands, climate change, and security concerns, such as proliferation of Weapons of Mass Destruction (WMD) and the movement of people across borders, contribute to the complexity of future disasters. These challenges indicate a future environment that presents a wide range of problems that occur unpredictably and perhaps simultaneously.

Constraints on resources at all levels continue to force the Nation to reconsider which security and resilience activities are truly affordable and how partnerships can be built to accomplish the objectives for a secure and resilient Nation. The challenge is to build a culture of preparedness to empower the whole community to be resilient in the face of disruptions, disasters, and other crises while adapting to conditions that have changed as a result of an incident.

Federal departments and agencies are advocates for and ensure that all populations have equal access to acquire, use, and contribute to the core capabilities that strengthen resilience. Engaging all members of the whole community is essential to national preparedness, and individuals and communities are key components. With equal access to the pertinent knowledge and skills, all members of the community can contribute to national preparedness.

Risk and Threat

Risk is the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.⁶ It is assessed based on applicable threats and hazards, vulnerabilities, and consequences. For the Protection mission area, the emphasis on risk-informed decision making and planning promotes an understanding of what needs to be protected and ensures that security, resilience, and sustainability guide investment decisions.

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

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

⁶ DHS Risk Steering Committee, *DHS Risk Lexicon*, Washington, DC, 2011.

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

The SNRA results contained in the National Preparedness Goal focus on contingency incidents, which are typically defined by beginning and end points. With the exception of climate change, only incidents with a distinct beginning and end, and those with an explicit nexus to homeland security missions, were included. The SNRA results do not explicitly assess a range of persistent steady state risks, such as border and trade violations, illegal immigration, drug trafficking, and intellectual property violations, which account for a significant component of the steady state Protection efforts. Recognition of routine and ongoing Protection responsibilities, along with the SNRA results within the National Preparedness Goal, guided the development of the National Protection Framework and the Protection FIOP and should inform capability-based analysis.

Mission

The Federal Government will conduct the Protection mission through *coordinating activities* that secure the homeland against natural, technological, and adversarial hazards. The Federal Government also works with local, state, tribal, and territorial partners to build capacity, share best practices, and enable coordination and integration of Protection core capabilities across geographic and jurisdictional boundaries.

Organization

The Protection FIOP is organized (Table 3, below) as a single base plan with annexes for the joint development of core capabilities and the mutual support of Protection *coordinating activities*.

Table 3: Protection FIOP Organization

Section	Description
Base Plan	Provides a concept of operations and describes the mechanisms by which independent <i>coordinating activities</i> conducted under applicable legal authorities are mutually supportive and coordinated as required.
Annex A	Orients the Protection FIOP within the overall scheme of the National Preparedness System.
Annex B	Describes the Federal role in building Protection core capabilities and describes the shared execution structure for critical tasks.
Annex C	Provides summary appendices for key Protection <i>coordinating activities</i> . Each operational appendix describes the concept of operations, coordination structures, connection to other mission areas, key plans, and key authorities and references for each activity. This section serves as an operational guide to protection coordination and highlights applicable legal authorities, existing plans, and coordination structures for protection.
Annex D	Includes a glossary of key terms for Protection.

Planning Assumptions

Assumptions consist of information accepted by planners as true in the absence of facts. Assumptions are not predictions. Assumptions are only used when facts are unavailable. Using assumptions allows planners to further define the scenario, identify potential response requirements, and move forward with the planning process. Assumptions are a baseline set for planning purposes, and they do not take the place of specific activities or decision points related to specific risks or *coordinating activities*. The following planning assumptions assist in the development of an operational environment for this FIOP.

- A catastrophic incident or attack, including follow-on attacks, will occur at any time of day with little or no warning, will involve single or multiple geographic areas, and will result in mass casualties.
- Situational awareness of the operational environment will be incomplete.
- Protection core capability critical tasks take place continuously and may be implemented concurrently with Prevention, Mitigation, Response, and Recovery core capabilities.
- Federal Protection resources are acquired, allocated, and assigned through the normal Federal budget and program processes.
- Protection responsibilities are decentralized and capabilities are distributed among local, state, tribal, territorial, and Federal departments and agencies, depending on the mission activity.

Nothing in this document is intended to alter or impede Federal departments' and agencies' (or local, state, tribal, and territorial governments') abilities to perform their statutory responsibilities, nor does it alter or impede Presidential guidance. Nothing in this FIOP is intended to interfere with the execution of the roles and responsibilities and the authorities of individual departments and agencies concerning counterterrorism, counterintelligence, law enforcement, or other related missions.

Critical Considerations

Critical considerations are elements of information that must be taken into account when developing a plan. The following are critical considerations when developing a Protection plan:

- The value proposition for the Protection FIOP is to promote interconnectivity and mutual support across Protection *coordinating activities* by providing a concept of operations based on aligning

mutually supportive activity to address emergent or persistent Protection issues across Federal departments and agencies.

- Federal departments and agencies conduct Protection *coordinating activities* pursuant to existing authorities.
- Protection *coordinating activities* are conducted with local, state, tribal, and territorial governments and Protection mission partners operating under existing authorities.
- Coordination of independent Federal Protection activities occurs as described in this FIOP.
- Priorities to employ Federal Protection capabilities will change based on the situation. During escalated decision making conditions or an actual terrorist incident, Protection, Prevention, and Response mission operations will be concurrent.
- Unity of effort will be required with Prevention and Response mission areas to resolve threats, save lives, and protect property.

Concept of Operations

The Protection FIOP is an all-hazards plan that describes how the Federal Government will develop shared situational awareness and operational alignment within the Protection mission. This document describes how the Federal departments and agencies work together to deliver Protection core capabilities through *coordinating activities* during steady state and escalated decision making operations that flow from emergent threats and elevated risks.

The Protection mission is executed without a centralized management structure, funding source, or single command and control paradigm (see Figure 1). Protection *coordinating activities* are conducted independently under existing authorities, using existing coordinating mechanisms. To deliver Protection core capabilities, these activities are mutually supportive and rely on shared situational awareness. Coordination occurs within both steady state delivery of protection capabilities and the escalated decision making and heightened protective activity that accompany emergent threats or elevated risks.

A broad range of existing legal authorities, policies, Executive orders (EO), and regulations order the way that *coordinating activities* operate within the Protection mission. In defining and describing the Protection mission, the National Preparedness System promotes a mutually supportive Federal Protection ecosystem and illustrates the way that *coordinating activities* are aligned and the concept of operations for the Protection mission.

Protection *coordinating activities* deliver the core capabilities for the mission area and execute the critical tasks associated with each core capability. Annex B of this FIOP summarizes the way tasks are shared across *coordinating activities*, and Annex C provides greater detail regarding their execution.

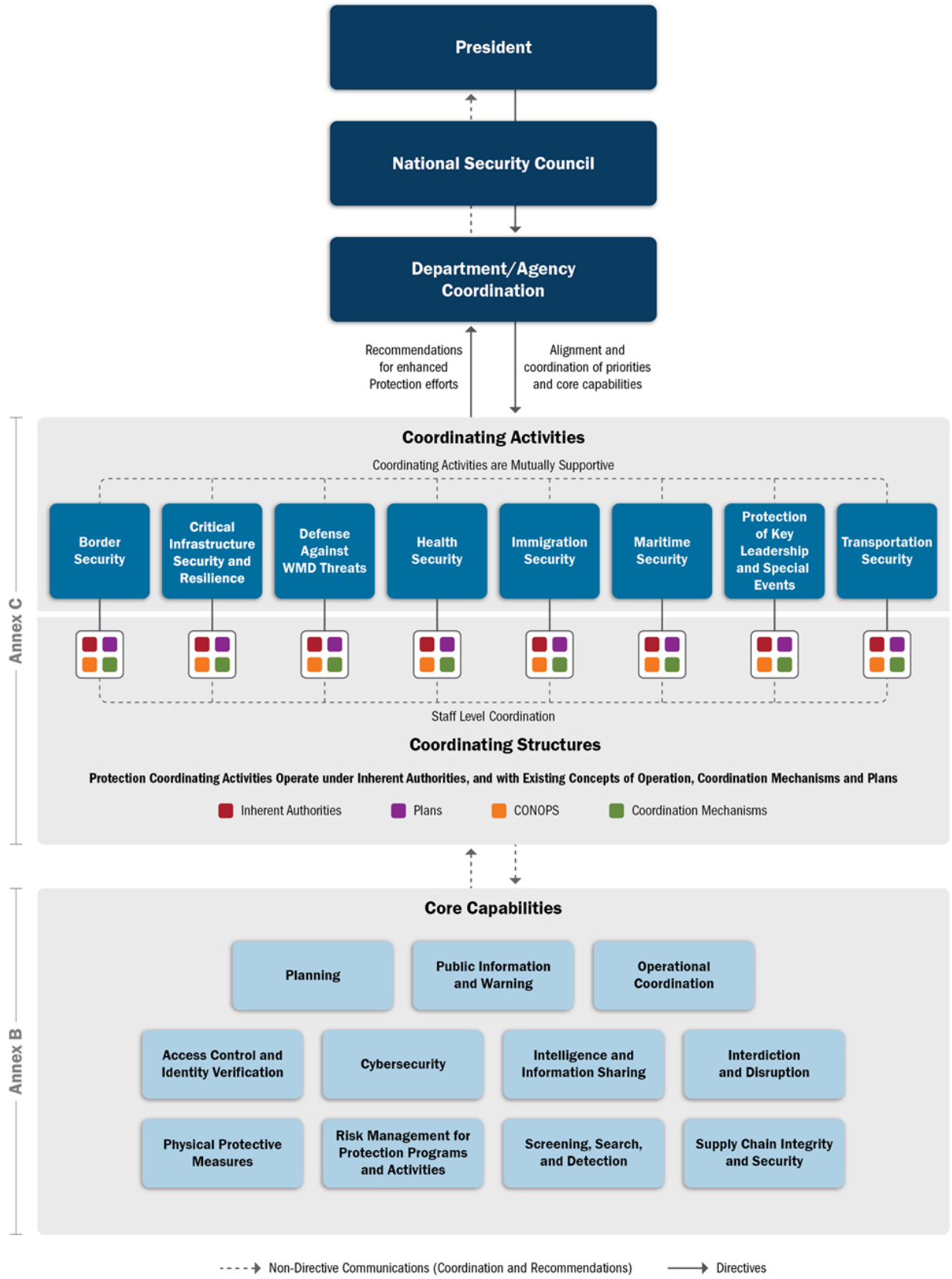


Figure 1: Protection Concept of Operations

Steady State Protection

During steady state operations, Protection *coordinating activities* are conducted independently under applicable legal authorities through plans, concepts of operation, and coordination structures. The decision making process outlined in the National Protection Framework (see Figure 2) serves as a model for assessing and responding to risks, and the Protection core capabilities further described in Annex B of this FIOP provide a model for the steady state development of Federal core capabilities and Federal mechanisms for either supporting or delivering those capabilities.

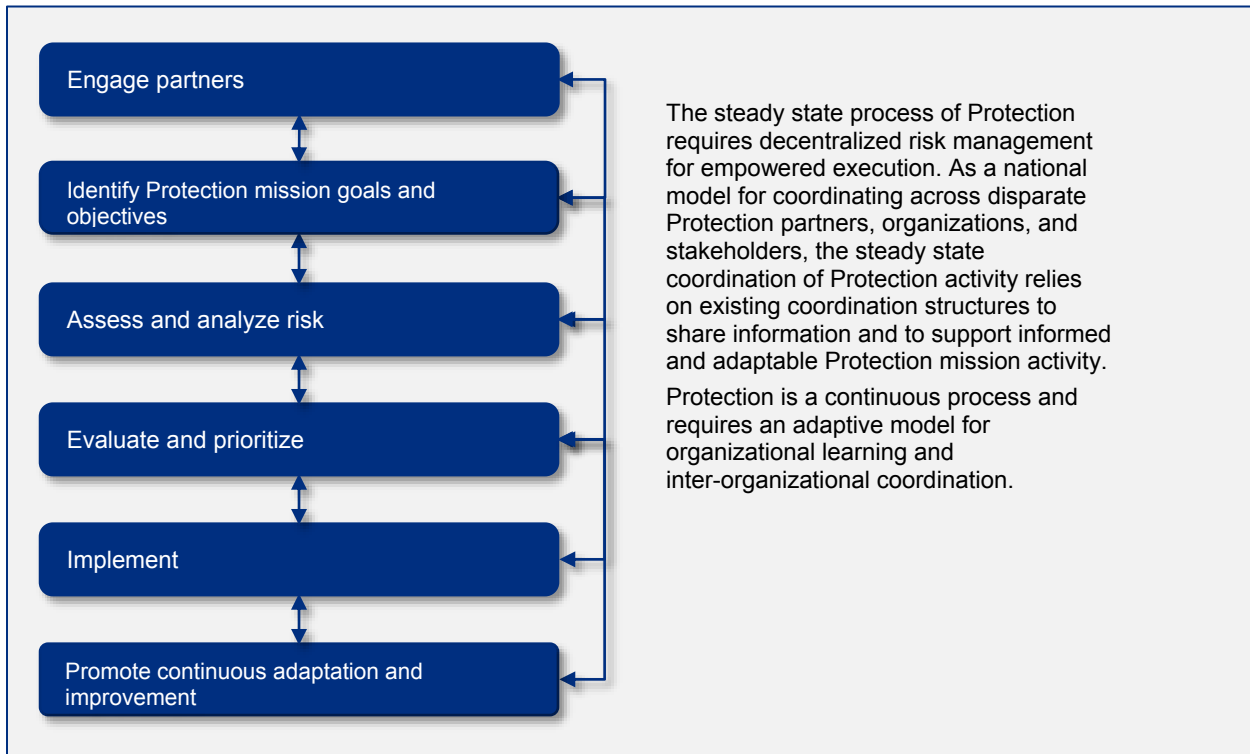


Figure 2: Steady State Protection Decision Making

Escalated Operations

Protection activity may escalate in response to elevated threats or increased risks and often requires coordination across multiple mission departments, agencies, coordination mechanisms, and existing plans and structures. This coordination follows the model described in this FIOP for escalation and coordination and includes transitioning support to other mission area activities (particularly Response and Prevention mission areas). Protection partners may increase their posture based on internal requirement and legal authorities. Coordination and the incorporation of other Protection capabilities occur through existing arrangements and deliberate plans, but may also require coordination across Protection activities. The decision to escalate Protection activity can originate with any Federal department or agency, as well as within any of the Protection coordination mechanisms, but follows a common decision making process.

This page intentionally left blank.

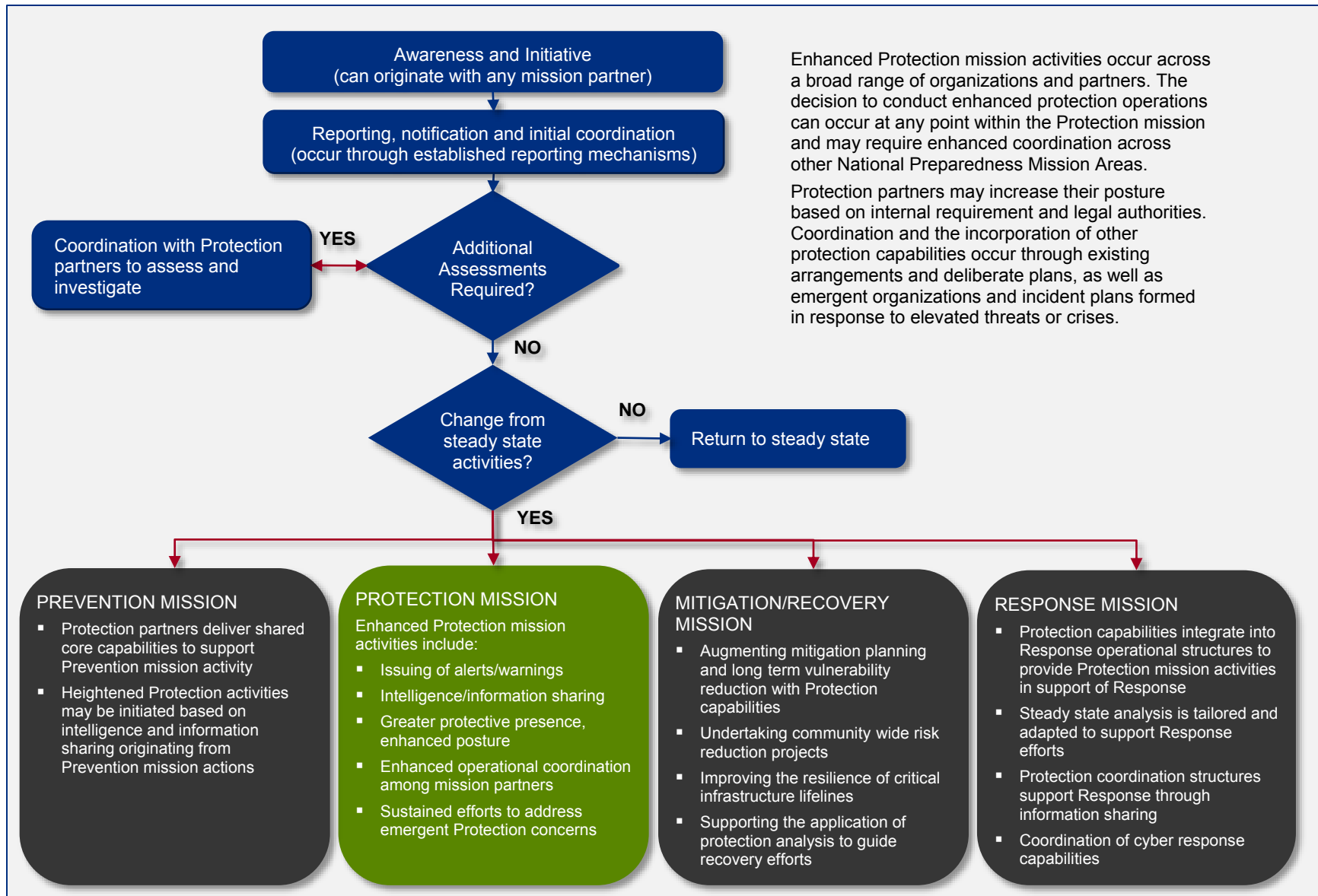


Figure 3: Decision Making for Enhanced Protection Activity

This page intentionally left blank.

As shown in Figure 4, during Response, Recovery, or Prevention operations, steady state Protection continues uninterrupted, even when additional capabilities and resources are delivered in support of enhanced Protection activities or in support of other mission area activities. Protection capabilities also mobilize to support Prevention, Response, and Recovery operations, as described in the FIOPs for those mission areas.

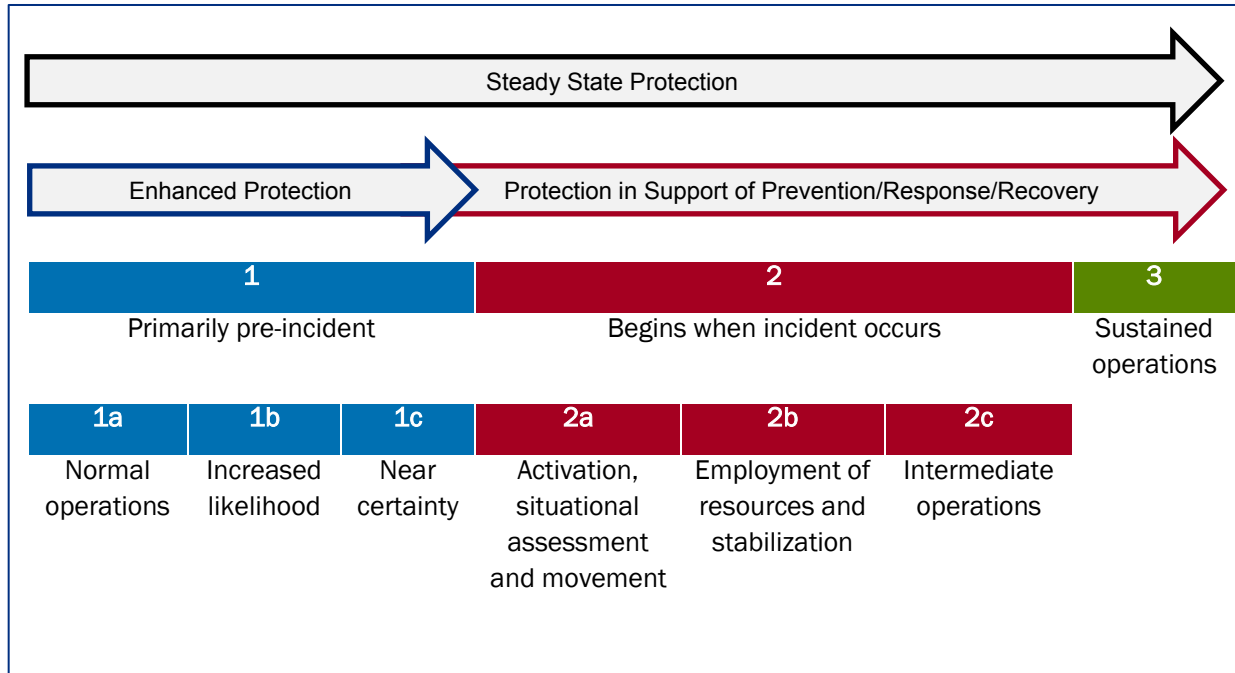


Figure 4: Protection Capabilities Support Operational Phases

Core Capabilities

As described in the National Protection Framework, Protection core capabilities are developed and delivered across the whole community of national preparedness. Protection capabilities provide a common structure for developing and ordering protection planning efforts and a means to assess preparedness efforts. Annex B provides a detailed description of the Federal role in supporting and delivering protection core capabilities.

- **Planning:** Conducting a systematic process that engages the whole community, as appropriate, in the development of executable strategic, operational, tactical and community-based approaches to meet defined Protection objectives. Planning includes the development, exercise, and maintenance of multidisciplinary plans that provide joint guidance across Protection mission activities.
- **Public Information and Warning:** 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.
- **Operational Coordination:** Establishing and maintaining unified and coordinated operational structures and processes that appropriately integrate all critical stakeholders and support the execution of core capabilities.

- **Access Control and Identity Verification:** 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.
- **Intelligence and Information Sharing:** Providing timely, accurate, and actionable information resulting from intelligence processes concerning threats to the United States, its people, property, or interests; the development, proliferation, or use of WMD; or any other matter bearing on U.S. national or homeland security by local, state, tribal, territorial, Federal, and other stakeholders.
- **Interdiction and Disruption:** Delaying, diverting, intercepting, halting, apprehending, or securing threats and/or hazards.
- **Screening, Search, and Detection:** 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.
- **Physical Protective Measures:** 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.
- **Risk Management for Protection Programs and Activities:** Identifying, assessing, and prioritizing risks to inform Protection activities and investments.
- **Cybersecurity:** Protecting against damage to, unauthorized use of, and/or malicious exploitation of (and, if needed, the restoration of) information and communications technologies (and the data contained therein).
- **Supply Chain Integrity and Security:** Strengthening the security and resilience of the supply chain.

Coordinating Activities

Protection covers multiple spheres of operation. These stem from existing authorities and Federal coordination structures that are led, coordinated, and integrated by the Federal Government to secure the homeland against natural, technological, and adversarial hazards. Protection *coordinating activities* are existing means of ordering and coordinating the Protection mission and maintaining plans, coordination structures, and resource arrangements. The Protection FIOP describes the way that departments and agencies align separate Protection *coordinating activities*.

This FIOP contains separate Protection Activity Appendices that provide a description of Federal department and agency responsibilities and coordinating structures for existing Protection *coordinating activities*, as well as how they engage and contribute to the delivery of core capabilities discussed in the National Protection Framework. The Protection *coordinating activities* addressed in this FIOP are not an exhaustive or exclusive list. As Protection concerns emerge, the mission adapts and evolves to address them. The eight *coordinating activities* described in this FIOP are existing means of conducting Protection activity within distinct and established domains of operation, while preserving civil rights, respecting privacy, and protecting civil liberties.

The Protection *coordinating activities* deliver the core capabilities for the mission area and execute the critical tasks associated with each core capability. Annexes addressed in this FIOP are summarized below:

- **Border Security:** Securing U.S. air, land, and sea ports and borders against the illegal flow of people and goods, while facilitating the flow of lawful travel and commerce.

- **Critical Infrastructure Security and Resilience:** Protecting the physical and cyber elements of critical infrastructure. This includes actions to deter the threat, reduce vulnerabilities, or minimize the consequences associated with a terrorist attack, natural disaster, or manmade disaster. Critical infrastructure security and resilience is detailed in the National Infrastructure Protection Plan (NIPP 2013).⁷
- **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.
- **Health Security:** Securing the Nation and its people to be prepared for, protected from, and resilient in the face of incidents with health consequences.
- **Immigration Security:** Securing the Nation from illegal immigration through the effective and efficient enforcement of immigration law, through systems and processes that respect human and civil rights.
- **Maritime Security:** Securing U.S. maritime infrastructure, resources, and the Marine Transportation System (MTS) from terrorism and other threats and hazards and securing the homeland from an attack from the sea, while preserving civil rights, respecting privacy and protected civil liberties, and enabling legitimate travelers and goods to move efficiently without fear of harm or significant disruption.
- **Protection of Key Leadership and Special Events:** Safeguarding Government executive leadership from hostile acts by terrorists and other malicious actors and ensuring security at events of national significance.⁸
- **Transportation Security:** Securing U.S. transportation systems and the air domain against terrorism and other threats and hazards, while preserving civil rights, respecting privacy and protected civil liberties, and enabling legitimate travelers and goods to move without fear of harm or significant disruption.

Coordination Mechanisms

The National Protection Framework and the concept of operations for this FIOP describe the decentralized and network-centric way that the Federal Government delivers Protection core capabilities. An array of existing coordinating structures provides the mechanisms to develop and field Protection core capabilities. Across the Federal Government, these coordinating structures facilitate partnerships, planning, information sharing, and resource and operational coordination

⁷ Critical infrastructure, as defined by section 1016(e) of the USA PATRIOT Act of 2001 (42 U.S.C. Section 5195c (e)), includes those systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security; economy; public safety or health; environment; or any combination of these matters, across any jurisdiction. Critical infrastructure security and resilience addresses sectors along common functions that include chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

⁸ Key leaders are defined as current and former Presidents, Vice Presidents, their families, and others who receive protection from the United States Secret Service. Events of national significance fall within two categories: National Special Security Events (NSSE) as defined in Title 18, U.S.C. Section 3056(e) and further clarified in PPD-22, and events assessed under the Special Event Assessment Rating (SEAR) process by the DHS and the Federal Bureau of Investigation (FBI) based on input from local, state, tribal, territorial, and Federal law enforcement entities.

within the Protection mission. The Protection core capabilities and the critical tasks associated with them are shared across eight *coordinating activities* and aligned across departments and agencies by existing coordination mechanisms. Coordination for Protection occurs through existing department and agency mechanisms and through the range of coordinating structures within the Protection mission.

National Security Council (NSC)

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

Federal Departments and Agencies

Policy coordination, guidance, dispute resolution, and periodic in-progress reviews for the functions and programs described and assigned are provided through the interagency process established in Presidential Policy Directive/PPD-1: Organization of the NSC System of February 13, 2009, or any successor.

Under the Protection Framework, various Federal departments or agencies assume roles based on their authorities, the specific *coordinating activities*, and the nature of the threat, hazard, or risk. As needed, the Secretary of Homeland Security will convene a meeting or meetings, as appropriate, among Federal department and agency representatives to discuss and consider the coordination of Federal Protection *coordinating activities*, focusing on the following:

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

In addition to the Secretary of Homeland Security’s responsibilities as described in Homeland Security Presidential Directive (HSPD)-5, the Secretary of Homeland Security is responsible for coordinating the domestic all-hazards preparedness efforts of all executive departments and agencies, in consultation with State, local, tribal, and territorial governments, NGOs, private-sector partners, and the general public. Further, the heads of all Federal departments and agencies with a role in Protection are responsible for national preparedness efforts consistent with their statutory roles and responsibilities.

Federal Leadership Coordination

Protection Federal leadership coordination consists of senior leaders designated by Federal departments and agencies collectively coordinating the diverse Protection efforts implemented across the Nation. They are responsible for monitoring and assessing the effectiveness of Protection core capabilities and working to improve the efficiency and effectiveness of Federal interagency

coordination practices and operations regarding how the Nation manages risk through Protection core capabilities.

Senior leaders regularly identify and assess gaps in Protection mission capabilities and capacities. These assessments should be coordinated with the DHS Joint Requirements Council and the component-led Integrated Product Teams (IPT) managed by the DHS Science and Technology Directorate (S&T), which identifies capability gaps and coordinates and prioritizes DHS research and development efforts to address the identified gaps.

In order to ensure that scientific efforts are both relevant to and incorporated into National Preparedness efforts under the Protection mission area, coordination is necessary across the National preparedness and scientific communities. A well-coordinated research-to-operations pipeline between the senior leaders coordinating the diverse protection efforts and the National Science and Technology Council Subcommittee on Disaster Reduction (SDR) will ensure that operational needs are prioritized in scientific research and technology development and can advance operational capabilities.

Advancing the principles and objectives of the National Protection Framework and this Protection FIOP requires interagency information exchange, sharing best practices and updates on programs and policies that directly affect the National Protection Framework, and setting the strategic national direction and integrated priorities relative to implementation of the National Protection Framework. This is accomplished through a range of standing and existing Federal interagency coordination groups and bodies.

Department of Homeland Security (DHS) Processes

Several Protection *coordinating activities* are principally coordinated by DHS components. Internal DHS processes for coordinating Protection mission responsibilities rely on unity of effort within the Department. The DHS approach to unity of effort includes the management of senior leadership councils, advisory boards, and forums for information sharing and coordination. These function in concert with DHS operations centers and operational components to conduct and coordinate steady state and escalated Protection mission requirements.

Steady state coordination includes bodies such as the Counter Terrorism Advisory Board (CTAB), which brings together the intelligence, operational, cyber, and policy-making elements from across DHS to facilitate a cohesive and coordinated operational response, so that DHS can deter and disrupt terrorist operations. Chaired by the DHS Coordinator for Counterterrorism, the DHS CTAB is an intradepartmental body with representatives from DHS component senior leadership and offices that carry out counterterrorism-related operational, information sharing, and policy related activities. The purpose of the CTAB is to enable effective and consistent department-wide coordination and collaboration to address terrorist threats/incidents impacting the homeland security enterprise. The CTAB coordinates and facilitates DHS's actions for preventing current terrorist acts and for addressing emerging, perceived, or possible terrorist threats. It provides timely and accurate advice and recommendations to the Secretary on counterterrorism issues.

The National Operations Center (NOC) is the principal operations center for DHS and provides situational awareness in the event of a natural disaster, act of terrorism, or other disaster. For the Protection mission, which addresses both steady state risks and enhanced Protection during periods of heightened risk, the NOC serves as the principal situational awareness center for DHS. The NOC consists of five elements: the NOC Watch; National Response Coordination Center (NRCC); National Infrastructure Coordinating Center (NICC); Intelligence Watch; and a planning element. The Secretary of Homeland Security is the principal Federal official for domestic incident

management, per HSPD-5. In executing this responsibility, the Secretary must remain aware of Protection mission risks as they emerge and the actions taken by the Nation related to those risks. The NOC provides this service to the Secretary.

Coordinating Structures

The existing plans, concepts of operation, and established means of coordination across the eight Protection *coordinating activities* provide the network of shared situational awareness, joint objective setting, and operational alignment for the Protection mission. Table 4 below provides an overview of the coordination structures described in Annex C of this FIOP. Each coordinating activity operates through existing coordination structures to deliver Protection core capabilities. Some coordination structures are shared across multiple *coordinating activities*. The coordination structures listed below serve as points of connection for coordinating Protection mission objectives and as initiating mechanisms for enhanced Protection measures in response to elevated or emerging risks.

Table 4: Protection Coordinating Activities and Coordinating Structures

Coordinating Activity	Coordination Structures (<i>italics indicates shared coordination structures</i>)
Border Security	<ul style="list-style-type: none"> ▪ <i>U.S. Customs and Border Protection (CBP) Immigration Advisory Program (IAP)⁹</i> ▪ <i>U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) Export Enforcement Coordination Center (E2C2)¹⁰</i> ▪ <i>ICE Enforcement and Removal Operations (ERO) Law Enforcement Support Center (LESC)¹¹</i> ▪ <i>Federal Law Enforcement Training Centers (FLETC)¹²</i> ▪ <i>Border Intelligence Fusion Section (BIFS)¹³</i> ▪ <i>Alliance to Combat Transnational Threats (ACTTs)¹⁴</i> ▪ <i>Global Maritime Operational Threat Response Coordination Center (GMCC)¹⁵</i> ▪ <i>DHS Joint Task Force (JTF) (East, West, Investigations)¹⁶</i> ▪ <i>DHS NOC¹⁷</i> ▪ National Targeting Center–Passenger (NTC-P) ▪ Foreign Terrorist Tracking Task Force (FTTTF) ▪ <i>ICE HSI Border Enforcement Security Taskforces (BEST)¹⁸</i> ▪ <i>DHS IPTs¹⁹</i>

⁹ Also a coordination structure for Immigration Security.

¹⁰ Also a coordination structure for Immigration Security.

¹¹ Also a coordination structure for Immigration Security.

¹² Also a coordination structure for Critical Infrastructure Security and Resilience, Immigration Security, Maritime Security, and Transportation Security.

¹³ Also a coordination structure for Immigration Security.

¹⁴ Also a coordination structure for Immigration Security.

¹⁵ Also a coordination structure for Immigration Security and Maritime Security.

¹⁶ Also a coordination structure for Immigration Security, Maritime Security, and Transportation Security.

¹⁷ Also a coordination structure for all activities.

¹⁸ Also a coordination structure for Maritime Security.

¹⁹ Also a coordination structure for Immigration Security, Maritime Security, and Transportation Security.

Coordinating Activity	Coordination Structures (<i>italics indicates shared coordination structures</i>)
Critical Infrastructure Security and Resilience	<ul style="list-style-type: none"> ▪ Sector-Specific Agency (SSA) structure ▪ NICC ▪ <i>DHS NOC</i> ▪ National Cybersecurity and Communications Integration Center (NCCIC) ▪ Government Coordinating Council (GCC) ▪ Sector Coordinating Councils (SCC) ▪ Critical Infrastructure Cross-Sector Council ▪ Federal Senior Leadership Council (FSLC) ▪ Critical Infrastructure Partnership Advisory Council (CIPAC) ▪ State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) ▪ Information Sharing Advisory Councils ▪ Regional Consortia ▪ The Homeland Security Information Network—Critical Infrastructure (HSIN-CI) ▪ <i>FLETC</i>
Defense Against WMD Threats	<ul style="list-style-type: none"> ▪ Integrated Consortium of Laboratory Networks (ICLN) ▪ Laboratory Response Network for Biological Threats (LRN-B) ▪ Laboratory Response Network for Chemical Threats (LRN-C) ▪ WMD Strategic Group (WMDSG) ▪ Countering Nuclear Threats Interagency Policy Committee (IPC) ▪ <i>ICE HSI Export Enforcement Coordination Center</i> ▪ Global Nuclear Detection Architecture (GNDA) sub-IPC ▪ GNDA Interagency Working Group (IWG) ▪ Domestic Nuclear Detection Office (DNDO) Joint Analysis Center ▪ Federal Bureau of Investigation (FBI) Strategic Information Operations Center (SIOC) ▪ <i>DHS NOC</i> ▪ Department of Defense (DOD) National Military Command Center (NMCC) ▪ National Counterterrorism Center (NCTC) ▪ CBP Laboratories and Scientific Services Directorate Teleforensic Center (LSSD-TC) ▪ State Fusion Centers ▪ The Nuclear Defense Research and Development (NDRD) Working Group, convened by the White House Office of Science and Technology Policy (OSTP), facilitates the coordination of planning and information exchange for U.S. Government (USG) technical radiological and nuclear (R/N) detection research and development activities ▪ Combatting Terrorism Technical Support Office (CTTSO) Technical Support Working Group (TSWG) ▪ National Infrastructure Protection Plan sector coordination (see critical infrastructure security and resilience coordination structures) ▪ BioWatch ▪ National Biosurveillance Integration Center (NBIC)
Health Security	<ul style="list-style-type: none"> ▪ Public Health Emergency Medical Countermeasures Enterprise (PHEMCE) ▪ Health and Human Services (HHS) Secretary's Operations Center (SOC) ▪ <i>DHS NOC</i>

Coordinating Activity	Coordination Structures (<i>italics indicates shared coordination structures</i>)
Immigration Security	<ul style="list-style-type: none"> ▪ <i>ICE HSI E2C2</i> ▪ <i>CBP IAP</i> ▪ <i>DHS NOC</i> ▪ <i>ICE ERO LESC</i> ▪ <i>FLETC</i> ▪ <i>BIFS</i> ▪ <i>ACTTs</i> ▪ <i>GMCC</i> ▪ <i>DHS JTFs (East, West, Investigations)</i> ▪ <i>DHS IPTs</i>
Maritime Security	<ul style="list-style-type: none"> ▪ National Maritime Intelligence Center ▪ Interagency Operation Centers (IOC) at 35 large ports ▪ <i>DHS NOC</i> ▪ <i>GMCC</i> ▪ National Maritime Security Advisory Committee (NMSAC) ▪ Maritime Government Coordinating Council (MGCC) ▪ CBP/U.S. Coast Guard (USCG) Joint Protocols for the Expeditious Recovery of Trade ▪ Area Maritime Security Plans (AMSP) ▪ Maritime Transportation Security Waterways Management Services ▪ U.S. Maritime Administration (MARAD) ▪ Port Security Grant Program (PSGP) ▪ USCG HOMEPORT ▪ <i>ICE HSI E2C2</i> ▪ <i>HSI BEST</i> ▪ <i>DHS JTFs (East, West, Investigations)</i> ▪ HSIN-CI ▪ <i>DHS IPTs</i> ▪ <i>FLETC</i>
Protection of Key Leadership And Special Events	<ul style="list-style-type: none"> ▪ Department and Agency Operations Centers ▪ National Special Events Data Call ▪ <i>DHS NOC</i> ▪ DHS Special Events Program ▪ FBI Special Events Program ▪ Special Events Working Group (SEWG) ▪ Integrated Federal Support Overview (IFSO) ▪ Federal Coordinator Program
Transportation Security	<ul style="list-style-type: none"> ▪ National Infrastructure Protection Plan sector coordination (see critical infrastructure security and resilience coordination structures) ▪ <i>DHS NOC</i> ▪ <i>ICE</i> ▪ <i>DHS JTFs (East, West, Investigations)</i> ▪ <i>DHS IPTs</i> ▪ <i>FLETC</i>

Aligning Protection Coordinating Activities

Alignment of the eight separate *coordinating activities* takes place through the above existing structures which serve as forums for both existing and emergent Protection issues. These coordinating structures help align department and agency coordination and action and may also serve to enhance coordination across multiple existing structures.

Activation for Enhanced Protection

When needed and appropriate, in response to increased risk or the requirement for heightened activity around Protection mission issues, the Secretary of Homeland Security may notify departments and agencies of the need to support the escalated decision process outlined in this framework. Alternately, leadership within departments and agencies may notify the Secretary of Homeland Security of such a need. DHS and other departments and agencies coordinate decision making during periods of escalated deployment of protection capabilities. This process will elevate unresolved policy, program, and operational issues to the NSC and make recommendations on Federal interagency protection policies and practices during routine and escalated periods.

Coordinating structures across the eight Protection *coordinating activities* serve as nodes in the network of Federal Protection, and through their ongoing function, identify and escalate protection issues that require enhanced activity or increased coordination across the Protection mission.

Integration of Federal Capabilities with Other Partners

The U.S. Government (USG) uses a variety of coordination mechanisms to ensure the Nation is protected from all threats and all hazards. Because the Protection mission area is ongoing and does not stop, coordination mechanisms must exist in a constant and flexible posture.

To this end, the Federal Government supports, participates in, and hosts a variety of local, state, tribal, territorial, and regionally focused cross-capability forums to combine and coordinate resources, authorities, and mission to achieve the Protection mission. One example of these forums includes the U.S. Secret Service (USSS) Electronic Crimes Task Forces. DHS also staffs Protective Security Advisors in the field who assist in information sharing and preparedness activities across a variety of partners. These local, state, tribal, territorial, and regional forums and imbedded personnel share information between state and national bodies to ensure that protection capabilities at all levels of government are operating to achieve common goals and objectives.

Coordination and Support

Coordinating activities are mutually supportive. Protection *coordinating activities* are the mechanism for delivering Protection core capabilities, and as such they provide and rely on support across each activity area. Coordinating activity appendices in Annex C provide greater detail on mutual support across *coordinating activities*. Each appendix within Annex C follows a similar outline, providing a common framework for mutual support across activities that deliver Protection core capabilities.

Table 5: Annex C, Appendix Structure

Appendix Section	Description
Purpose	Summarizes the content and intended use of the appendix
Scope	Describes the audience
Objectives	Describes what the appendix accomplishes
Concept of Operations	Provides an overview of the way that the coordinating activity is managed across the Federal Government including key roles and responsibilities
Coordination Structures	Describes the structures used to deliver Protection core capabilities within this activity
Support to Other Coordinating Activities	Summarizes the support this activity provides to other activities
Support from Other Coordinating Activities	Summarizes the support this activity receives from other activities
Support to Other Mission Areas	Summarizes the support this activity provides to other mission areas outside Protection
Key Plans	Identifies key plans that organize the conduct of this activity
Key Authorities and References	Identifies key authorities that govern the conduct of this activity

A critical component of how the Protection mission area works to meet the National Preparedness Goal is how each of the *coordinating activities* provide both interoperability and well-practiced, coordinated, and integrated Protection support.

The National Protection Framework focuses on core capabilities that contribute to protecting the Nation domestically, but it does not address the protection of U.S. interests overseas. While the National Protection Framework focuses on domestic activities, Protection capabilities often are interconnected globally. While many agencies have understandings and agreements with foreign governments concerning mutual Protection efforts, the U.S. Department of State (DOS) is responsible for the overall conduct of U.S. foreign relations and engagement. As such, Protection efforts with international partners require coordination with DOS. DOS will assist agencies pursuing their Protection policy and operational requirements and will ensure that USG collaboration with foreign partners is coordinated and congruent with U.S. foreign policy priorities.

Oversight, Plan Development, and Maintenance

The authorities that guide the structure, development, and implementation of the Protection FIOP are statutes, EOs, regulations, and Presidential directives. Congress has provided the broad statutory authority necessary for this FIOP, and the President has issued EOs and Presidential directives to supply direction to Federal departments and agencies.

Federal departments and agencies with Protection responsibilities, in close coordination with the Secretary of Homeland Security, are the executive agents for the Protection FIOP management and maintenance.

To maintain the National Preparedness System, each executive department and agency develops and maintains deliberate department-level operational plans where needed, to deliver Protection core capabilities to fulfill the organization's responsibilities described in the FIOPs. Department- and agency-level operations plans will describe how the organization's capabilities support the application of Protection core capabilities within the respective agency's authorities and funding limitations. Existing plans, SOPs, or guides may be used for the development of these plans. The department- and agency-level plans should contain the level of detail necessary to clearly identify the department or agency's specific critical tasks, responsibilities, and resources required to fulfill mission area tasks as appropriate under the FIOP. The frequency for reviewing and updating these plans will depend on each department or agency's internal business practices.

Suggested plan elements include:

- Description of department or agency's vision for Protection
- Description of authorities, responsibilities, and ability to implement Protection core capabilities
- Summaries of overall trends visible within Protection
- Identification of Protection core capabilities that show the highest degree of progress
- Identification of Protection core capabilities that show the most significant gaps/needs for improvement
- Interagency coordination
- Identification of resources to support activities
- Submission date and update schedule consistent with department or agency business practices
- Evaluation and consideration of methods to integrate Protection strategies across department or agency programs to ensure and supplement the civil rights of individuals with disabilities, from religious, racially, and culturally diverse backgrounds, and with limited English proficiency.

In addition, the department- and agency-level operational plans could be used to:

- Help promote understanding of Protection to department or agency mission and operations to increase efficiency of national-level operations and identify possible changes to regulations, guidance, or policy to further the implementation of the Protection core capabilities
- Serve as a means to conduct a self-assessment of department or agency activities that have a Protection connection and/or have Protection effects
- Serve as an internal department document and inform plan development
- Develop an action plan with milestones to be consistent with department or agency business practices

- Serve as a source of information for sharing lessons learned.

Federal roles and responsibilities to improve the Nation's resilience should focus, where possible, not only on using and expanding existing strategic planning documents, interagency implementation activities and coordinating structures, but also on supporting the guidance set forth in this FIOP and in departmental operating plans.

This FIOP will be regularly reviewed to evaluate consistency with both new and existing policies; evolving threats and hazards; and experience gained from use. Interagency partners will be engaged in the review and maintenance process for this FIOP. The first review of this FIOP will be completed no more than 18 months after its release, and subsequent reviews will be conducted on a quadrennial basis. The review and maintenance process may include developing incident-specific and classified annexes, which include the delivery schedule for federally coordinated assets and resources, as appropriate. The FIOP will be updated periodically, as required, to incorporate new executive guidance and statutory and procedural changes, as well as lessons learned from exercises and actual Protection operations. Significant updates to the Protection FIOP will be vetted through a Federal senior-level interagency review process.

This page intentionally left blank.

Annex A: Alignment

Integration with Existing Plans, Strategies, and Doctrine

Existing plans, strategies, and doctrinal publications provide the foundation for the Protection FIOP. These documents set the conditions to enable the Federal Government to deliver Protection core capabilities for each of the eight *coordinating activities*.

The Protection FIOP does not supersede or direct planning conducted under applicable legal authorities, but serves as the National Preparedness System construct and concept of operations for aligning and coordinating across existing Protection plans and efforts.

Relationship with National Preparedness Planning Frameworks and FIOPs

The National Preparedness Goal is designed to prepare our Nation for the risks that will severely tax our collective capabilities and resources. Each of the five mission areas serves as an aid in organizing national preparedness activities and does not constrain or limit integration across mission areas and core capabilities. Mission area coordination (command, control, and communication) is conducted through established organizational protocols with other mission areas. These mission areas exist along a continuum, and there is a dynamic interplay between and among them and even some commonality in the core capabilities essential to each.

The National Protection Framework describes the way that the whole community safeguards against natural, technological, and adversarial hazards. The principles described in the National Protection Framework serve as the basis for the Protection FIOP and provide a national approach to the Protection mission.

Protection capabilities are often called upon to support Response and Recovery activities. During these situations, Protection integrates within the mission and operational structures of Response and Recovery. This FIOP provides an overview of the way that Protection connects to other mission areas, with special attention to the Prevention mission, which shares some core capabilities and *coordinating activities* with Protection.

The Prevention and Protection mission areas are closely linked, in that Protection actions may uncover an imminent (suspected or actual) terrorist threat during the conduct of their steady state Protection missions, such as screening, search, and detection operations at borders and ports of entry (POE), at special events, etc. When detected, such threats may require urgent action to resolve the immediate situation, such as reporting, detention, or arrest activities. In such cases, upon resolution of the immediate situation, the information and investigation must be seamlessly transitioned to the Prevention mission so the threat can be fully investigated in order to identify additional plots, accomplices, or other attacks. (Table 6, below, provides a summary of the mission area alignment).

This page intentionally left blank.

Table 6: Relationship of the Protection Mission Area with the Other Mission Areas

	Prevention	Mitigation	Response	Recovery
Definition	The capabilities necessary to avoid, prevent, or stop a threatened or actual act of terrorism. For the purposes of the prevention framework, the term “prevention” refers to preventing imminent threats.	The capabilities necessary to reduce loss of life and property by lessening the impact of disasters.	The capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred.	The capabilities necessary to assist communities affected by an incident to recover effectively.
Alignment	<p>The Prevention mission area focuses on those intelligence, technical, and law enforcement actions, which prevent an adversary from carrying out an attack within the United States when the threat is imminent in order to thwart an initial or follow-on terrorist attack. Protection activities, on the other hand, focus on measures that detect, deter, and/or disrupt terrorist surveillance, planning, and/or execution activities or deter and disrupt other threats and hazards and, like mitigation, focus on minimizing the consequences of significant incidents. In some cases, the same capabilities that are used for Protection functions are also used in Prevention operations.</p> <p>Prevention and Protection operate simultaneously and provide for integration when needed. For example, during a period of imminent terrorist threat, Prevention activities may focus on information sharing, law enforcement operations, and other activities to prevent, deter, and preempt terrorism. Protection may assess the increased risks and coordinate information sharing and other actions needed to enhance specific protective measures.</p>	<p>The Mitigation and Protection mission areas work together to ensure the Nation is resilient. Activities in the Mitigation and Protection missions typically are performed in a steady state or well before an event. Protection places particular emphasis on security and deterring threats, while Mitigation emphasizes achieving resilience by reducing vulnerabilities. Both seek to minimize consequences and include critical infrastructure security and resilience. Risk analysis is necessary to effectively design successful strategies for Mitigation and Protection. Integration of risk information, planning activities, and coordinating structures reduces duplication of effort and streamlines risk management actions in both mission areas.</p>	<p>The Response and Protection mission areas will occur concurrently. Protection does not cease during Response. Protection capabilities deployed to support Response efforts conform to and integrate into Response organizational structures, including the Incident Command System (ICS) and the Emergency Support Function structures.</p> <p>Analytic products developed in support of Protection activities during steady state conditions are also designed to support Response planning efforts and provide the basis for operational planning during incident response.</p> <p>Assessments of infrastructure impacts and prioritization efforts during Response also rely on the structures and relationships developed within the Protection mission.</p>	<p>The Recovery and Protection mission areas will occur concurrently. Protection does not cease 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.</p> <p>Establishing Recovery priorities and ensuring that resilience and risk management are central to the Recovery effort requires the Protection mission to structure its activities in a way that supports Recovery efforts.</p>

This page intentionally left blank.

Annex B: Protection Core Capability Planning

This annex describes the Federal Government’s approach to building, supporting, and delivering Protection mission core capabilities. The National Preparedness Goal describes core capabilities as “distinct critical elements necessary to achieve the National Preparedness Goal.” Protection core capabilities are the distinct critical elements that undergird Protection mission activities. Within Federal Protection efforts, the core capabilities serve as both the means of organizing preparedness planning efforts and a construct for measuring mission readiness.

These national capabilities serve the function of providing a common structure and lexicon to Protection planning and are meant to inform Protection planning efforts. Building on this common structure, protection plans achieve greater alignment and better facilitate the coordination described in this FIOP during periods of escalated Protection activity.

Protection mission *coordinating activities* deliver Protection core capabilities. However, the objectives, tactics, and tasks for many operational plans within the *coordinating activities* are not organized by Protection core capabilities. For example, Sector Specific plans (SSP) produced within the NIPP 2013 structure are organized according to PPD-21, while Protection of Key Leadership and Special Events planning is organized by activity-specific functions and capabilities at a level of greater detail than the Protection core capabilities. The Protection core capabilities serve the vital function of providing a common approach to assessing preparedness capacity at the strategic level, but do not form a compulsory structure for operational planning.

Protection Critical Tasks by Core Capability

The National Protection Framework identifies critical tasks for each Protection mission core capability. This FIOP expounds on those critical tasks by summarizing the structure under which the Federal Government performs them.

Most critical tasks for Protection are delivered across, and are common to, all *coordinating activities*. This reinforces the overall concept of operations for Protection, which stresses that Protection activities are decentralized and conducted under existing laws, appropriations, regulations, and coordinating structures. These *coordinating activities* are the mechanism for delivering Protection capabilities and the structure for executing critical Protection tasks.

Some tasks are unique to a single coordinating activity while others are shared between only a few *coordinating activities*.

Protection critical tasks do not encompass the full range of operations that take place in a given coordinating activity—for example Maritime Security operations include a range of requirements outside of the Protection mission, as well as outside the National Preparedness System. The Protection critical tasks provide the common list of critical actions which must occur across the full spectrum of Protection in order to achieve the National Preparedness goal.

The shared nature of Protection critical tasks highlights the key areas where *coordinating activities* work together and develop shared situational awareness and joint priorities to deliver Protection core capabilities.

The responsibility for performing Protection critical tasks is distributed across *coordinating activities*, demonstrating the general principle of Protection task execution: that it is distributed and shared across multiple *coordinating activities* rather than being assigned to single activities.

The critical tasks for the Protection mission do not describe the entirety of each coordinating activity, but they provide a common—and largely shared—set of Protection mission tasks. Each coordinating activity executes these tasks according to their concepts of operation, coordinating and aligning mission activity according to the Concept of Operations in the base plan portion of this FIOP.

The three core capabilities common to all National Preparedness mission areas are Planning, Operational Coordination, and Public Information and Warning. These capabilities are also shared across all Protection activities. Appendix 1 describes the delivery of these core capabilities within the Protection mission area. Core capabilities unique to the Protection mission area are described in further detail in Appendices 2–9.

Appendix 1 to Annex B: Common Core Capabilities (Planning, Public Information and Warning, and Operational Coordination)

Planning

Protection mission planning accounts for the way that *coordinating activities* (see Annex C) support one another and for how the Protection mission supports other mission areas.

Planning is a systematic process that engages the whole community, as appropriate, in the development of executable strategic, operational, tactical, and community-based approaches to meet defined Protection objectives. Planning includes the development exercise and maintenance of multidisciplinary plans that provide joint guidance across Protection mission activities.

Critical Tasks:

- Initiate a flexible planning process that builds on existing plans as part of the National Planning System;
- Establish partnerships that facilitate coordinated information sharing between partners to support the protection of critical infrastructure within single and across multiple jurisdictions and sectors;
- Identify and prioritize critical infrastructure and determine risk management priorities;
- Conduct vulnerability assessments, perform risk analyses, identify capability gaps, and coordinate protective measures on an ongoing basis in conjunction with the private sector and local, state, tribal, territorial, and Federal organizations and agencies;
- Establish joint Protection objectives within and across mission area activities;
- Implement security, protection, resilience, and continuity plans and programs, train and exercise, and take corrective actions;
- Integrate Protection planning for the whole community;
- Leverage existing community partnerships to bolster and enhance resiliency efforts;
- Develop and document continuity plans and their supporting procedures so that, when implemented, the plans and procedures provide for the continued performance of essential functions under all circumstances; and
- Ensure that Protection planning mutually supports other mission area plans, especially with analytic and risk management products and complementary concepts of operation.

Delivery of Federal Planning to the Protection Mission:

- Provide a flexible Federal planning process that builds on existing plans and facilitates the development of additional plans to Protection stakeholders.
- Sustain existing and establish new information sharing mechanisms among Protection stakeholders to enable planning/protection of critical infrastructures within jurisdictions.
- Support the training of planners from local, state, tribal, and territorial authorities, the Federal Government, the private sector, and nonprofits or NGOs using approved Federal planning processes and current best practices. Incorporate new best practices discovered during training, exercises, and operations into the training programs.
- Provide standard Federal metrics to facilitate the identification/prioritization of critical infrastructure and determination of risk.

- Integrate Federal grants to support funding of Protection planning efforts as appropriate.
- Provide a national vulnerability assessment capability to support 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.
- Develop and disseminate a series of Federal Protection resilience and continuity plans and programs to address specific Protection requirements.
- Develop, coordinate, and execute Protection-related exercises on a recurring annual basis; integrate lessons learned into plans, policies, and procedures as appropriate.
- Leverage research and development resources to develop technology to enhance Protection capabilities and/or fill Protection capability gaps/shortfalls
- Identify and assess gaps in Protection core capabilities and Protection critical tasks. For capability gaps that require research and development, engage the DHS research and development community (S&T, DNDO, USCG Research and Development Center) to develop technology to fill or mitigate the gaps. The DHS research and development community will engage with other local, state, Federal, international, private industry, and academia sources to identify solutions.

In summary, Federal departments and agencies will identify their ability to assess the threat, identify authorities for key decision points, deploy and employ assets and capabilities, and identify requirements and request support to protect people, critical assets, systems, and networks against the greatest risks to the Nation. Planning activities will also identify assumptions to inform decision making. If necessary, departments and agencies will adjust their operational plans based on direction from the President of the United States. Prior to such direction, departments and agencies will execute their roles and responsibilities pursuant to law, national policy, national plans, and their respective agency plans. Lessons learned will be integrated into training, plans, policies, and procedures as appropriate.

Public Information and Warning

Delivering coordinated, prompt, reliable, and actionable information to stakeholders 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.²⁰

The Federal role in 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

²⁰ The President of the United States has directed the Secretary of Homeland Security and the Attorney General to coordinate with each other to execute key responsibilities that provide public information and warning to the Nation regarding terrorist threats and attacks. Where there is an imminent terrorist threat or a suspected act of terrorism, consult Presidential Decision Directives to identify necessary coordination mechanisms.

²¹ Public information and warning systems must provide effective communication to individuals with disabilities, such as through audio and video captioning for multimedia, sign language interpreters for public media events, and

Critical Tasks:

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

Delivery of Public Information and Warning to the Protection Mission:

- Establish mechanisms and provide the full spectrum of support necessary for appropriate and ongoing information sharing among all levels of government, the private sector, NGOs, and the public.
- Integrate appropriate coordination mechanisms (such as the Integrated Public Alert and Warning System, NTAS, and social media sites and technology).
- Establish coordination mechanisms that facilitate the rapid exchange of information sharing among stakeholders during steady state, escalated decision making and response environments.

Operational Coordination

Operational coordination is establishing and maintaining unified and coordinated operational structures and processes that appropriately integrate all critical stakeholders and support the execution of core capabilities.

Critical Tasks:

- The concept of operations contained in this FIOP provides the Federal model for executing critical operational coordination tasks, encompassing coordination across decentralized Federal partners operating under applicable legal authorities. Annex C of this FIOP provides a more detailed overview of Protection activities.

Delivery of Operational Coordination to the Protection Mission:

- Within the Protection mission, operational coordination is achieved according to the concept of operations outlined in the base plan of this document.

use-accessible Web sites. Information and warning should also be communicated using various languages and culturally diverse media outlets.

This page intentionally left blank.

Appendix 2 to Annex B: Access Control and Identity Verification

Access control and identity verification include the application of 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.²²This capability relies on the implementation and maintenance of protocols to verify identity and authorize, grant, or deny physical and cyber access to specific locations, information, and networks.

Critical Tasks:

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

Delivery of Access Control and Identity Verification Capability to the Protection Mission:

The responsibility for performing Protection critical tasks is distributed across *coordinating activities*, demonstrating the general principle of Protection task execution—that it is distributed and shared across multiple *coordinating activities* rather than being assigned to single activities. Table 7 provides a summary of how Protection *coordinating activities* are responsible for executing critical tasks for Access Control and Identity Verification.

Table 7: Access Control and Identity Verification Critical Tasks by Coordinating Activity

Critical Tasks	Border Security	Critical Infrastructure Security and Resilience	Defense Against of WMD Threats	Health Security	Immigration Security	Maritime Security	Protection of Key Leadership and Special Events	Transportation Security
Verify identity to authorize, grant, or deny physical and cyber access to physical and cyber assets, networks, applications, and systems that could be exploited to do harm	•	•	•	•	•	•	•	•
Control and limit access to critical locations and systems to authorized individuals carrying out legitimate activities	•	•	•	•	•	•	•	•

²² For suspected or actual terrorist incidents, the FBI On-Scene Commander has primary responsibility to conduct, direct, and oversee crime scenes, their security, and evidence management through all phases of the response, including access control and identity verification.

This page intentionally left blank.

Appendix 3 to Annex B: Intelligence and Information Sharing

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

Intelligence sharing is providing timely, accurate, and actionable information resulting from intelligence processes concerning threats to the United States, its people, property, or interests; the development, proliferation, or use of WMD; or any other matter bearing on U.S. national or homeland security by local, state, tribal, territorial, Federal, and other stakeholders.²³

Information sharing is the capability to exchange intelligence and other information; data; or knowledge among local, state, tribal, territorial, Federal, or private sector entities, or international partners as appropriate. For example, terrorist threat-related information collected domestically is shared through Federal Bureau of Investigation (FBI) joint terrorism task forces (JTTF), fusion centers, etc.

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

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

Critical Tasks:

- Monitor, detect, and analyze threats and hazards to public safety, health, and security, which include:
 - Participate in public, local, state, tribal, territorial, and national education and awareness programs; and
 - Participate in the routine exchange of security information—including threat assessments, alerts, attack indications and warnings, and advisories—among partners;
- Determine requirements for protection stakeholder intelligence, information, and information sharing;

²³ Intelligence cycle processes include the following steps: planning; direction; the collection, exploitation, processing, and analysis of available information; production; dissemination; evaluation; and feedback.

- Develop or identify and provide access to mechanisms and procedures for intelligence and information sharing between the public, private sector, faith-based, and government protection partners;²⁴
- Use intelligence processes to produce and deliver relevant, timely, accessible, and actionable intelligence and information products to others as applicable, to include partners in the other mission areas;
- Adhere to appropriate mechanisms for safeguarding sensitive and classified information and protecting privacy, civil rights, and civil liberties;
- Establish and update local, state, tribal, territorial, regional, and national education awareness programs to facilitate information/intelligence sharing among all Protection stakeholders;
- Conduct recurring training and exercises of intelligence/information sharing at multiple levels and echelons and integrate lessons learned as appropriate;
- Establish and implement routine exchange of security information—including threat assessments, alerts, attack indications and warnings, and advisories—among Protection stakeholders at all levels and echelons;
- Produce and disseminate relevant, timely, accessible, and actionable intelligence and information products to others as applicable (including “tear lines” to facilitate information sharing);
- Educate stakeholders on safeguarding and sharing sensitive and classified information; and
- The Federal Government will monitor, gather, and analyze intelligence and information in order to protect people, critical assets, systems, and networks against the greatest risks to the Nation.

Delivery of Intelligence and Information Sharing to the Protection Mission:

The responsibility for performing Protection critical tasks is distributed across *coordinating activities*, demonstrating the general principle of Protection task execution—that it is distributed and shared across multiple *coordinating activities* rather than being assigned to single activities. Table 8 provides a summary of how Protection *coordinating activities* are responsible for executing critical tasks for Intelligence and Information Sharing.

²⁴ Information sharing must provide effective communication to individuals with disabilities and others with access and functional needs, including those who are deaf, hard of hearing, blind, or have low vision, through the use of appropriate auxiliary aids and services, such as sign language and other interpreters, captioning of audio and video materials and user-accessible Web sites. Information sharing also should include communication in various languages and use of culturally diverse media outlets.

Table 8: Intelligence and Information Sharing Critical Tasks by Coordinating Activity

Critical Tasks	Border Security	Critical Infrastructure Security and Resilience	Defense Against of WMD Threats	Health Security	Immigration Security	Maritime Security	Protection of Key Leadership and Special Events	Transportation Security
	Monitor, detect, and analyze threats and hazards to public safety, health, and security	•	•	•	•	•	•	•
Participate in public, local, state, tribal, territorial, and national education and awareness programs	•	•	•	•	•	•	•	•
Participate in the routine exchange of security information—including threat assessments, alerts, attack indications and warnings, and advisories—among partners	•	•	•	•	•	•	•	•
Determine requirements for Protection stakeholder intelligence, information, and information sharing	•	•	•	•	•	•	•	•
Develop or identify and provide access to mechanisms and procedures for intelligence and information sharing between the public, private sector, faith-based, and government protection partners	•	•	•	•	•	•	•	•
Use intelligence processes to produce and deliver relevant, timely, accessible, and actionable intelligence and information products to others as applicable, to include partners in the other mission areas	•	•	•	•	•	•	•	•
Adhere to appropriate mechanisms for safeguarding sensitive and classified information and protecting privacy, civil rights, and civil liberties	•	•	•	•	•	•	•	•
Establish and update local, state, tribal, territorial, regional, and national education awareness programs to facilitate information/intelligence sharing among all Protection stakeholders	•	•	•	•	•	•	•	•
Conduct recurring training and exercises of intelligence/information sharing at multiple levels and echelons and integrate lessons learned as appropriate	•	•	•	•	•	•	•	•
Establish and implement routine exchange of security information—including threat assessments, alerts, attack indications and warnings, and advisories—among Protection stakeholders at all levels and echelons	•	•	•	•	•	•	•	•
Produce and disseminate relevant, timely, accessible, and actionable intelligence and information products to others as applicable (including “tear lines” to facilitate information sharing)	•	•	•	•	•	•	•	•
Educate stakeholders on safeguarding and sharing sensitive and classified information	•	•	•	•	•	•	•	•
The Federal Government will monitor, gather, and analyze intelligence and information in order to protect people, critical assets, systems, and networks against the greatest risks to the Nation	•	•	•	•	•	•	•	•

This page intentionally left blank.

Appendix 4 to Annex B: Interdiction and Disruption

Interdiction and disruption activities include delaying, diverting, intercepting, halting, apprehending, or securing threats and/or hazards.

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

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

In the context of Protection this capability 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 POEs into the United States. It might also include urgent activities required when an imminent threat is encountered unexpectedly through the course of day-to-day Protection activities. In such cases, upon resolution of the immediate situation, the information and investigation must be seamlessly transitioned to the Prevention mission so the threat can be fully investigated in order to identify additional plots, accomplices, or other attacks.

Critical Tasks:

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

Delivery of Interdiction and Disruption Capability to the Protection Mission:

The responsibility for performing Protection critical tasks is distributed across *coordinating activities*, demonstrating the general principle of Protection task execution—that it is distributed and shared across multiple *coordinating activities* rather than being assigned to single activities. Table 9 provides a summary of how Protection *coordinating activities* are responsible for executing critical tasks for Interdiction and Disruption.

Table 9: Interdiction and Disruption Critical Tasks by Coordinating Activity

Critical Tasks	Border Security	Critical Infrastructure Security and Resilience	Defense Against of WMD Threats	Health Security	Immigration Security	Maritime Security	Protection of Key Leadership and Special Events	Transportation Security
Deter movement and operation of terrorists into or within the United States and its territories	•				•	•		•
Ensure the capacity to detect CBRNE devices or resolve CBRNE threats	•	•	•	•	•	•	•	•
Interdict conveyances, cargo, and persons associated with a potential threat or act	•		•		•	•	•	•
Implement public health measures to mitigate the spread of disease threats abroad and prevent disease threats from crossing national borders	•	•		•		•		
Disrupt terrorist financing or conduct counter-acquisition activities to prevent weapons, precursors, related technology, or other material support from reaching its target	•		•	•	•	•		•
Enhance the visible presence of law enforcement to deter or disrupt threats from reaching potential target(s)	•	•	•		•	•	•	•
Intervene to protect against the spread of violent extremism within U.S. communities	•	•			•			•
Employ wide-area search and detection assets in targeted areas in concert with local, state, tribal, or territorial personnel or other Federal agencies (depending on the threat)	•	•	•	•	•	•	•	•

Appendix 5 to Annex B: Screening, Search, and Detection

Screening, search, and detection activities include 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.

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

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

Consistent with the DHS Strategic Plan, screening and vetting operations integrate critical enterprise and partner data sources, such as biometric identity screening, validation, and verification data consolidated and shared through the Department's Office of Biometric Identity Management (OBIM). OBIM consolidates, stores, matches, and shares biometric data collected by DHS components that include *coordinating activities* in this plan, and cross-references the data with Department of Defense (DOD) and Department of Justice (DOJ) systems. These DHS Enterprise Identity and Screening Services provide real-time human biometric verification capabilities and other biometric expertise and services, including:

- Establishing or verifying identity through DHS biometric systems located at OBIM, supplemented with fingerprint analysis conducted by fingerprint examiners;
- Enhancing biometric identification and intelligence vetting of persons of interest through associated biographic information and data integrity analysis; and
- Supporting law enforcement and intelligence operational activities to improve the accuracy and usefulness of identities maintained by the office.

Critical Tasks:

- Identify potential threats resulting from persons or networks;
- Screen persons, baggage, mail, cargo, and conveyances using technical, nontechnical, intrusive, and nonintrusive means without unduly hampering the flow of legitimate commerce; consider additional measures for high-risk persons, conveyances, or items;
 - Conduct CBRNE search and detection operations;
 - Conduct passive and active detection of CBRNE agents;
 - Operate safely in a hazardous environment;
 - Consider the deployment of Federal teams and capabilities to enhance local, state, tribal, and territorial efforts, including the use of incident assessment and awareness assets;
- Conduct biosurveillance of data relating to human health, animal, plant, food, water, and environmental domains;
- Use systematic examinations and assessments, sensor technologies, public health disease surveillance, laboratory testing, or physical investigation and intelligence, to include poison control centers, electronic death certificate reporting, point of care diagnostics or clinical care,

and other venues for detection of a potential outbreak condition that may or may not be reported through standard public health disease surveillance;

- Establish integrated local, regional, and national mechanisms to develop and engage an observant Nation (individuals, families, communities, and local, state, tribal, and territorial government and private sector partners);
- Integrate active screening of persons, baggage, mail, cargo, and conveyances using technical, nontechnical, intrusive, and nonintrusive means;
- Establish training /periodic exercising of all surveillance and search procedures, and integrate lessons learned as appropriate;
- Consider deployment of Federal teams and capabilities to enhance capabilities to enhance local, state, tribal, and territorial efforts, including use of incident assessment and awareness assets;
- Establish mechanisms to enhance nationwide CBRNE surveillance of health threats and hazards; and
- Integrate Federal grant programs to support programs and initiatives.

Delivery of Screening, Search, and Detection to the Protection Mission:

The responsibility for performing Protection critical tasks is distributed across *coordinating activities*, demonstrating the general principle of Protection task execution—that it is distributed and shared across multiple *coordinating activities* rather than being assigned to single activities. Table 10 provides a summary of how Protection *coordinating activities* are responsible for executing critical tasks for Screening, Search, and Detection.

Table 10: Screening, Search, and Detection Critical Tasks by Coordinating Activity

Critical Tasks	Border Security	Critical Infrastructure Security and Resilience	Defense Against of WMD Threats	Health Security	Immigration Security	Maritime Security	Protection of Key Leadership and Special Events	Transportation Security
	Identify potential threats resulting from persons or networks	•	•	•		•	•	
Screen persons, baggage, mail, cargo, and conveyances using technical, nontechnical, intrusive, and nonintrusive means without unduly hampering the flow of legitimate commerce; consider additional measures for high-risk persons, conveyances, or items	•	•	•	•	•	•	•	•
Conduct CBRNE search and detection operations	•	•	•	•		•		•
Conduct passive and active detection of CBRNE agents	•	•	•	•		•		•

Critical Tasks	Border Security	Critical Infrastructure Security and Resilience	Defense Against of WMD Threats	Health Security	Immigration Security	Maritime Security	Protection of Key Leadership and Special Events	Transportation Security
	Operate safely in a hazardous environment	•	•	•	•	•	•	•
Conduct biosurveillance of data relating to human health, animal, plant, food, water, and environmental domains	•	•	•	•	•	•		
Use systematic examinations and assessments, sensor technologies, public health disease surveillance, laboratory testing, or physical investigation and intelligence	•	•	•	•	•	•		•
Establish integrated national, regional, and local mechanisms to develop and engage an observant Nation (individuals, families, communities, and local, state, tribal, and territorial government and private sector partners)	•	•	•	•	•	•	•	•
Establish training /periodic exercising of all surveillance and search procedures, and integrate lessons learned as appropriate	•	•	•	•	•	•	•	•
Establish mechanisms to enhance nationwide CBRNE surveillance of health threats and hazards	•	•	•	•	•	•		•
Integrate Federal grant programs to support programs and initiatives	•	•	•	•	•	•	•	•
Apply active and passive surveillance and search procedures to identify, discover, or locate threats or hazards	•	•	•	•	•	•	•	•

This page intentionally left blank.

Appendix 6 to Annex B: Physical Protective Measures

Physical protective measures include implementing and maintaining risk-informed countermeasures and policies protecting people, borders, structures, materials, products, and systems associated with key operational activities and critical infrastructure sectors. The Federal workforce is a critical asset requiring protection considerations.

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

Critical Tasks:

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

Delivery of Physical Protective Measures to the Protection Mission:

The responsibility for performing Protection critical tasks is distributed across *coordinating activities*, demonstrating the general principle of Protection task execution—that it is distributed and shared across multiple *coordinating activities* rather than being assigned to single activities. Table 11 provides a summary of how Protection *coordinating activities* are responsible for executing critical tasks for Physical Protective Measures.

Table 11: Physical Protective Measures Critical Tasks by Coordinating Activity

Critical Tasks	Border Security	Critical Infrastructure Security and Resilience	Defense Against of WMD Threats	Health Security	Immigration Security	Maritime Security	Protection of Key Leadership and Special Events	Transportation Security
Identify and prioritize assets, systems, networks, and functions that need to be protected		•				•	•	•
Identify necessary physical protections, countermeasures, and policies through a risk assessment of key operational activities and infrastructure	•	•	•	•	•	•	•	•
Protect critical lifeline functions, which include energy, communications, transportation, and water and wastewater management		•				•		
Develop and implement security plans, including business continuity plans, that address identified security risks	•	•	•	•	•	•	•	•
Develop and implement risk-based physical security measures, countermeasures, policies, and procedures	•	•	•	•	•	•	•	•
Implement security training for workers, focused on awareness and response	•	•	•	•	•	•	•	•
Develop and implement biosecurity and biosafety programs and practices, similar to the Maritime Operations Threat Response (MOTR) process that was utilized for the 2015 Ebola Virus outbreak		•	•	•		•		
Leverage Federal acquisition programs, as appropriate, to ensure maximum cost efficiency, security, and interoperability of procurements	•	•	•	•	•	•	•	•

Appendix 7 to Annex B: Risk Management for Protection Programs and Activities

Risk management for Protection programs and activities includes identifying, assessing, and prioritizing risks to inform Protection activities and investments.

Risk management is accomplished by implementing and maintaining risk assessment processes to identify and prioritize assets, systems, networks, and functions, as well as implementing and maintaining appropriate tools to identify and assess threats, vulnerabilities, and consequences.

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

Critical Tasks:

- Gather required data in a timely and accurate manner to effectively identify risks;
- Develop and use appropriate tools to identify and assess threats, vulnerabilities, and consequences;
- Build the capability within communities to analyze and assess risk and resilience;
- Identify, implement, and monitor risk management plans;
- Update risk assessments to reassess risk based on changes in the following areas: the physical environment, aging infrastructure, new development, new mitigation projects and initiatives, post-event verification/validation, new technologies or improved methodologies, and better or more up-to-date data;
- Validate, calibrate, and enhance risk assessments by relying on experience, lessons learned, and knowledge beyond raw data or models;
- Use risk assessments to design exercises and determine the feasibility of mitigation projects and initiatives; and
- Develop a unified approach to making investments in secure and resilient infrastructure to enable communities to withstand the effects of a disaster, respond effectively, recover quickly, adapt to changing conditions, and manage future disaster risk.

Delivery of Risk Management for Protection Programs and Activities to the Protection Mission:

The responsibility for performing Protection critical tasks is distributed across *coordinating activities*, demonstrating the general principle of Protection task execution—that it is distributed and shared across multiple *coordinating activities* rather than being assigned to single activities. Table 12 provides a summary of how Protection *coordinating activities* are responsible for executing critical tasks for Risk Management for Protection Programs and Activities.

Table 12: Risk Management for Protection Programs and Activities Critical Tasks by Coordinating Activity

Critical Tasks	Border Security	Critical Infrastructure Security and Resilience	Defense Against of WMD Threats	Health Security	Immigration Security	Maritime Security	Protection of Key Leadership and Special Events	Transportation Security
	Gather required data in a timely and accurate manner to effectively identify risks	•	•	•	•	•	•	•
Develop and use appropriate tools to identify and assess threats, vulnerabilities, and consequences	•	•	•	•	•	•	•	•
Build the capability within communities to analyze and assess risk and resilience	•	•	•	•	•	•	•	•
Identify, implement, and monitor risk management plans	•	•	•	•	•	•	•	•
Update risk assessments to reassess risk based on changes in the following areas: the physical environment, aging infrastructure, new development, new mitigation projects and initiatives, post-event verification/validation, new technologies or improved methodologies, and better or more up-to-date data	•	•	•	•	•	•	•	•
Validate, calibrate, and enhance risk assessments by relying on experience, lessons learned, and knowledge beyond raw data or models	•	•	•	•	•	•	•	•
Use risk assessments to design exercises and determine the feasibility of mitigation projects and initiatives	•	•	•	•	•	•	•	•
Develop a unified approach to making investments in secure and resilient infrastructure to enable communities to withstand the effects of a disaster, respond effectively, recover quickly, adapt to changing conditions, and manage future disaster risk		•						

Appendix 8 to Annex B: Cybersecurity

Cybersecurity includes protecting against damage to, unauthorized use of, and/or malicious exploitation of (and, if needed, the restoration of) information and communications technologies (and the data contained therein).

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

Critical Tasks:

- Implement countermeasures, technologies, and policies to protect physical and cyber assets, networks, applications, and systems that could be exploited to do harm;
- Secure, to the extent possible, public and private networks and critical infrastructure (e.g., communication, financial, power grid, water, and transportation systems), based on results from risk assessment, mitigation, and incident response capabilities;
- Formalize partnerships with governmental and private sector cyber incident or emergency response teams to accept, triage, and collaboratively respond to incidents in an efficient manner;
- Formalize partnerships between communities and disciplines responsible for cybersecurity and physical systems dependent on cybersecurity;
- Formalize relationships between information communications technology and information system vendors and their customers for ongoing product cybersecurity, business planning, and transition to Response and Recovery when necessary;
- Share actionable cyber threat information with the domestic and international, government, and private sectors to promote shared situational awareness²⁵;
- Implement risk-informed standards to ensure the security, reliability, integrity, and availability of critical information, records, and communications systems and services through collaborative cybersecurity initiatives and efforts;
- Detect and analyze malicious activity and support mitigation activities;
- Collaborate with partners to develop plans and processes to facilitate coordinated incident response activities;
- Leverage law enforcement and intelligence assets to identify, track, investigate, disrupt, and prosecute malicious actors threatening the security of the Nation's public and private information systems; and
- Create resilient cyber systems that allow for the uninterrupted continuation of essential functions.

Delivery of Cybersecurity to the Protection Mission:

The responsibility for performing Protection critical tasks is distributed across *coordinating activities*, demonstrating the general principle of Protection task execution—that it is distributed and shared across multiple *coordinating activities* rather than being assigned to single activities. Table 13

²⁵ This includes ensuring the protection of sensitive information.

provides a summary of how Protection *coordinating activities* are responsible for executing critical tasks for Cybersecurity.

Table 13: Cybersecurity Critical Tasks by Coordinating Activity

Critical Tasks	Border Security	Critical Infrastructure Security and Resilience	Defense Against of WMD Threats	Health Security	Immigration Security	Maritime Security	Protection of Key Leadership and Special Events	Transportation Security
Implement countermeasures, technologies, and policies to protect physical and cyber assets, networks, applications, and systems that could be exploited to do harm	•	•	•	•	•	•	•	•
Secure, to the extent possible, public and private networks and critical infrastructure (e.g., communication, financial, power grid, water, and transportation systems), based on results from risk assessment, mitigation, and incident response capabilities		•				•		•
Formalize partnerships with governmental and private sector cyber incident or emergency response teams to accept, triage, and collaboratively respond to incidents in an efficient manner		•				•		•
Formalize partnerships between communities and disciplines responsible for cybersecurity and physical systems dependent on cybersecurity		•				•		•
Formalize relationships between information communications technology and information system vendors and their customers for ongoing product cybersecurity, business planning, and transition to response and recovery when necessary		•				•		•
Share actionable cyber threat information with the domestic and international, government, and private sectors to promote shared situational awareness ²⁶		•				•		•
Implement risk-informed standards to ensure the security, reliability, integrity, and availability of critical information, records, and communications systems and services through collaborative cybersecurity initiatives and efforts		•				•		•
Detect and analyze malicious activity and support mitigation activities		•				•		•
Collaborate with partners to develop plans and processes to facilitate coordinated incident response activities		•				•		•
Leverage law enforcement and intelligence assets to identify, track, investigate, disrupt, and prosecute malicious actors threatening the security of the Nation's public and private information systems		•				•		•

²⁶ This includes ensuring the protection of sensitive information.

Critical Tasks	Border Security	Critical Infrastructure Security and Resilience	Defense Against of WMD Threats	Health Security	Immigration Security	Maritime Security	Protection of Key Leadership and Special Events	Transportation Security
Create resilient cyber systems that allow for the uninterrupted continuation of essential functions		<ul style="list-style-type: none"> • 						

This page intentionally left blank.

Appendix 9 to Annex B: Supply Chain Integrity and Security

Supply chain integrity and security Protection activities include strengthening the security and resilience of the supply chain.

This capability relies on securing and making resilient key nodes, methods of transport between nodes, and materials in transit between a supplier and consumer.

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

Critical Tasks:

- Integrate security processes into supply chain operations to identify items of concern and resolve them as early in the process as possible;
- Analyze key dependencies and interdependencies related to supply chain operations;²⁷
- Use risk management principles to identify threat, vulnerability, and consequence and protect key assets, infrastructure, and support systems;
- Implement physical protections, countermeasures, and policies to secure and make resilient key nodes, methods of transport between nodes, and materials in transit;
- Use verification and detection capabilities to identify goods that are not what they are represented to be, are contaminated, are not declared, or are prohibited; and to prevent cargo from being compromised or misdirected as it moves through the system; and
- Use layers of defense to protect against a diverse range of traditional and asymmetric threats.

Delivery of Supply Chain Integrity and Security to the Protection Mission:

The responsibility for performing Protection critical tasks is distributed across *coordinating activities*, demonstrating the general principle of Protection task execution—that it is distributed and shared across multiple *coordinating activities* rather than being assigned to single activities. Table 14 provides a summary of how Protection *coordinating activities* are responsible for executing critical tasks for Supply Chain Integrity and Security.

²⁷ Dependency is a one-directional reliance on input, interaction, or another source in order to function properly. Interdependency is a mutually reliant relationship between objects, individuals, or groups. The degree of interdependency does not need to be equal in both directions.

Table 14: Supply Chain Integrity and Security Critical Tasks by Coordinating Activity

Critical Tasks	Border Security	Critical Infrastructure Security and Resilience	Defense Against of WMD Threats	Health Security	Immigration Security	Maritime Security	Protection of Key Leadership and Special Events	Transportation Security
Integrate security processes into supply chain operations to identify items of concern and resolve them as early in the process as possible	•	•				•		•
Analyze key dependencies and interdependencies related to supply chain operations ²⁸	•	•				•		•
Use risk management principles to identify threat, vulnerability, and consequence and protect key assets, infrastructure, and support systems		•	•			•		
Implement physical protections, countermeasures, and policies to secure and make resilient key nodes, methods of transport between nodes, and materials in transit	•	•	•			•		•
Use verification and detection capabilities to identify goods that are not what they are represented to be, are contaminated, are not declared, or are prohibited; and to prevent cargo from being compromised or misdirected as it moves through the system	•	•	•		•	•		•
Use layers of defense to protect against a diverse range of traditional and asymmetric threats	•	•	•	•	•	•	•	•

²⁸ Dependency is a one-directional reliance on input, interaction, or another source in order to function properly. Interdependency is a mutually reliant relationship between objects, individuals, or groups. The degree of interdependency does not need to be equal in both directions

Annex C: Coordinating Activities

This annex provides a summary of the concept, plans, arrangements and key authorities that coordinate Protection mission activity across eight major areas. As described in the base plan, the Protection *coordinating activities* addressed in this FIOP are not an exhaustive or exclusive list. As Protection concerns emerge, the mission adapts and evolves to address them. The eight *coordinating activities* described in this FIOP are existing means of coordinating Protection activity within distinct and established domains of operation:

- **Border Security:** Securing U.S. air, land, and sea ports and borders against the illegal flow of people and goods, while facilitating the flow of lawful travel and commerce.
- **Critical Infrastructure Security and Resilience:** Protecting the physical and cyber elements of critical infrastructure. This includes actions to deter the threat, reduce vulnerabilities, or minimize the consequences associated with a terrorist attack, natural disaster, or manmade disaster. Critical infrastructure security and resilience is detailed in NIPP 2013.²⁹
- **Defense Against WMD Threats:** Safeguarding the Nation from threats associated with WMD and related materials and technologies including their malicious acquisition, movement, and use within the United States.
- **Health Security:** Securing the Nation and its people to be prepared for, protected from, and resilient in the face of incidents with health consequences.
- **Immigration Security:** Securing the Nation from illegal immigration through effective and efficient immigration systems and processes that respect human and civil rights.
- **Maritime Security:** Securing U.S. maritime infrastructure, resources, and the MTS from terrorism and other threats and hazards and securing the homeland from an attack from the sea, while preserving civil rights, respecting privacy and protected civil liberties, and enabling legitimate travelers and goods to move efficiently without fear of harm or significant disruption.
- **Protection of Key Leadership and Special Events:** Safeguarding government executive leadership from hostile acts by terrorists and other malicious actors and to ensure security at events of national significance.
- **Transportation Security:** Securing U.S. transportation systems and the air domain against terrorism and other threats and hazards while preserving civil rights, respecting privacy and protected civil liberties, and enabling legitimate travelers and goods to move without fear of harm or significant disruption.

Protection *coordinating activities* are mutually supportive. When *coordinating activities* work together to conduct Protection operations, the core capability structure of the National Protection Framework provides a structure for developing joint objectives and shared situational awareness.

²⁹ For a definition of critical infrastructure, see footnote 7.

This page intentionally left blank.

Appendix 1 to Annex C: Border Security

Purpose

Border Security supports the Protection mission by interdicting terrorist threats, immigration violators, drug traffickers, and other threats to national security, economic security, and public safety. The Federal Government will deliver, synchronize, and integrate protection core capabilities to enforce the laws of the United States, facilitate economic security through lawful international trade and travel, and secure the Nation's border. Border Security is accomplished through U.S. Customs and Border Protection (CBP) and U.S. Immigration and Customs Enforcement (ICE), in strong partnership with other DHS and interagency members, including U.S. Citizenship and Immigration Services (USCIS), the U.S. Coast Guard (USCG), the Transportation Security Administration (TSA), the Department of Agriculture (USDA), and the Environmental Protection Agency (EPA).

Critical functions of Border Security include:

- Facilitating the entry of legitimate travel and trade into and out of the U.S.;
- Heightening awareness and increasing vigilance in the targeting of high-risk travelers planning to enter or depart the U.S. (via land, air, and sea) through robust screening programs both at home and abroad;
- Detaining and removing priority aliens;
- Establishing multilayered protocols to identify high-risk shipments arriving at U.S. POEs (land, air and sea), pre-investigation facilities, and Container Security Initiative (CSI) locations worldwide, to:
 - Protect the commerce and agriculture of the U.S.; and
 - Prevent the export of weapons, munitions and technology that adversaries could divert from allies for use against the United States.

Adversarial networks impact the current Border Security environment, which change not only the Border Protection mission but the Border Security response. To provide for Border Security, CBP and ICE must collaborate with other local, state, Federal, and foreign stakeholders to identify multilayer threats created by adversarial networks. These efforts include identifying adversaries' strengths and vulnerabilities, both tangible and intangible, as they relate to enforcement strategies in support of the Homeland Security Mission. This collaboration creates a Border Security enforcement operation that is an integrated shield of protection for both the border and the homeland. Protection in this context means the proactive, offensive, and defensive deployment of friendly network resources to disrupt, dismantle, and destroy adversarial networks.

Scope

This appendix focuses only on the Federal *coordinating activities* for Border Security. It specifically includes the Federal coordinating structures and mechanisms required to deliver the Protection core capabilities and achieve Border Security objectives. While Border Security efforts overlap with Immigration Security, Maritime Security, and Transportation Security efforts, those *coordinating activities* are distinct and are addressed in separate Protection FIOP appendices.

Objectives

This appendix will accomplish the following:

- Provide a concept of operations for integrating existing Federal capabilities to secure the Nation’s borders;
- Describe Federal operational coordination mechanisms that integrate resources and personnel for Border Security; and
- Lay the foundation for further department or agency Border Security planning, including integration among *coordinating activities*.

Concept of Operations

The Federal Government protects the Nation’s borders by maintaining air, land, and sea border security measures while ensuring the continued safe and lawful flow of travel and commerce. Achieving this objective requires a focus on three interrelated goals, including the following:

1. **Sustaining effective control of the physical and approaches to the United States.** This includes preventing illegal entry of inadmissible persons and/or contraband and the illegal exit of dangerous goods, proceeds of crime, and malicious actors without disrupting the free flow of commerce and travel.
2. **Identifying and disrupting threats before they reach the United States.** This requires close coordination with international partners and the private sector to prevent exploitation of interconnected trading, transportation, and transactional systems that move people and commerce. These activities must also avoid damaging or degrading the free flow of commerce and travel.
3. **Disrupting and dismantling transnational criminal and terrorist organizations that smuggle or traffic people, illicit goods, or the proceeds of crime across the U.S. border.** Disrupting and dismantling these organizations is essential to secure the Nation’s border.

Several key elements to Border Security are employing border inspection, patrol, the efficient removal of aliens apprehended illegally entering the United States, investigative activities, immigration enforcement, and developing friendly networks. These combined efforts allow friendly networks to combat adversary networks by deploying personnel and assets into any geographic region where adversary networks operate—land or maritime; urban, rural, or remote. Border inspection, patrol, and investigative operations may 1) target specific or general smuggling activities; 2) prevent or deter smuggling activities; or 3) move or shape smuggling activities into conditions where law enforcement agencies have the advantage.

The modern operating environment demands that Border Security agencies work with stakeholders across the borders and homeland and within the friendly network to assess risks, benefits and impacts of operations and to design friendly network solutions to defeat adversary networks, accomplish the border security mission and balance the public’s interests at large. The Border Patrol may serve as the lead (or supported) organization in counter network operations, but it will also frequently serve as a supporting organization through its enforcement mechanisms to other agencies. To facilitate friendly networks, CBP and ICE will partner with:

- Other components within DHS (e.g., USCIS and USCG);
- Other Federal Government departments such as the Department of Defense (DOD) and the Department of Justice (DOJ);
- Local, state, and tribal governments or law enforcement;
- NGOs; and

- Other public and private communities of interest.

POE environments and partners differ from location to location; however, each POE is required to coordinate emergency procedures with other CBP component offices and external government agencies as needed. Continuity of Operations and Business Continuity Management Plans guide port management through this process.

Roles and Responsibilities

Border Security requires a unity of effort throughout the Federal Government. Several departments and agencies play a critical role in securing U.S. air, land, and sea ports and borders against the illegal flow of people and goods, while facilitating the flow of lawful travel and commerce. These departments and agencies include:

- CBP
- ICE
- USCG
- USCIS
- DOD
- DOS
- DOJ
- FBI
- Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)
- Department of the Interior (DOI)
- FLETC
- U.S. Marshals Service
- TSA
- USDA
- EPA.

Each of these Federal partners supports the delivery of the Protection core capabilities required for Border Security. The table below describes how the Federal Government delivers each Protection core capability in the Border Security mission space.

Table 15: Border Security Core Capabilities Critical Task Summary

Core Capability	Border Security Critical Task Summary
Access Control and Identity Verification	<ul style="list-style-type: none"> ▪ Control and limit access to critical locations and systems. ▪ Support verification efforts to authorize, grant, or deny physical and cyber access to key assets.
Intelligence and Information Sharing	<ul style="list-style-type: none"> ▪ Set requirements for intelligence and information sharing across all sectors. ▪ Monitor, detect, and analyze threats to public safety, health and security and provide sufficient safeguards to prevent their entry into the U.S. ▪ Gather and analyze information to identify potential threats and determine appropriate strategies to address those threats before they can enter the U.S.

Core Capability	Border Security Critical Task Summary
Interdiction and Disruption	<ul style="list-style-type: none"> ▪ Deter movement of terrorists into the U.S. and disrupt financing and logistical support from reaching potential threats in the U.S. ▪ Coordinate efforts with local, state, tribal, and territorial partners to detect threats and prevent them from reaching their targets. ▪ Ensure Border Security stakeholders have the ability to detect CBRNE devices and resolve CBRNE threats. ▪ Focus on smart and effective immigration enforcement, which prioritizes the removal of convicted criminal aliens, threats to national security, recent border crossers, illegal re-entrants, those who have significantly abused the visa or visa waiver program, and immigration fugitives, utilizing the latest technology through coordination with science and technology on all fronts.
Screening, Search, and Detection	<ul style="list-style-type: none"> ▪ Provide active screening and surveillance of people, baggage, mail, cargo, and conveyances to detect and identify any potentially threatening materials or persons prior to their entry into the U.S. ▪ Provide CBRNE screening of persons, baggage, mail, cargo, and conveyances to prevent their entry into the U.S. ▪ Support intelligence and information sharing to help stakeholders identify potential threats and capability gaps.
Physical Protective Measures	<ul style="list-style-type: none"> ▪ Develop and implement physical security measures to support border security efforts and enhance border security stakeholders' abilities to safeguard against potential threats to border security personnel and assets. ▪ Use risk assessments to identify physical protective measures that support improved protection of key activities and assets.
Risk Management for Protection Programs and Activities	<ul style="list-style-type: none"> ▪ Develop and use appropriate tools to identify and assess threats, vulnerabilities, and consequences that could impact border security efforts. ▪ Develop and implement risk assessments to look at physical environment, infrastructure, new technologies, and improved methodologies to determine appropriate risk mitigation measures that can increase Border Security stakeholders' ability to protect against threats being introduced into the U.S.
Cybersecurity	<ul style="list-style-type: none"> ▪ Implement countermeasures, technologies, and policies to protect physical and cyber assets, networks, applications, and systems that support Border Security efforts. ▪ Safeguard against the introduction of people or materials that could impact the physical security of cyber assets into the U.S.
Supply Chain Integrity and Security	<ul style="list-style-type: none"> ▪ Analyze Border Security assets and networks to identify key dependencies and risks, and implement physical and cyber protection measures to secure and make resilient the key nodes, transportation hubs and modes, and materials needed for border security operations. ▪ Develop multilayer defense and planning efforts to safeguard necessary supplies for border security operations against asymmetrical and traditional threats. ▪ Use verification and detection capabilities to identify goods that are misrepresented or contaminated and prevent their entry into the U.S. or the U.S. supply chain. ▪ Prevent cargo and supplies from being misdirected or compromised as they move into or out of the U.S.

Ports and infrastructure sectors have developed and implemented locality based “Border Security Protocols,” which are coordinated with local authorities. Field office and sector levels collaborate on and review these protocols to further coordinate and integrate civil/law support from local, state, tribal, and Federal civil and law enforcement authorities. Additionally, and throughout all levels of national border security, there are established local, state, tribal, and Federal law enforcement task forces, including Border Enforcement Security Task Force(s) (BEST) and JTTFs. Other security mechanisms for border protection include:

- Facilities—POEs and checkpoints
- Checkpoint personnel with support command/control structures
- Migrant Processing Facilities (MPF)
- Inspections and Boarding of vessels
- Technological measures:
 - Detection and surveillance assets (unmanned aerial surveillance, cameras, sensors, biometrics)
 - Nonintrusive inspection (NII) (large-scale inspection systems [LSIS])
 - Portable identifier systems (Transportation Worker Identification Credential [TWIC] card)
 - License plate readers
- Air, land, and maritime craft/equipment with support command/control structures. Each year, Federal Law Enforcement Training Centers (FLETC) train approximately 65,000 law enforcement officers (LEO) who are responsible for performing a broad range of missions, including U.S. border, maritime, transportation security, and critical infrastructure security and resilience/security, from more than 95 agencies including:
 - CBP
 - ICE
 - USCG
 - ATF
 - U.S. Marshals Service.
- Organizational Risk analysts and supervisors; DHS Regional Coordination Mechanisms (ReCOMs), GMCC, multi-agency coordination centers (MACC), DHS PLCY, and DOJ; training for insider threats.
- Risk analysis tools; information sharing networks, DHS/National Protection and Programs Directorate (NPPD) Office of Cyber and Infrastructure Analysis (OCIA); deployed Federal officers, Threat and Hazard Identification and Risk Assessment (THIRA), JTTFs, Maritime Security Risk Analysis Model (MSRAM); NTAS; National Targeting Center (NTC); FBI investigative and analytical personnel.
- Many other Federal agencies such as the Food and Drug Administration (FDA).

Coordination Structures

- CBP Immigration Advisory Program (IAP)
- ICE HSI E2C2
- ICE Law Enforcement Support Center (LESC)
- FLETC
- Border Intelligence Fusion Section (BIFS)
- Alliance to Combat Transnational Threats (ACTTs)

- GMCC
- NTCP
- DHS IPTs
 - Senior leaders regularly identify and assess gaps in Protection mission capabilities and capacities. These assessments should be coordinated with the component-led IPTs managed by the DHS Science and Technology Directorate (S&T), which identifies capability gaps and coordinates and prioritizes DHS research and development efforts to address the identified gaps.
- DHS Regional Coordination Mechanisms (ReCoM)
- DHS Joint Task Force (JTF) (East, West, Investigations)
 - The Secretary of Homeland Security established three pilot JTFs to coordinate the Southern Border and Approaches (SBA) Campaign. The JTFs coordinate, on behalf of the Secretary, operational priorities to synchronize capabilities in order to achieve SBA Campaign objectives and lead coordinating efforts for their respective JTF. In addition, JTFs coordinate integrated joint investigations and operations within their joint operating areas or functions, supported by DHS Operational Components, to enhance DHS unity of effort in securing the SBA. Finally, JTFs enhance Departmental flexibility by coordinating multi-DHS Component “joint” capability as needed within the SBA area of operations.
- National Targeting Center–Passenger (NTC-P)
 - Coordinates with CBP field-level activities related to antiterrorism efforts and plays a vital role in identifying individuals who pose a national security concern at 327 U.S. POEs and over 30 Border Patrol checkpoints throughout the U.S.
 - Is the CBP focal point for all possible Terrorist Screening Database (TSDB) encounters with CBP field entities.
 - Is the primary contact between CBP field offices and other government agency case agents on all positive TSDB encounters.
 - Uses several automated enforcement data processing systems that detect and prevent terrorist access to the United States, including the Automated Targeting System–Passenger (ATS-P) and the Intelligence Operations Framework System, which allow NTCP to screen passenger manifests and related information prior to a passenger’s arrival in the United States, respond to terrorism related alerts, and provide time-sensitive research and support on any issues related to international passengers and travel at and between U.S. POEs.
- NTC-Cargo unit (NTC-C)
 - Targets high-risk cargo shipments that may pose a threat to the internal security of the United States. Its primary function is similar to NTC-P in support of CBP’s mission. The unit partners internationally with customs units in other countries around the world as well as
 - In order to maintain a nimble ability to address emerging and imminent threats, CBP subject matter experts develop targeting rules based on actionable intelligence derived from current Intelligence Community (IC) reporting or other law enforcement information available to CBP.
- HSI Border Enforcement Security Task Forces

- HSI has stood up 37 BESTs throughout the nation, composed of many local, state, and Federal agencies, including CBP, Drug Enforcement Administration (DEA), USCG, ATF, and many others. BEST teams are led by HSI special agents and address a myriad of border, maritime, and transportation security issues, including contraband smuggling, safety violations to aircraft and marine vessels, and security and access to restricted areas at airports/seaports.
- In coordination with CBP, ICE also conducts background and licensing investigations to determine eligibility for Customs Brokers, as well as all facilities considered functional equivalents of the border (FEBs), including Customs Bonded Warehouses, Foreign Trade Zones, and Container Freight stations.

Support to Other Coordinating Activities

The Border Security coordinating activity provides support to the other *coordinating activities* in a variety of ways:

- It supports **Critical Infrastructure Security and Resilience** by providing sector-specific information and analysis, as infrastructure systems can span geographic and political boundaries. This excludes terrorist threats, drug traffickers, and other threats to national security, economic security, and public safety.
- It supports **Defense Against WMD Threats** by providing shared intelligence and information, as Border Security operations support detection and interdiction efforts. Border security inspections are routinely conducted to detect or locate and report on radiological and nuclear (R/N) materials and devices.
 - ICE HSI special agents are assigned to JTTFs in support of the FBI's mission to prevent and protect against terrorist acts.
 - Both CBP and ICE have robust WMD programs relating to the interdiction of illegal import/export of either the precursors of or actual WMD and therefore have a significant role in this area.
 - HSI manages and operates the Export Enforcement Coordination Center (E2C2), established by EO 13558, which strengthens the enforcement of U.S. export laws through the facilitation of partner agency communication and collaboration to keep our Nation safe.
 - These counter proliferation efforts are executed by detecting, preventing, disrupting, investigating, and prosecuting violations of U.S. export control laws.
- It supports **Health Security** by maintaining awareness of health security priorities, information, and intelligence to support border-based screening and detection of health security threats.
 - It provides support during humanitarian crises, for example, by assessing health, safety, and security of at-risk populations, such as unaccompanied children along the southwest U.S. border.
- It supports **Immigration Security** efforts by aligning intelligence to drive border security and immigration security practices for both border and internal immigration security.
- It supports **Maritime Security** efforts by aligning protective efforts at POEs, coordinating operations, and sharing intelligence. The USCG also conducts a diverse set of protective activities designed to reduce human trafficking and contraband smuggling.

- These include waterborne, air, and shore patrols and security boarding of suspect vessels.
- This layered, risk-based approach is designed to detect, deter, and disrupt human trafficking.
- It supports the **Protection of Key Leadership and Special Events** by sharing intelligence and information related to the identification of individuals who may travel across our borders who may pose a threat to our leadership or disrupt special events.
 - Additionally, the work of ICE HSI, as a secondary agency in DHS for this responsibility, provides protection to Special Event Assessment Ratings (SEAR) 1 and SEAR 2 events and regularly assists the USSS as its primary backup for National Special Security Events (NSSE).
- It supports **Transportation Security** efforts by providing operational coordination and shared intelligence, especially where transportation systems and POEs operate jointly.

Support from Other Coordinating Activities

The Border Security coordinating activity receives support from the other *coordinating activities* in a variety of ways:

- It gets support from **Critical Infrastructure Security and Resilience** through the use of critical infrastructure systems and assets, including POEs and transportation infrastructure.
- It gets support from **Defense Against WMD Threats** through intelligence and information sharing.
- It gets support from **Health Security** through health security activities that provide information and intelligence to support border-based screening and detection of health security threats.
 - Border security activities can play a key role in supporting quarantine, tracking, and monitoring efforts to reduce potential public health risks.
 - This includes sharing key information on potential hazards and threats, indicators, and symptoms to watch for.
 - Border security teams share information on potential health-security threats they encounter or track.
- It gets support from **Immigration Security** through ICE HSI, which is the investigative arm of ICE.
 - ICE HSI conducts border related investigations for a myriad of offenses involving illicit trade, travel, and finance crossing our international borders and the enforcement of certain Federal laws for DHS and on behalf of other government agencies.
 - This mission includes narcotics, alien smuggling and human trafficking, contraband smuggling, endangered species smuggling, and bulk cash smuggling.
- It gets support from **Maritime Security** through the USCG, which performs drug interdiction, migrant interdiction, and Ports, Waterways, and Coastal Security (PWCS) activities to provide a layered approach that supports border security and immigration security.
 - Maritime security initiatives (e.g., PWCS and CSI) reduce threats to border security.
 - Maritime security operations work in concert with border security operations to share intelligence and information and conduct joint security initiatives.

- It gets support from **Protection of Key Leadership and Special Events** through intelligence and information sharing.
- It gets support from **Transportation Security** through coordination and support activities, including a wide range of resource sharing efforts, support for advanced research, and the development of new detection and security measures that can help protect key transportation systems and assets.
 - Border security systems provide support by helping protect against the introduction of threats and hazards into transportation systems, including screening for terrorists, criminals, hazardous materials (HAZMAT), and illicit materials.
 - These measures include new biometric screening tools, joint operations to monitor for threats in all sectors, particularly aviation and maritime transportation measures, and improved support for quickly and reliably screening cargo at the border or in foreign countries before it enters into U.S. transportation networks.
 - Integrated teams of border and transportation security personnel can quickly identify risks and corrective measures.
 - Support activities also include safeguarding transportation systems and personnel through improved information sharing and awareness.
 - Border security assets share information about particular threats or hazards to help develop corrective measures.
 - Information sharing can take place in formal environments that work to perform awareness operations and monitoring, such as the Air and Marine Operations (AMO) Center.

Support to Other Mission Areas

Response and recovery are integrated into the DHS, CBP and ICE Continuity of Operations Plan (COOP) for each POE. An important function of the COOP is to identify, plan, and prepare for the restoration of agency Mission Essential Functions (MEF) during and after a crisis event in order to support the Department's Primary Mission Essential Functions and Mission Essential functions in support of National Essential Functions. CBP and ICE have extensively developed and exercised "Business Resumption Plans," which ensure the continuity of national border security while facilitating and strengthening international trade and travel.

Key Plans

The DHS SBA Campaign Plan provides an actionable operational approach to address the enduring challenges DHS faces in those areas. It also establishes a pilot program, consisting of three Department joint task forces conducting integrated joint investigations and operations within their joint operating areas or functions and supported by DHS Operational Components, to enhance DHS unity of effort in securing the southern border and approaches.

The DHS SBA Land Migration Contingency Plan ensures DHS has a comprehensive and synchronized approach to prevent and respond to an attempted land migration surge affecting the United States southwest border.

The DHS SBA Maritime Migration Contingency Plan ensures DHS and its partners have a comprehensive and synchronized approach to prevent, deter, and respond to a potential or actual maritime migration affecting the United States and its maritime borders.

The DHS/DOS Mass Migration Communication Strategy provides a strategic messaging strategy for coordinated and effective communication before, during, and after a mass migration event.

Currently and in response to anticipated terrorist threats, DHS is working with interagency partners to develop counterterrorism contingency plan(s) for ensuring the continuity of national border security and to safeguard the Nation. Additionally and in response to recently implemented Presidential Directives, DHS is also developing implementation plans that ensure national security and strengthen national resilience.

Key Authorities and References

- Homeland Security Act of 2002 (Public Law 107–296), as amended
- Security and Accountability for Every Port (SAFE Port) Act of 2006 (Public Law 109-347)
- Implementing Recommendations of the 9/11 Commission Act of 2007
- Executive Order 13276, Delegation of Responsibilities Concerning Undocumented Aliens Interdicted or Intercepted in the Caribbean Region.

Appendix 2 to Annex C: Critical Infrastructure Security and Resilience

Purpose

The Federal Government's capability to secure the Nation's critical infrastructure against natural, technological, and adversarial hazards includes activities that 1) promote security by reducing the likelihood of incidents occurring, and 2) enhance resilience by reducing the impact and/or duration of disruptive incidents on critical infrastructure.

Scope

This appendix includes only the Federal *coordinating activities* for critical infrastructure security and resilience. It specifically includes the Federal coordinating structures and mechanisms required to deliver the Protection core capabilities and achieve critical infrastructure security and resilience objectives.

Objectives

This appendix will accomplish the following:

- Provide a concept of operations for integrating existing Federal capabilities to secure the Nation's critical infrastructure against acts of terrorism and manmade or natural disasters.
- Describe Federal operational coordination mechanisms that integrate resources and personnel for critical infrastructure security and resilience.
- Lay the foundation for further department or agency critical infrastructure security and resilience planning, including integration among *coordinating activities*.

Concept of Operation

This appendix explains how Federal departments and agencies work together to deliver core capabilities required to secure the Nation's critical infrastructure. The concept of operations provides the common platform for ensuring that Federal critical infrastructure security and resilience activities operate in concert to achieve joint interagency objectives and serves as the vehicle for synchronizing Federal efforts in the Protection mission area. It serves to coordinate the delivery of Federal capabilities only.

The effectiveness of these critical infrastructure security and resilience activities relies upon the close coordination and alignment of practices and functional relationships across the Federal Government, including partnerships with local, state, tribal, and territorial entities and critical infrastructure partners (including owners and operators).

Roles and Responsibilities

Critical infrastructure security and resilience requires a unity of effort throughout the Federal Government. Federal departments and agencies are required to assess their "internal critical infrastructure" in accordance with PPD-21. It is important to have the ability to prioritize Federal critical assets that, if degraded, could impact National Essential Functions, national security, and the ability to execute response and recovery operations. Several departments and agencies play a critical role in securing the Nation's critical infrastructure against natural, technological, and adversarial hazards. These departments and agencies include:

- DHS

- FLETC
- DOD
- Department of Energy (DOE)
- Department of the Treasury
- Department of Health and Human Services (HHS)
- USDA
- Department of Transportation (DOT)
- EPA
- DOS.

National Infrastructure Protection Plan (NIPP) 2013:

NIPP 2013: Partnering for Critical Infrastructure Security and Resilience outlines how government and private sector participants in the critical infrastructure community work together to manage risks and achieve security and resilience outcomes, by

- Building upon the critical infrastructure risk management framework of previous versions. Its vision, mission, and goals are supported by core tenets that focus on risk management and partnership to influence future critical infrastructure security and resilience planning at the international, national, regional, local, state, tribal, territorial, and owner and operator levels;
- Recognizing the overarching concepts relevant to all critical infrastructure sectors;
- Addressing the physical, cyber, and human considerations required for effective implementation of comprehensive programs;
- Including a “Call to Action,” which guides the collaborative efforts of the critical infrastructure community to advance security and resilience under three broad activity categories: building upon partnership efforts, innovating in managing risk, and focusing on outcomes;
- Including the overarching framework for a structured partnership approach between the government and private sector for protection, security, and resilience of critical infrastructure; and
- Establishing mechanisms for collaboration between private sector owners and operators and government agencies, as well as the requirements for partnerships between the Federal Government; critical infrastructure owners and operators; and local, state, tribal, and territorial government entities.

The below descriptions outline Federal Government roles and responsibilities within critical infrastructure security and resilience activities.

Title II of the Homeland Security Act of 2002, as amended, details DHS’s responsibilities as lead agency for critical infrastructure security and resilience. PPD-21: Critical Infrastructure Security and Resilience (PPD-21) recognizes that each critical infrastructure sector has unique characteristics, operating models, and risk profiles and designates Sector-Specific Agencies (SSA) that have institutional knowledge and specialized expertise about each sector. Descriptions of lead and SSA roles and responsibilities are below.

Lead Agency

The Secretary of Homeland Security provides strategic guidance, promotes a national unity of effort, and coordinates the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure. DHS's responsibilities as SSA or co-SSA for multiple sectors are described in the SSA sections below. In carrying out the responsibilities of the Homeland Security Act of 2002, as amended, the Secretary of Homeland Security:

- Evaluates national capabilities, opportunities, and challenges in securing critical infrastructure and making it resilient;
- Analyzes threats to, vulnerabilities of, and potential consequences from all hazards to critical infrastructure;
- Identifies security and resilience functions that are necessary for effective public-private engagement with all critical infrastructure sectors;
- Develops a national plan and metrics, in coordination with SSAs and other critical infrastructure partners;
- Integrates and coordinates Federal cross-sector security and resilience activities;
- Identifies and analyzes key interdependencies among critical infrastructure sectors; and
- Reports on the effectiveness of national efforts to strengthen the Nation's security and resilience posture for critical infrastructure.

DHS contains a cyber and physical critical infrastructure function that coordinates the effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure, as well as executes responsibilities as the SSA for multiple sectors, as described in the SSA sections below. This function also contains the designated national cyber and physical critical infrastructure centers as described below. The cyber and physical critical infrastructure function responsibilities include:

- Providing situational awareness of critical infrastructure security and resilience issues and activities by:
 - Developing and analyzing information, including:
 - Incident reporting, open source reporting, field reports and assessments
 - Modeling and simulation
 - .gov domain monitoring
 - Dynamic prioritization of infrastructure
 - Risk analysis
 - Sharing information across the government and private sector, including:
 - Data integration and visualization
 - Information exchange on threats and hazards.
- Identifying and enabling risk mitigation and reduction through:
 - Partnerships and capacity building:
 - Working with critical infrastructure owners and operators in the field and at the national level to identify risks and promote best practices

- Guiding the national unity of effort for critical infrastructure security and resilience
- Providing technical assistance to build capacity and mitigate risks
- Conducting and supporting assessments:
 - Conducting and supporting vulnerability and consequence assessments, including infrastructure sector-specific assessments, key asset assessments, and regional assessments
 - Conducting Federal facility assessments.
- Protecting physical and cyber infrastructure through:
 - Security and law enforcement services:
 - Federal network security
 - Protecting government assets, systems, and networks (physical, virtual, and human)
 - Regulating highest-risk chemical facilities and ammonium nitrate sales, purchase, and transfer
 - Incident management coordination:
 - Cybersecurity
 - Physical incident response support
 - Analytic support.

SSAs

Each critical infrastructure sector has unique characteristics, operating models, and risk profiles. The Federal SSA or co-SSA assigned to each sector has institutional knowledge and specialized expertise about their sector(s). Recognizing existing statutory or regulatory authorities of specific Federal departments and agencies, and leveraging existing sector familiarity and relationships, SSAs:

- Coordinate with DHS and other relevant Federal departments and agencies and collaborate with critical infrastructure owners and operators, with independent regulatory agencies, and with local, state, tribal, and territorial entities, as appropriate;
- Serve as a day-to-day Federal interface for the dynamic prioritization and coordination of critical infrastructure sector-specific activities;
- Carry out critical infrastructure incident management responsibilities consistent with statutory authority and other appropriate policies, directives, or regulations;
- Provide, support, or facilitate technical assistance and consultations for that sector to identify vulnerabilities and help mitigate incidents, as appropriate; and
- Support the Secretary of Homeland Security's statutorily required reporting requirements by providing, on an annual basis, sector-specific critical infrastructure information (CII).

Each critical infrastructure sector maintains an SSP, which details how the NIPP's risk management framework is implemented within the sector's unique characteristics and risk landscape. Each SSA develops an SSP through a coordinated effort involving its public and private sector partners.

Chemical Sector (SSA: DHS)

The Chemical Sector can be divided into five main segments, based on the end product produced: basic chemicals, specialty chemicals, agricultural chemicals, pharmaceuticals, and consumer products. Each of these segments has distinct characteristics, growth dynamics, markets, new developments, and issues. Because the majority of Chemical Sector facilities are privately owned, DHS builds stakeholder capacity and enhances critical infrastructure security and resilience through voluntary partnerships that provide training, resources, and exercises. DHS has also issued regulatory Chemical Facility Anti-Terrorism Standards (CFATS) for any facility that manufactures, uses, stores, or distributes certain chemicals at or above specified quantities or concentrations. DHS is designated as the SSA for the Chemical Sector.

Commercial Facilities Sector (SSA: DHS)

Facilities associated with the Commercial Facilities Sector operate on the principle of open public access, meaning that the general public can move freely throughout these facilities without the deterrent of highly visible security barriers. The Commercial Facilities Sector consists of eight subsectors:

- Public Assembly (e.g., arenas, stadiums, aquariums, zoos, museums, convention centers),
- Sports Leagues (e.g., professional sports leagues and federations),
- Gaming (e.g., casinos),
- Lodging (e.g., hotels, motels, conference centers),
- Outdoor Events (e.g., theme and amusement parks, fairs, campgrounds, parades),
- Entertainment and Media (e.g., motion picture studios, broadcast media),
- Real Estate (e.g., office and apartment buildings, condominiums, mixed use facilities, self-storage), and
- Retail (e.g., retail centers and districts, shopping malls).

DHS is designated as the SSA for the Commercial Facilities Sector.

Communications Sector (SSA: DHS)

PPD-21 identifies the Communications Sector as critical because it provides an “enabling function” across all critical infrastructure sectors. Over the last 25 years, the sector has evolved from predominantly a provider of voice services into a diverse, competitive, and interconnected industry using terrestrial, satellite, and wireless transmission systems. The transmission of these services has become interconnected; satellite, wireless, and wireline providers depend on each other to carry and terminate their traffic, and companies routinely share facilities and technology to ensure interoperability. DHS is the SSA for the Communications Sector.

Critical Manufacturing Sector (SSA: DHS)

The Critical Manufacturing Sector identified the following industries to serve as the core of the sector: primary metal manufacturing; machinery manufacturing; electrical equipment, appliance, and component manufacturing; and transportation equipment manufacturing. Products made by these manufacturing industries are essential to many other critical infrastructure sectors. DHS is designated as the SSA for the Critical Manufacturing Sector.

Dams Sector (SSA: DHS)

The Dams Sector is composed of assets that include dam projects, hydropower generation facilities, navigation locks, levees, dikes, hurricane barriers, mine tailings, other industrial waste impoundments, and other similar water retention and water control facilities. The Dams Sector is a vital part of the Nation’s infrastructure and provides a wide range of economic, environmental, and social benefits, including hydroelectric power, river navigation, water supply, wildlife habitat, waste management, flood control, and recreation. The Dams Sector has interdependencies with a wide range of other sectors. DHS is designated as the SSA for the Dams Sector.

Defense Industrial Base Sector (SSA: DOD)

The Defense Industrial Base Sector is the worldwide industrial complex that enables research and development, as well as design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts, to meet U.S. military requirements. The Defense Industrial Base partnership consists of DOD components, Defense Industrial Base companies and their subcontractors who perform under contract to the DOD, companies providing incidental materials and services to the DOD, and government-owned/contractor-operated and government-owned/government-operated facilities. Defense Industrial Base companies include domestic and foreign entities, with production assets located in many countries. The sector provides products and services that are essential to mobilize, deploy, and sustain military operations. The Defense Industrial Base Sector does not include the commercial infrastructure of providers of services such as power, communications, transportation, or utilities that the DOD uses to meet military operational requirements; these commercial infrastructure assets are addressed by other SSAs. The DOD is designated as the SSA for the Defense Industrial Base Sector.

Emergency Services Sector (ESS) (SSA: DHS)

A system of prevention, preparedness, response, and recovery elements, the ESS represents the Nation’s first line of defense in the prevention and mitigation of risk from both intentional and unintentional manmade incidents, as well as from natural disasters. The majority of ESS functions are performed at the local, state, tribal, and territorial levels, and are defined by five disciplines:

- Law Enforcement;
- Fire and Emergency Services;
- Emergency Management;
- Emergency Medical Services (EMS); and
- Public Works.

Additionally, the ESS includes several specialized capabilities, such as HAZMAT; search and rescue; explosive ordnance disposal (i.e., bomb squads); tactical operations (i.e., SWAT); aviation units (i.e., police and medevac helicopters); and public safety answering points (i.e., 9-1-1 call centers). DHS is designated as the SSA for the ESS.

Energy Sector (SSA: DOE)

The Energy Sector is divided into three subsectors: electricity, oil, and natural gas. The heavy reliance on pipelines to distribute petroleum products across the Nation highlights the interdependencies between the Energy and the Transportation Systems Sector. The reliance of virtually all industries on electric power and fuels means that all sectors have some dependence on the Energy Sector. PPD-21 identifies the Energy Sector as uniquely critical because it provides an “enabling function” across all critical infrastructure sectors. More than 80 percent of the country’s

energy infrastructure is owned by the private sector, supplying fuels to the transportation industry, electricity to households and businesses, and other sources of energy to growth and production across the Nation. DOE is designated as the SSA for the Energy Sector.

Financial Services Sector (SSA: Department of the Treasury)

Within the Financial Services Sector, financial institutions are organized and regulated based on services provided by institutions. The sector contains more than 18,800 federally insured depository institutions; thousands of providers of various investment products, including roughly 18,440 broker-dealer, investment adviser, and investment company complexes; providers of risk transfer products, including 7,948 domestic U.S. insurers; and many thousands of other credit and financing organizations. The Department of the Treasury is designated as the SSA for the Financial Services Sector.

Food and Agriculture Sector (Co-SSAs: HHS and USDA)

The Food and Agriculture Sector is almost entirely under private ownership, and this sector accounts for roughly one-fifth of the Nation's economic activity. The United States has roughly 2.1 million farms, encompassing 915 million acres of land. In 2014, there were more than 935,000 restaurants and institutional food service establishments and an estimated 114,000 supermarkets, grocery stores, and other food outlets. The USDA and FDA both regulate imported food products. FDA regulates the majority of food imported into the United States. The USDA Food Safety and Inspection Service (FSIS) maintains positive controls on its imports. Plants have to request from USDA to import FSIS-regulated products into the United States. USDA evaluates both the plant and government regulations to ensure they are equivalent to U.S. standards. Additionally, as of February 19, 2014, there were 81,575 FDA registered domestic food facilities (warehouses, manufacturers, processors) and 115,753 FDA registered foreign food facilities. The FSIS also regulates more than 6,500 establishments for meat, poultry, processed egg products, imported products, and voluntary inspection services. FDA only inspects after the imported food has caused an issue. APHIS maintains regulation to prevent disease and pests from entering the country which may be harmful to U.S. agriculture. The bulk of the inspections are done through memoranda of understanding with CBP who are present at the borders 24/7, while USDA and HHS may not be. The Food and Agriculture Sector has critical dependencies with many sectors, but particularly with the following:

- Water and Wastewater Systems, for clean irrigation and processed water;
- Transportation Systems, for movement of products and livestock;
- Energy, to power the equipment needed for agriculture production and food processing; and
- Financial Services, Information Technology, Chemical, and Dams.

USDA and HHS are designated as the Co-SSAs for the Food and Agriculture Sector.

Government Facilities Sector (Co-SSAs: DHS and General Services Administration [GSA])

The Government Facilities Sector includes a wide variety of buildings, located in the United States and overseas, that are owned or leased by local, state, tribal, territorial, and Federal entities. Many government facilities are open to the public for business activities, commercial transactions, or recreational activities, while others that are not open to the public contain highly sensitive information, materials, processes, and equipment. In addition to physical structures, the sector includes cyber elements that contribute to the protection of sector assets (e.g., access control systems and closed-circuit television systems) as well as individuals who perform essential functions or possess tactical, operational, or strategic knowledge.

- **The Education Facilities Subsector** covers pre-kindergarten through 12th grade schools, institutions of higher education, and business and trade schools. The subsector includes facilities that are owned by both government and private sector entities.
- **The National Monuments and Icons Subsector** encompasses a diverse array of assets, networks, systems, and functions located throughout the United States. Many National Monuments and Icons assets are listed in either the National Register of Historic Places or the List of National Historic Landmarks.

DHS and the General Services Administration are designated as the co-SSAs for the Government Facilities Sector.

Healthcare and Public Health Sector (SSA: HHS)

More information on Protection activities in the Healthcare and Public Health Sector is contained in Appendix 4 to Annex C: Health Security.

The Healthcare and Public Health Sector protects all sectors of the economy from hazards, including infectious disease outbreaks. Operating in all U.S. states, territories, and tribal areas, the sector plays a significant role in response and recovery across all other sectors in the event of a natural or manmade disaster. While healthcare tends to be delivered and managed locally, the public health component of the sector, focused primarily on population health, is managed across all levels of government: local, state, tribal, territorial, and national. The Healthcare and Public Health Sector is highly dependent on fellow sectors for continuity of operations and service delivery, including:

- Communications;
- Emergency Services;
- Energy;
- Food and Agriculture;
- Information Technology;
- Transportation Systems; and
- Water and Wastewater Systems.

HHS is designated as the SSA for the Healthcare and Public Health Sector.

Information Technology Sector (SSA: DHS)

More information on Protection activities in the Information Technology Sector is contained in Appendix 8 to Annex B: Cybersecurity.

The Information Technology Sector is central to the Nation's security, economy, and public health and safety. The Information Technology's virtual and distributed functions produce and provide hardware, software, and information technology systems and services, and—in collaboration with the Communications Sector—the Internet. Although information technology infrastructure has a certain level of inherent resilience, its interdependent and interconnected structure presents challenges as well as opportunities for coordinating public and private sector preparedness and protection activities. DHS is designated as the SSA for the Information Technology Sector.

Nuclear Reactors, Materials, and Waste Sector (SSA: DHS)

Nuclear power provides approximately 20 percent of America's electricity through 60 nuclear reactors. The sector includes nuclear power plants; nonpower nuclear reactors used for research,

testing, and training; manufacturers of nuclear reactors or components; radioactive materials used primarily in medical, industrial, and academic settings; nuclear fuel cycle facilities; decommissioned nuclear power reactors; and transportation, storage, and disposal of nuclear and radioactive waste. The sector is interdependent with other critical infrastructure sectors:

- Chemical Sector, as a consumer of chemicals through the nuclear fuel cycle and at reactor sites;
- Energy Sector, as a supplier of electricity to our Nation's electrical grid;
- Healthcare and Public Health Sector, as a supplier of nuclear medicine, radiopharmaceuticals, and in the sterilization of blood and surgical supplies; and
- Transportation Systems Sector, through the movement of radioactive materials.

DHS is designated as the SSA for the Nuclear Reactors, Materials, and Waste Sector.

Transportation Systems Sector (Co-SSAs: DHS and DOT)

More information on Protection activities in the Transportation Systems Sector is contained in Appendix 8 to Annex C: Transportation Security.

The Transportation Systems Sector consists of seven key subsectors, or modes:

- **Aviation** (including aircraft, air traffic control systems, and commercial and other airports, heliports, and landing strips, including those for civil and joint use with the military);
- **Highway infrastructure and motor carrier** (including roadways, bridges, and tunnels; as well as vehicles [automobiles, motorcycles, trucks, commercial freight vehicles, motor coaches, and school buses]);
- **Maritime transportation system** (coastline, ports, waterways, Exclusive Economic Zone, and intermodal landside connections);
- **Mass transit and passenger rail** (service by buses, rail transit, long-distance rail, cable cars, inclined planes, funiculars, and automated guideway systems);
- **Pipeline systems** (carrying natural gas, hazardous liquids, and chemicals, including liquefied natural gas processing and storage facilities);
- **Freight rail** (including major carriers, small railroads, active railroad, freight cars, and locomotives [also includes track and structures DOD-designated as critical to mobilization and resupply of U.S. forces]; and
- **Postal and shipping** (differentiated from general cargo operations).

DHS and DOT are designated as the Co-SSAs for the Transportation Systems Sector.

Water and Wastewater Systems Sector (SSA: EPA)

The Water and Wastewater Systems Sector includes public drinking water systems and wastewater treatment systems in the United States. The vast majority of the U.S. population receives their potable water from these drinking water systems and has its sanitary sewerage treated by these wastewater systems. The Water and Wastewater Systems Sector is vulnerable to a variety of attacks, including contamination with deadly agents, physical attacks such as the release of toxic gaseous chemicals, and cyber attacks. Critical sectors, such as ESS, Healthcare and Public Health, Energy, Food and Agriculture, and Transportation Systems, would suffer negative impacts from a denial of service in the Water and Wastewater Systems Sector. The EPA is designated as the SSA for the Water and Wastewater Systems Sector.

Critical Task Summary

Each of these Federal partners supports the delivery of the Protection core capabilities required for critical infrastructure security and resilience. The table below describes how the Federal Government delivers each Protection core capability in the Critical Infrastructure Security and Resilience mission space.

Table 16: Critical Infrastructure Security and Resilience Core Capabilities Critical Task Summary

Core Capability	Critical infrastructure security and resilience Critical Task Summary
Access Control and Identity Verification	<ul style="list-style-type: none"> ▪ Control and limit access to critical locations and systems. ▪ Support verification efforts to authorize, grant, or deny physical and cyber access to key infrastructure assets and support systems.
Intelligence and Information Sharing	<ul style="list-style-type: none"> ▪ Set requirements for intelligence and information sharing across critical infrastructure sectors. ▪ Establish intelligence and information sharing processes between critical infrastructure stakeholders at all levels of government and critical infrastructure owners and operators to share threat information, advisories, attack indicators, and corrective measures. ▪ Gather, analyze, and share threat information, vulnerability assessment, attack indicators, and other security information. ▪ Use intelligence and information to provide routine support to CI protection measures and to support the development of protection measures to help safeguard CI assets and systems.
Interdiction and Disruption	<ul style="list-style-type: none"> ▪ Ensure sufficient capacity to address issues caused by CBRNE incidents through detection, deterrence, and mitigation measures. ▪ Provide support to infrastructure necessary to protect U.S. communities against the potential impacts of extremist terrorist incidents. ▪ Provide sufficient law enforcement and security presence at critical infrastructure sites to effectively deter or disrupt efforts to reach critical infrastructure assets or personnel.
Screening, Search, and Detection	<ul style="list-style-type: none"> ▪ Provide support to CBRNE detection and deterrence efforts at critical infrastructure assets to help prevent CBRNE devices from reaching their targets at CI sites. ▪ Coordinate local, state, tribal, territorial, Federal, and private sector efforts to conduct vulnerability and threat assessments, identify present threats to CI assets, develop suitable training and remedial measures to protect CI assets, and share resources and information. ▪ Identify Federal grant programs to help support improved screening, search, and detection measures at CI assets.
Physical Protective Measures	<ul style="list-style-type: none"> ▪ Develop and implement risk-based physical and cybersecurity measures, policies, security plans, business continuity plans, and procedures for both public and private CI assets. ▪ Identify assets, systems, networks, and functions of critical infrastructure that require protection and conduct risk assessments of those assets and systems. ▪ Develop appropriate training, physical protection measures, and policies to encourage improved protection capabilities for CI owners and operators. ▪ Develop measures to identify threats to critical lifeline sector infrastructure assets and devise protection measures to address those threats.

Core Capability	Critical infrastructure security and resilience Critical Task Summary
<p>Risk Management for Protection Programs and Activities</p>	<ul style="list-style-type: none"> ▪ Build the capacity for risk and resilience analysis and assessment skills in all critical infrastructure sectors and for owners and operators. ▪ Develop a unified approach for investment and grant funding for secure and resilient infrastructure. ▪ Gather data and conducting risk assessments to help drive effective sharing of threat information, risk management plans, and corrective measures that enhance the protection capability of critical infrastructure. ▪ Update comprehensive risk assessments to incorporate changes to aging infrastructure, changes in the physical and threat environments, new technologies, and more up-to-date data.
<p>Cybersecurity</p>	<ul style="list-style-type: none"> ▪ Develop resilient cyber systems that can maintain continuous service of essential functions and develop resilient infrastructure systems that support continuous operations during attacks on supporting cyber systems. ▪ Identify and analyze information on cyber threats to physical systems, threats to the physical elements of cyber systems, and the impact of cyber incidents on critical infrastructure sectors. ▪ Build partnerships between cybersecurity key stakeholders and industry representatives to support cyber protection planning and protection measures. ▪ Share actionable cyber threat information with critical infrastructure key stakeholders and leverage law enforcement and intelligence assets to support identification and disruption of cyber threats to critical infrastructure systems. ▪ Secure public and private cyber networks and critical infrastructure by implementing countermeasures, technologies, and policies.
<p>Supply Chain Integrity and Security</p>	<ul style="list-style-type: none"> ▪ Analyze key dependencies and interdependencies of supply chain operations and their reliance on and support of critical infrastructure systems, assets, and networks, and use risk management principles to identify new threats and vulnerabilities. ▪ Implement physical protection measures and policies to secure and make resilient the key nodes and transportation networks and assets that support protection of supplies. ▪ Integrate security processes into supply chain operations planning and use layers of defense planning to protect against a diverse range of threats to the supply chain and materials contained therein. ▪ Use verification and detection capabilities to identify goods that are misrepresented or contaminated and prevent their entry into the U.S. or the U.S. supply chain. ▪ Prevent cargo and supplies from being misdirected or compromised as they move into or out of the U.S.

Coordination Structures

The mechanisms for collaboration between private sector owners and operators and government agencies is outlined in NIPP 2013, which includes the protocols to be used to synchronize communication and actions within the Federal Government and the identified functional relationships within DHS and across the Federal Government, including the public-private partnership model.

Within this partnership model, Federal Government coordination occurs within Government Coordinating Councils (GCC), the SSAs (as described above), and the Federal Senior Leadership Council (FSLC). Furthermore, Sector Coordinating Councils (SCC) play a critical role in private sector coordination for each critical infrastructure sector.

Sector and Cross-Sector Coordinating Structures

Critical Infrastructure Sector	Sector-Specific Agency	Critical Infrastructure Partnership Advisory Council		
		Sector Coordinating Councils (SCCs)	Government Coordinating Councils (GCCs)	Regional Consortia
Chemical	Department of Homeland Security	✓	✓	
Commercial Facilities <i>i</i>		✓	✓	
Communications <i>i</i>		✓	✓	
Critical Manufacturing		✓	✓	
Dams		✓	✓	
Emergency Services <i>i</i>		✓	✓	
Information Technology <i>i</i>		✓	✓	
Nuclear Reactors, Materials & Waste		✓	✓	
Food & Agriculture	Department of Agriculture, Department of Health and Human Services	✓	✓	
Defense Industrial Base <i>i</i>	Department of Defense	✓	✓	
Energy <i>i</i>	Department of Energy	✓	✓	
Healthcare & Public Health <i>i</i>	Department of Health and Human Services	✓	✓	
Financial Services <i>i</i>	Department of the Treasury	Uses separate coordinating entity	✓	
Water & Wastewater Systems <i>i</i>	Environmental Protection Agency	✓	✓	
Government Facilities	Department of Homeland Security, General Services Administration	Sector does not have an SCC	✓	
Transportation Systems <i>i</i>	Department of Homeland Security, Department of Transportation	Various SCCs are broken down by transportation mode or subsector.	✓	

i Indicates that a sector (or a subsector within the sector) has a designated information-sharing organization.

Figure 5: Infrastructure Sector and Cross-Sector Coordination Structure

GCCs

The GCCs enable interagency, intergovernmental, and cross-jurisdictional coordination within and across sectors. They comprise representatives not only from the Federal Government, but also local, state, tribal, and territorial entities (as appropriate to the operating landscape of each individual sector). Each GCC is co-chaired by a representative from the designated SSA with responsibility to ensure appropriate representation on the council and provide cross-sector coordination with local,

state, tribal, and territorial governments. The GCC coordinates strategies, activities, policies, and communications across governmental entities within each sector.

SCCs

The SCCs are self-organized and self-governed councils that enable critical infrastructure owners and operators, their trade associations, and other industry representatives to interact on a wide range of sector-specific strategies, policies, and activities. The SCCs coordinate and collaborate with SSAs and related GCCs to address the entire range of critical infrastructure security and resilience policies and efforts for that sector.

FSLC

The FSLC is composed of senior officials from the designated SSAs and other Federal departments and agencies identified in PPD-21. The FSLC facilitates enhanced Federal communication and coordination across the sectors focused on critical infrastructure security and resilience.

The Federal Government has established cybersecurity centers and other government organizations with missions that include executing cyber operations, enhancing information sharing, maintaining situational awareness, and serving as conduits between public and private sector entities. Federal Cybersecurity Centers provide a platform from which a Cyber Unified Coordination Group (UCG) can coordinate the Federal Government's response to a malicious cyber incident.

NICC

The NICC is an operational component of the NPPD and the national physical infrastructure watch operations element of the DHS NOC, as designated by the Secretary of Homeland Security. The NICC coordinates a national network dedicated to the security and resilience of the critical infrastructure of the United States by providing 24/7 situational awareness and information sharing and fostering a unity of effort. Establishing and maintaining relationships with critical infrastructure partners both within and outside the Federal Government is at the core of the NICC's ability to execute its functions. The NICC collaborates with Federal departments and agencies and private sector partners to monitor potential, developing, and current regional and national operations of the Nation's critical infrastructure sectors.

National Cybersecurity and Communications Integration Center (NCCIC)

The NCCIC is the cyber operational component of NPPD and is the national cyber critical infrastructure center designated by the Secretary of Homeland Security. The NCCIC secures Federal civilian agencies in cyberspace; provides support and expertise to private sector partners and local, state, tribal, and territorial entities; and coordinates with international partners. The NCCIC also coordinates the Federal Government protection, mitigation, response, and recovery efforts for significant cyber and communications incidents affecting critical infrastructure, in accordance with PPD-21. Furthermore, the NCCIC serves as the primary platform for a Cyber UCG to coordinate the Federal Government's asset response to a significant cyber incident. The NCCIC is authorized under Section 3 of the National Cybersecurity Protection Act of 2014.

Support to Other Coordinating Activities

The Critical infrastructure security and resilience coordinating activity provides support to the other *coordinating activities* in a variety of ways:

- It supports **Border Security** through work relating to critical infrastructure systems and assets that include POEs and transportation infrastructure.

- It supports **Defense Against WMD Threats** through cross-sector risk assessment, analysis, and impact modeling.
 - In particular, this includes assessments conducted through the DHS OCIA that inform impact assessment and planning efforts for WMD defense.
- It supports **Health Security** by supporting the SSA, as delineated by NIPP 2013.
 - HHS serves as the SSA for Healthcare and Public Health Sector (HPH Sector), supporting the public-private partnership focused on enhancing the HPH Sector's security and resilience.
 - This includes managing risks, promoting cybersecurity, sharing information, and coordinating response and recovery efforts.
- It supports **Immigration Security** efforts by supporting robust national infrastructure across multiple infrastructure sectors, especially Transportation Systems.
 - SSPs and the sector partnership structure support immigration security efforts through planning and strategic assessment.
- It supports **Maritime Security** through efforts to promote and protect maritime critical infrastructure.
 - Maritime critical infrastructure includes facilities, structures, systems, assets, or services vital to the port area and its economy.
 - Some maritime critical infrastructure, predominantly shoreside facilities that transfer cargo (passengers, bulk liquids and solids, packaged goods, and containers), warrant USCG visits only when vessels carrying such cargoes are present.
 - Some maritime critical infrastructure has relatively high likelihood and consequence scores for a particular terrorist attack mode, when their risks are compounded by the presence of a high-risk ship or barge that is engaged or about to engage in transfer operations.
 - USCG maritime security regimes comprise the rules and protocols that enhance collaboration on all-hazard maritime infrastructure resilience and recovery planning, exercises, and operations. This element of layered security implements domestic and international statutes, regulations, and agreements that coordinate partnerships and establish maritime security standards.
 - The Maritime Transportation Security Act (MTSA) requires the identification of threats to maritime critical infrastructure and key resources; periodic assessment of the effectiveness of antiterrorism measures in both U.S. and foreign ports; and action in cases where effective antiterrorism measures are not in place.
 - USCG and CBP AMO Maritime Domain Awareness (MDA) comprise the effective understanding of objects and activities in or near marine critical infrastructure/key resources that could affect their security or safety.
 - The USCG and CBP AMO conduct a diverse set of Air and Maritime Security and Response Operations (MSRO) activities designed to reduce risks associated with terrorist attack scenarios on critical infrastructure. These include security boardings of vessels suspected of supporting terrorism or other illegal activities that may pose a threat to critical infrastructure; waterborne, air, and shoreside patrols; and enforcement of fixed security zones at maritime

critical infrastructure. This layered, risk-based approach is designed to detect, deter, and disrupt terrorist attacks against maritime critical infrastructure.

- It supports the **Protection of Key Leadership and Special Events** by supporting infrastructure sectors.
 - The Commercial Facilities and Government Facilities infrastructure sectors include many assets where special events take place, and those SSAs play an active role (DHS for both including Federal Protective Service (FPS) and GSA for government facilities) in supporting Protection of Key Leadership and Special Events.
 - DHS Protective Security Advisors (PSAs) also support these Protection efforts.
- It supports **Transportation Security** efforts by promoting interagency efforts on protecting critical transportation infrastructure.
 - DOT, TSA, and USCG work jointly to support the Transportation Systems Sector, and the NIPP 2013 partnership structure supports security coordination and planning for the Transportation Systems Sector.

Support from Other Coordinating Activities

The Critical Infrastructure Security and Resilience coordinating activity receives support from the other *coordinating activities* in a variety of ways

- It gets support from **Border Security** by providing sector-specific information and analysis, as infrastructure systems can span geographic and political boundaries. Border Security interdicts terrorist threats, drug traffickers, and other threats to national security, economic security, and public safety.
 - ICE HSI conducts investigations into intellectual property rights (IPR), trade transparency, money laundering, general smuggling, and cybercrime investigations that cross silos with almost all critical infrastructure sectors.
 - Additionally, ICE HSI conducts sensitive investigations into the counter proliferation and illegal export of nuclear materials, munitions systems, weapons, technology, and other critical manufacturing and defense related industries, as well as investigations into dual use chemicals and compounds imported and exported contrary to law.
- It gets support from **Defense Against WMD Threats** through the NIPP 2013 partnership structure that supports CBRN equities through sector coordination structures and SSA functions.
 - This includes SSPs for related sectors (Chemical sector—DHS, Defense Industrial Base—DOD, Nuclear Reactors, Materials, and Waste Sector—DHS, Food and Agriculture Sector, USDA and HHS, Healthcare and Public Health Sector—HHS).
- It gets support from **Health Security** through the work supporting the critical infrastructure sectors.
 - Healthcare and Public Health is a critical infrastructure sector.
 - HHS is the SSA for this sector.
- It gets support from **Immigration Security** through ICE HSI, which conducts insider threat investigations under its Title 8 authorities to identify foreign nationals and aliens employed at

critical infrastructure who may pose a threat to national security. It gets support from **Maritime Security** through work supporting the critical infrastructure sectors.

- The maritime transportation mode is a subsector or mode of the Transportation Systems Sector, one of the critical infrastructure sectors.
 - Maritime critical infrastructure includes facilities, structures, systems, assets, or services vital to the port area and its economy.
 - USCG maritime security regimes comprise the rules and protocols that enhance collaboration on all-hazard maritime infrastructure resilience and recovery planning, exercises, and operations.
 - This element of layered security implements domestic and international statutes, regulations, and agreements that coordinate partnerships and establish maritime security standards. For example, MTSA requires the identification of threats to maritime critical infrastructure and key resources; periodic assessment of the effectiveness of antiterrorism measures in both U.S. and foreign ports; and action in cases where effective antiterrorism measures are not in place.
 - USCG MDA comprises the effective understanding of objects and activities in or near the marine environment that could affect the security, safety, economy, or environment of the U.S.
 - The USCG conducts a diverse set of MSRO activities designed to reduce risks associated with terrorist attack scenarios on critical infrastructure. These include security boardings of various vessels; waterborne, air, and shoreside patrols; and enforcement of fixed security zones at maritime critical infrastructure.
 - This layered, risk-based approach is designed to detect, deter, and disrupt terrorist attacks against maritime critical infrastructure.
- It gets support from **Protection of Key Leadership and Special Events** through work by the FBI, USSS, and ICE HSI to investigate and prosecute actual or attempted terrorist attacks on, sabotage of, or disruptions of critical infrastructure and key resources, as well as investigating Federal criminal violations which fall within their jurisdictions.
- The Commercial Facilities and Government Facilities sectors include many assets where special events take place and those where SSAs play an active role (DHS is SSA for both sectors, including Federal Protective Service (FPS) and General Services Administration (GSA) for government facilities).
- It gets support from **Transportation Security** through work supporting the SSAs, as delineated by NIPP 2013, particularly with regard to coordination efforts.
- The co-SSAs for Transportation Systems under NIPP 2013 are DHS (USCG and TSA) and DOT.
 - Transportation security supports intelligence and information sharing on cross-sector issues between/among interdependent sectors, such as the Energy Sector.
 - Coordination among these partners is critical, as the Transportation Systems Sector is considered a “lifeline function” within the NIPP construct—as critical transportation infrastructure supports everything from national security and economic stability to public health and safety.

Support to Other Mission Areas

Within the context of critical infrastructure security and resilience, Prevention activities are most closely associated with efforts to address threats; Protection efforts generally address vulnerabilities; and Response and Recovery efforts help minimize consequences. Mitigation efforts transcend the entire threat, vulnerability, and consequence spectrum. To support efforts in advance of or during an incident, the Federal Government critical infrastructure community collaborates, based on the structures established in each of the National Planning Frameworks and FIOPs. Specific to the Response preparedness mission area, the Secretary of Homeland Security is the principal Federal official for domestic incident management and coordinates Federal Government responses to significant cyber or physical incidents affecting critical infrastructure (consistent with statutory authorities).

Operational Coordination for Infrastructure Systems

The NOC is DHS's principal operations center. It provides situational awareness and a common operating picture for the Federal Government, and for local, state, and tribal governments as appropriate, in the event of a natural disaster, act of terrorism, or other manmade disaster. The NOC ensures that critical terrorism and disaster-related information reaches government decision makers. As the infrastructure coordination element of the NOC, the NICC receives situational, operational, and incident-related information regarding the status of the Nation's critical infrastructure sectors during incidents. It collects input from every SSA, which is consolidated into a comprehensive report and included in National Level Reporting (NLR) and the NOC Senior Leader Brief (SLB). The OCIA Integrated Analysis Cell (IAC),³⁰ which is co-located with the NICC Watch and Warning, serves as the risk integration and analysis function for critical infrastructure. The IAC supports the NICC and the NCCIC with security and resilience strategic risk analysis to better understand and address incidents, threats, and emerging risks to critical infrastructure. The DHS Office of Intelligence and Analysis (I&A) Cyber Division provides onsite cyber threat intelligence support to the NCCIC and provides analysis focused on cyber threats to the .gov, state, local, and critical infrastructure networks.

Key Plans

- NIPP 2013: Partnering for Critical Infrastructure Security and Resilience
- SSPs.

Key Authorities and References

The following laws, policy directives, strategies, and EOs are included in addition to the general authorities/references provided in the base plan for the Critical Infrastructure Security and Resilience mission activity:

- Title II of the Homeland Security Act of 2002 (Public Law 107–296), as amended
- CII Act of 2002
- 6 C.F.R. Part 29, "Procedures for Handling Critical Infrastructure Information," September 2006
- PPD–17, Countering Improvised Explosive Devices, June 2012

³⁰ OCIA was established in 2014 within NPPD to provide critical infrastructure risk analysis, decision support, and modeling capabilities to public and private sector partners.

- PPD–21, Critical Infrastructure Security and Resilience, February 2013
- HSPD–5, Management of Domestic Incidents, February 2003
- HSPD–9, Defense of United States Agriculture and Food, January 2004
- EO 12977, Interagency Security Committee, October 1995
- EO 13636, Improving Critical Infrastructure Cybersecurity, February 2013
- EO 13650, Improving Chemical Facility Safety and Security, August 2013
- DHS Fiscal Years 2014-2018 Strategic Plan
- The NPPD Strategic Plan for Fiscal Years 2014–2018, May 2013
- NPPD Office of Infrastructure Protection Strategic Plan: 2012–2016, August 2012
- 2014 Quadrennial Homeland Security Review (QHSR), June 2014
- National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, February 2003
- Critical Infrastructure and Key Resources Support Annex to the National Response Framework (NRF), May 2013
- 40 U.S.C. § 1315 entitled, “Law Enforcement Authority of the Secretary of Homeland Security for Protection of Public Property”
- FPS Policy Directive 15.1.2.1, Law Enforcement Authorities and Powers, November 2011.

Appendix 3 to Annex C: Defense Against WMD Threats

Purpose

WMD, in any of the CBRNE forms, in the possession of hostile states and terrorists, represents one of the greatest security challenges facing the United States. The organizations that defend the country cannot assume that they will identify an adversary early enough to study and gather intelligence on them before an attempted attack. Nevertheless, the objective is to prevent or stop the first attack (not just defeat the adversary). Consequently, considerable resources and effort have been invested in creating defenses against the use of WMD as represented by the *coordinating activities* to follow. Individually and collectively their mission is to make WMD terrorism a prohibitively difficult undertaking for our adversaries. To do this, the United States must maintain constant vigilance and aggressively plan to counter the evolving threat of WMD terrorism.

Scope

The scope of this document includes only the *coordinating activities* of the counter-WMD (CWMD) stakeholders and their communities. The operational deployment and employment of response elements is not included in the scope of this document, as they are part of the programmatic efforts of individual departments and agencies. The relevant CBRNE strategic plans, as well as associated implementing documents, domestic and international guidance, annual reviews, and other efforts and documentation, define the scope and constituents of the CWMD communities.

Objectives

This appendix will accomplish the following:

- Provide a concept of operations for integrating existing Federal capabilities to secure the homeland against WMD.
- Describe Federal operational coordination mechanisms that integrate resources and personnel for defense against WMD.
- Lay the foundation for further department or agency Protection planning for defense against WMD, including integration among *coordinating activities*.

Concept of Operations

This appendix explains how Federal departments and agencies work together to deliver core capabilities required to secure the homeland against WMD. The concept of operations provides the common platform for ensuring that Federal actions operate in concert to achieve joint interagency objectives and serves as the vehicle for synchronizing Federal WMD efforts in the Protection mission area. It serves to coordinate the delivery of Federal capabilities only.

In general, WMD Defense coordination activities are a specialized subset of the Counter-Terrorism or Critical infrastructure security and resilience efforts. Specific WMD Defense coordination is predominantly supports these efforts on a modality basis, i.e. biological, chemical, and nuclear/radiological.

Biological protection activities generally include two mechanisms:

- Biosurveillance
- Biosecurity.

Roles and Responsibilities

Defense Against WMD threats requires a unity of effort throughout the Federal Government. Several departments and agencies play a critical role in detecting, analyzing, and reporting on WMD-related threats. These departments and agencies include:

- Domestic Nuclear Detection Office (DNDO)
- The FBI WMD Directorate
- DOD
- DOE
- CBP
- DHS, Office of Health Affairs (OHA)
- The Office of the Director of National Intelligence (ODNI)
- The U.S. Nuclear Regulatory Commission (NRC)
- ICE HSI Export Enforcement Coordination Center (E2C2)
- DOS.

Each of these Federal partners supports the delivery of the Protection core capabilities and the continued defense against WMD. The table below describes how the Federal Government delivers each Protection core capability in the WMD mission space.

Table 17: Defense Against WMD Threats Core Capabilities Critical Task Summary

Core Capability	Defense Against WMD Threats Critical Task Summary
Access Control and Identity Verification	<ul style="list-style-type: none"> ▪ Support verification efforts to authorize, grant, or deny physical and cyber access to key assets.
Intelligence and Information Sharing	<ul style="list-style-type: none"> ▪ Set requirements for intelligence and information sharing across all sectors. ▪ Establish intelligence and information sharing processes between stakeholders at all levels of government and key private sector partners to share threat information, advisories, attack indicators, and corrective measures that can help address WMD issues. ▪ Monitor, detect, and analyze threats to public safety, health, and security that could be posed by a WMD attack and work to develop education and awareness programs to help address those threats. ▪ Gather, analyze, and share threat information, vulnerability assessment, attack indicators, and other security information. ▪ Use intelligence and information to provide routine support for WMD protection measures, training, and exercises.
Interdiction and Disruption	<ul style="list-style-type: none"> ▪ Disrupt financing and logistical support for potential terrorist activities in the U.S. and prevent weapons, precursors, related technology, or WMD materials from reaching intended targets. ▪ Coordinate efforts with local, state, tribal, and territorial partners to detect WMD threats and ensure that key stakeholders and assets have the capacity to detect CBRNE devices and resolve CBRNE threats. ▪ Increase visible law enforcement and security presence and interdict conveyances, cargo, people, or modes of transportation that could be utilized to deliver a WMD to its intended target.

Core Capability	Defense Against WMD Threats Critical Task Summary
Screening, Search, and Detection	<ul style="list-style-type: none"> ▪ Provide active screening and surveillance of people, baggage, mail, cargo, and conveyances to detect and identify any potentially threatening materials or persons using CBRNE detection, biosurveillance, and screening for health threats. ▪ Provide nationwide active and passive CBRNE screening of persons, baggage, mail, cargo, and conveyances. ▪ Support intelligence and information sharing to help stakeholders identify potential threats and capability gaps. ▪ Establish coordinated efforts that help develop and train an engaged surveillance network from across all levels of government, the private sector, and the public at large to identify WMD threats. ▪ Support threat assessments, improvements in sensor technologies, testing, and intelligence gathering and analysis to improve national capacity to detect, identify, locate, and address WMD threats and hazards.
Physical Protective Measures	<ul style="list-style-type: none"> ▪ Develop and implement risk-based physical security measures, policies, and procedures, including biosecurity and biosurveillance program and practices. ▪ Identify necessary physical protection measures that will support key functions and operations and need to be protected against WMD threats. ▪ Improve training and acquisition programs that will help improve the acquisition of key resources and skills needed to address WMD threats.
Risk Management for Protection Programs and Activities	<ul style="list-style-type: none"> ▪ Develop tools and community capacity for analyzing and assessing threats, risks, and vulnerabilities to WMD attacks. ▪ Gather and share relevant information and use that collective information to develop risk assessments that incorporate changes to the physical environment, aging infrastructure, technological developments, and updated data. ▪ Use risk assessments to develop exercises and other work to validate and enhance future risk assessments and mitigation projects and initiatives.
Cybersecurity	<ul style="list-style-type: none"> ▪ Implement countermeasures, technologies, and policies to protect physical and cyber assets, networks, applications, and systems that support Defense Against WMD Threats operations. ▪ Perform protection risk assessments and corrective measures on key cyber systems and assets that could be impacted by a WMD attack. ▪ Perform protection risk assessments and corrective measures on key systems and assets that could be impacted by a WMD attack on physical and electronic cyber assets and systems.
Supply Chain Integrity and Security	<ul style="list-style-type: none"> ▪ Develop multilayer defense and planning efforts to safeguard necessary supplies for Defense Against WMD Threats operations against asymmetrical and traditional threats. ▪ Safeguard against introduction of WMD into the supply chain through risk and vulnerability assessments and information and resource sharing.

DNDO’s Role in Defending Against WMD Threats

For the R/N community, the Global Nuclear Detection Architecture (GNDA) serves as a mechanism for Prevention and Protection. Its Federal stakeholders include DHS, DOS, DOD, DOJ, DOE, and ODNI as well as the NRC. However, the GNDA is not only a Federal enterprise; there are roles for local, state, tribal, and territorial law enforcement agencies, the private sector, academia, foreign governments, and international organizations.

The GNDA is a framework for detecting (through technical and nontechnical means³¹), analyzing, and reporting on nuclear and other radioactive materials that are out of regulatory control.³² As a coordinating activity, the GNDA stakeholders seek to unify, synchronize, and integrate programs and authorities to fill gaps and minimize vulnerabilities. Although the GNDA does not constitute the entire approach to preventing R/N terrorism, it plays a unifying role. The 2014 GNDA Strategic Plan provides greater detail on the GNDA as it describes the programs, capabilities, and activities of the GNDA and its Federal partners.³³

The whole-of-government approach to countering nuclear terrorism leverages routine security activities that act as a force multiplier for countering nuclear or radiological security threats. As with the prevention of broader terrorist activity, no single tool can defeat nuclear terrorism. A comprehensive system, as described by the Nuclear Security Spectrum, includes controls over nuclear materials and weapons; technical measures that detect signatures unique to radioactive material; intelligence; law enforcement; reporting and information sharing; border security; inter alia; the deterrent effect of a robust attribution capability, and other means. Each of these means contribute to nuclear security and should not be viewed in isolation, as the defenses are complementary.

As with the broader counterterrorism challenge, absolute security against the threat posed by nuclear or radioactive materials is neither fiscally nor operationally possible. Instead, nuclear security is about managing risk. The GNDA stakeholders employ a systematic method to effectively reduce risk through a layered approach. In this layered approach, careful consideration should be given toward where best to focus efforts. There should not be one dominant layer but rather prioritization based on strategic needs. Each layer must contribute to the overall risk reduction because no one layer, program, or other effort can fully eliminate risk. The combination of risk reduction across all layers opposes the entire threat pathway from material acquisition to adversary attack, reduces the risk to the greatest extent possible, and provides the most efficient use of resources.

In order to achieve the most cost-effective, risk-informed GNDA, the GNDA should serve as “a coordinated, layered defense of effective capabilities for rapid and responsive detection, analysis, and reporting on nuclear and other radioactive materials out of regulatory control that makes nuclear terrorism prohibitively difficult.”³⁴

Existing strategic policies, directives, and guidance provide the basis for the development of the broad lines of effort to counterterrorism and provide security to the Nation. Four lines of effort or ways to organize activities and operations can be derived from this guidance that, used broadly, form a part of a coherent framework to address the threat of nuclear terrorism. The GNDA-related capabilities and the activities of its stakeholders reduce the risk of R/N attacks in three fundamental ways: they seek to deter adversaries from attempting such attacks; they detect and report nuclear and other radioactive materials out of regulatory control; and they induce changes in the tactics of

³¹ Detection of nuclear or other radioactive material out of regulatory control may be accomplished through multiple methods. Technical detection refers to an alarm caused by use of technology such as a radiation detection system. Nontechnical detection refers to an alert caused by law enforcement or intelligence efforts and collected by GNDA partners under their statutory authorities and consistent with national policy.

³² The term “out of regulatory control” refers to materials that are being imported, possessed, stored, transported, developed, or used without authorization by the appropriate regulatory authority, either inadvertently or deliberately.

³³ For further information please visit <http://www.dhs.gov/global-nuclear-detection-architecture>.

³⁴ GNDA Strategic Plan 2014.

adversaries that increase the likelihood of detection by technical or nontechnical means. The four lines of effort are:

- Deter,
- Detect/Locate,
- Integrate tools/capabilities, and
- Build partnerships.

Deter: The capabilities and activities of the GNDA partners, when properly messaged and demonstrated to the public, have the potential to deter adversaries by convincing them an R/N attack would be prohibitively difficult. Adversaries may decide against attempting such attacks or change tactics, which may increase the likelihood of detection by technical or nontechnical means. GNDA-related capabilities and activities contribute to deterrence by making R/N attacks more costly for the adversary to undertake, more difficult to carry out, and less likely to succeed.

It is important that deterrence concepts are considered early in the planning process to ensure effective application as part of the current GNDA-related capabilities. The deterrent nature of GNDA-related capabilities and activities is an important element to overall risk reduction, as deterrence multiplies the effect of deployed capabilities. Fending off endless methods of attacks is difficult and costly. In fact, if a nuclear threat reaches the point of execution and is thwarted at the last moment, the GNDA has largely failed. Hence, deterring attacks before they begin becomes increasingly important.

Concepts or approaches that help to achieve this end include:

- Coordinated messaging
- Visible presence
- Unpredictable operations.

Detect/Locate: Detection as a means to find or locate material out of regulatory control includes traditional technical means to sense particles emitted from radioactive materials; technical means that use NII; other technical means, such as ultrasound or weight measurement; and nontechnical approaches, to include conventional intelligence and law enforcement activities, intelligence cues, surveillance, or operational encounters by law enforcement. A “detection event” could entail either an instrument alarm or an information alert. In practical terms, what detect/locate means for the GNDA is recognition that a R/N material potential threat is present and determination of its specific location so that when the “detector/locator” relays or reports the discovery to the appropriate response organization for action, no inherent delay occurs in that response.³⁵ Concepts or approaches include:

- Detector enhancement and sustainment
- Chokepoints/checkpoints
- Domain awareness
- Layered defense in depth

³⁵ In accordance with PPD-25, all WMD threat information having a potential impact on the United States is immediately passed to the FBI to conduct a timely Threat Credibility Evaluation (TCE).

- Intelligence-driven processes.

Integrate Tools/Capabilities: One way to increase capability and reduce the resource burden on individual stakeholders is to integrate their tools and capabilities, thereby eliminating redundancy across GNDA stakeholders. Efforts might involve linking established hubs of coordination, information sharing, and conducting analysis. Integration of operational capabilities across overlapping missions aids in this effort.

Build Partnerships: Reducing the risk of nuclear terrorism requires full integration and coordination of domestic and international partner activities. It is important to coordinate the goals, purposes, and reporting/data exchange mechanisms of the various stakeholders that implement the GNDA, so that the GNDA performs as a whole rather than a collection of separate efforts.

This requires developing appropriate and necessary partnerships. Many GNDA partners are often engaged in the full range of cooperative counterterrorism activities—from intelligence sharing to joint training and operations, and from countering radicalization to pursuing community resilience programs. The focus of GNDA efforts to build partnerships must be shared security concerns. Partner cooperation established in other security-related settings can transfer smoothly and efficiently to the GNDA. Concepts or approaches include:

- Regional nuclear detection architectures

The Securing the Cities program seeks to design and implement or enhance existing architectures for coordinated and integrated detection and interdiction of nuclear and other radioactive materials that are out of regulatory control and which may be used as a weapon within high-risk metropolitan areas. The program issues financial assistance and support to state and local stakeholders' efforts to build a regional nuclear detection architecture that may be integrated with federal efforts.

- Bilateral engagements
- International efforts (e.g., International Atomic Energy Agency (IAEA), INTERPOL, United Nations Security Council Resolution 1540, and Global Initiative to Combat Nuclear Terrorism)
- Domestic partnerships (DNDO's Securing the Cities program).

These lines of effort, undertaken in sequence, in parallel, and in blended form, contribute to a coordinated GNDA to address the threat of nuclear terrorism.

GNDA Modes of Operation

It is useful to define GNDA modes of operation to describe the state of response or readiness of the execution of operations of the GNDA.

The primary modes of operation are steady state, enhanced steady state, and crisis situations. These modes aid in a general understanding of both the capability level of a GNDA response and the resource allocation level, as well as give a general indicator of the threat environment. These modes are summarized from the GNDA International Implementation Plan as:

- **Steady state operations:** Represent day-to-day R/N detection operations which are overlaid on existing mission areas as part of a daily routine. Steady state operations provide a multilayered approach to detection efforts and occur on a daily basis regardless of any credible threat.
- **Enhanced steady state operations:** Represent augmented operations in support of a heightened threat environment or planned security-related activities.

- **Crisis situations:** Represent an additional layer of coordination and support in response to a significant threat/detection event and/or request from a partner nation for assistance.

Steady State

Steady state operations consist of a diverse combination of R/N detection capabilities. They are conducted routinely to detect or locate and report on R/N materials and devices. These include routine law enforcement or counterterrorism activities such as border security, cargo security, physical security, maritime boarding/inspections, and immigration enforcement. Steady state operations are decentralized, involving single or multiple agencies in different areas of the country, without specific intelligence available to influence operations.

Ground passengers and cargo are screened for radiation signatures at border crossings and points of entry, as are rail cars and maritime craft, and air passengers and air cargo. GNDA partners receive information from the NRC to understand registered and scheduled movements of radiological sources across the borders and around the country for both significant industrial sources and significant locations of radiation-based medical treatment. Inside the borders, substantial local, state, tribal, and territorial resources are available to conduct interior screening, executed through a combination of law enforcement, HAZMAT and radiation safety organizations, teams and equipment. Technical resources support and respond to front line detection efforts, including additional and specialized detection and identification equipment and national reachback resources.

Depending on their capabilities, resources, and threat conditions, local, state, tribal, and territorial jurisdictions conduct steady state operations on a regular basis. These operations are conducted by different organizations with different authorities—law enforcement, fire department, emergency response or HAZMAT teams, and public health and environmental protection teams. GNDA stakeholders primarily conduct GNDA operations as a secondary piece of their primary missions.

Under steady state conditions, the GNDA is supported by general intelligence awareness. This refers to intelligence that comes from assessments provided by intelligence community (IC) members that describes, in general terms, the capabilities and intent of adversaries to acquire and use radioactive materials. This strategic intelligence can inform general decision making about resource allocation and employment; it is different from the operational or tactical intelligence that would influence operations by providing sufficient detail as to warrant movement to an enhanced steady state or search mode.

Enhanced Steady State

When necessary, enhanced steady state operations include augmented operations in support of a heightened threat environment or planned security-related activities. Enhanced steady state operations provide an additional layer of response by altering the steady state posture by introducing or “surging” additional capabilities to increase the probability of locating threat materials or devices. The USG can conduct enhanced steady state operations for a period of days, weeks, or longer as necessary, and the operations are characterized by a greater-than-normal level of screening, inspection, reporting, and awareness, which may or may not focus on a particular location.

The USG can provide a variety of additional support resources designed to augment and strengthen local, state, tribal, and territorial capabilities; these include technical reachback capabilities; DHS Mobile Detection Deployment Program (MDDP) assets; WMD civil support teams (CST); DOE Radiological Assistance Program (RAP) teams; USCG support and DHS/DNDO training, exercises, and red team support. The CBP Laboratories and Scientific Services Directorate Teleforensic Center (LSSD-TC) provides WMD adjudication and support to CBP, all DHS components, and select state and local entities. TSA operations include visible intermodal prevention and response (VIPR) teams

who deploy nationwide with preventive radiological nuclear detection (PRND) equipment, randomly and unpredictably scheduling operations with a risk-based framework.

The importance of enhanced steady state planning and operations is to make the GNDA a flexible and adaptable national capability that represents a stronger deterrent to and defense against R/N threats to the homeland. The GNDA must include the ability to surge assets and capabilities and to augment or introduce additional R/N detection capacity and capability into a geographical area or pathway for a period of time to address a potential threat or heightened vulnerability, increase deterrence, or respond to a credible threat.

One reason for enhancing steady state operations is to support special events. For example, escalated operations may increase presence at transportation nodes during holiday travel seasons, foreign head of state visits, major special events, high profile activities, anniversaries, and other significant events or dates. These situations often call for an increased level of security, and surged R/N detection capabilities are often employed at special events as part of increased security. Special events also provide important opportunities to exercise expanded operations and capabilities.

Expanded operations can occur over both large areas and checkpoints at borders and other logical places; they will likely be done in coordination with law enforcement and investigation activities. As with steady state, enhanced steady state operations are based on the mission environment (low profile, overt, large/small area, speed of conveyance, etc.) and will be influenced by the available intelligence. A decision to escalate to enhanced steady state may also trigger other activities such as standing up other crisis action teams, preparing NTAS guidance, or conducting actions supporting the FBI's WMD crisis operations.

Adjustments from steady state conditions include:

- Enhanced operations or employment of additional resources
- Increased operations tempo on the part of both existing full-time teams and many part-time teams and other resources shifting towards full time operations.

Adjusted operational procedures to balance detection probabilities and the impact on the flow of commerce are based on the threat characterization level.

Crisis Situations

Crisis or emergency situations may arise that require additional capabilities, coordination, and support in response to a significant threat/detection event, and/or request from a partner nation or non-Federal entity for assistance. The response for crisis situations depends on the circumstances and nature of the crisis. A domestic crisis situation as identified by the FBI's Threat Credibility Evaluation (TCE) would involve coordination with and support to FBI-led RNSO. An international search requires an additional layer of coordination and support. The Counterterrorism Security Group (CSG), operating in accordance within the PPD-1 structure, determines appropriate (including non-GNDA) responses in these incidents.

For domestic crisis situations involving R/N material, the USG has approved an "Interagency Domestic Radiological/Nuclear Search Plan (May 2011)," which describes how the USG, through the FBI, will organize and coordinate interagency RNSO when the FBI's TCE process determines there is a credible R/N threat. Given a credible threat, the FBI will conduct a criminal or national security investigation and may initiate RNSO if the potential impact of the threat and the threat scenario warrant a search response. RNSO is one component of the investigation and will focus on coordinating the unique multidiscipline elements and technical challenges in locating and interdicting R/N materials or devices. The Interagency Domestic Radiological/Nuclear Search Plan describes

search as localized operations under command and control of a FBI tactical commander, where local, state, tribal, territorial, and Federal GNDA activities are integrated with supplemental R/N search assets into a defined search area.

When a TCE identifies an R/N threat requiring a response, the FBI, acting through the JTTF, will open an investigation or continue to investigate an existing opened case on the R/N threat. The JTTF will use traditional law enforcement/national security techniques as the primary means to investigate the R/N threat. All RNSO will directly support this investigation and as such, must be closely coordinated with the JTTF.

The FBI will be the lead for the R/N threat investigation and will synchronize the Federal response and coordinate with the local, state, tribal, and territorial entities where appropriate to ensure the R/N investigation objectives are met, deconflict response elements' roles and responsibilities, and take steps to avoid compromise of the investigation. R/N search assets will work closely with and support the FBI to preserve investigative efforts, evidence, and crime scene integrity, and will comply with all applicable safety rules.

The Nation could be in either steady state or enhanced steady state conditions at the time of the decision to execute RNSO. If at steady state, the initiation of RNSO could trigger initiation of enhanced steady state in some regions, although the specifics may be limited by the investigation and associated operational security considerations.

During response to imminent WMD threats, the Federal departments and agencies conducting the Prevention and Protection mission areas coordinate closely to share information and to resolve the threat.

FBI's Role in Defending Against WMD Threats

Like other Executive Branch departments and agencies, the DOJ and the FBI will endeavor to coordinate their activities with other members of the law enforcement community and with members of the IC to achieve maximum cooperation consistent with the law and operational necessity.

The Attorney General has lead responsibility for criminal investigations of terrorist acts or terrorist threats by individuals or groups inside the United States, or directed at United States citizens or institutions abroad, where such acts are within the Federal criminal jurisdiction of the United States, as well as for related intelligence collection activities within the United States, subject to the National Security Act of 1947 (as amended) and other applicable law, EO 12333 (as amended), and Attorney General-approved procedures pursuant to that EO. Generally acting through the FBI, the Attorney General, in cooperation with other Federal departments and agencies engaged in activities to protect our national security, shall also coordinate the activities of the other members of the law enforcement community to detect, prevent, preempt, and disrupt terrorist attacks against the United States. Generally acting through the FBI Director, the Attorney General has primary responsibility to search for, find, and neutralize WMD within the United States.

The FBI Director exercises lead agency responsibility in investigating all crimes for which it has primary or concurrent jurisdiction and that involve terrorist activities, or acts in preparation of terrorist activities, within the statutory jurisdiction of the United States. Within the United States, this responsibility includes the collection, coordination, analysis, management, and dissemination of intelligence and criminal information in collaboration with other executive branch departments as appropriate. This includes the receipt and resolution of suspicious activity reports of terrorist activities or acts in preparation of terrorist activities.

Relating to any foreign counterintelligence matter, the FBI Director is designated by Presidential directives to take charge of investigative work regarding espionage, sabotage, subversive activities, and other foreign counterintelligence matters, to include investigations of counterintelligence related to WMD proliferation. Working with other departments when appropriate, the Attorney General, generally acting through the FBI Director, will reduce domestic threats and will thwart and investigate attacks on, or criminal disruptions of, critical infrastructure. The Attorney General, generally acting through the FBI Director, serves as the Federal lead on terrorism investigations and prosecution within the statutory jurisdiction of the United States for threats, acts in furtherance of, attempts, or actual terrorist attacks. The Attorney General and the Secretary of Homeland Security shall use applicable statutory authority and attendant mechanisms for cooperation and coordination, including but not limited to those established by Presidential directive.

Following a terrorist threat or an actual incident that falls within the criminal jurisdiction of the United States, the full capabilities of the United States shall be dedicated, consistent with U.S. law and with activities of other Federal departments and agencies, to protect our national security, assist the Attorney General to identify the perpetrators, and bring them to justice.

ODNI's Role in Defending Against WMD Threats

ODNI serves as the head of the IC, acts as the principal advisor to the President for intelligence matters relating to national security, and oversees and directs implementation of the National Intelligence Program. The IC, comprising 17 elements across the Federal Government, functions consistent with law, EOs, regulations, and policy to support the national security-related missions of the USG. It provides a range of analytic products, including those that assess threats to the homeland and inform planning, capability development, and operational activities of homeland security enterprise partners and stakeholders. In addition to IC elements with specific homeland security missions, ODNI maintains a number of mission and support centers that provide unique capabilities for homeland security partners.

DOD's Role in Defending Against WMD Threats

The Secretary of Defense conducts homeland defense and civil support missions to prevent an imminent terrorist attack from occurring. DOD is responsible for domestic military activities that protect U.S. sovereignty, U.S. territory, the domestic population, and the critical defense infrastructure against external threats and aggression or other threats as directed by the President or the Secretary of Defense. DOD also provides defense support of civil authorities for domestic incidents as directed by the President or the Secretary of Defense, when consistent with military readiness and appropriate under the circumstances and the law.

DOE's Role in Defending Against WMD Threats

The National Nuclear Security Administration (NNSA), through its Office of Defense Nuclear Nonproliferation, works closely with a wide range of international partners, key U.S. Federal agencies, the U.S. national laboratories, and the private sector to detect, secure, and dispose of dangerous R/N material and related WMD technology and expertise. NNSA prevents and counters WMD proliferation by strengthening export control systems in other countries and transitioning WMD expertise and infrastructure in partner countries to peaceful purposes.

NRC's Role in Defending Against WMD Threats

The Commission as a whole formulates policies and regulations governing nuclear reactor and materials safety, issues orders to licensees, and adjudicates legal matters brought before it. The Executive Director for Operations carries out the policies and decisions of the Commission and

directs the activities of the program offices. The offices reporting to the Executive Director for Operations ensure that the commercial use of nuclear materials in the United States is safely conducted. As part of the regulatory process, the four regional offices conduct inspection, enforcement, and emergency response programs for licensees within their borders.

CBP's Role in Defending Against WMD Threats

CBP has a comprehensive network of radiation detection devices at each of the 328 ports of entry and between the ports of entry. This network is used to deter WMD, and detect and identify them if not deterred. The CBP LSSD-TC acts as the central adjudication point for all WMD cases for DHS, and coordinates with DOE and FBI when suspect threats are encountered. CBP is able to provide surge capability for R/N detection either with uniformed law enforcement personnel or with laboratory personnel. Laboratory personnel also bring the capability for on-site adjudication of R/N threats.

OHA, National Biosurveillance Integration Center (NBIC) Role in Defending against WMD Threats

NBIC works to enhance the Federal Government's ability to respond to biological incidents of national concern, whether accidental, intentional, or naturally occurring. The threat of bioterrorism and the global reach of emerging diseases requires our Nation's decision-makers to have timely, accurate and actionable information.

The NBIC is a collaboration of Federal partners to integrate information about threats to human, animal, plant, and environmental health from thousands of sources to develop a more comprehensive picture of the threat landscape. The resulting information helps the Nation better prepare, protect, and respond.

Coordination Structures

WMD Defense oriented coordination structures include:

- Nuclear Coordination
- DNDO.

Biocoordination

- National Biosurveillance Strategy

The National Biosurveillance Strategy provides critical information and ongoing situational awareness that enables better decision making throughout the whole community.

- Laboratory Response Network for Biological Threats (LRN-B)

The LRN runs a network of more than 150 labs that can respond to biological and chemical threats and other public health emergencies. It includes state and local public health, veterinary, military, and international labs. In addition to being able to test for Category A biological agents, a few LRN public health labs are able to measure human exposure to toxic chemicals through tests on clinical specimens.

- Bio Watch and National Biosurveillance Integration Center

DHS is responsible for key programs that provide decision support and the other situational awareness information for Federal and local decision makers.

Chemical Threat Coordination

- LRN-B: The LRN-B runs a network of more than 150 labs that can respond to biological threats. It includes state and local public health, veterinary, military, and international labs.
- Laboratory Response Network for Chemical Threats (LRN-C): The LRN-C is a national laboratory network that responds to chemical threats and other public health emergencies. The LRN-C operates 24/7 to provide laboratory diagnostics and surge capacity for chemical emergencies. Network members can detect exposure to a number of toxic chemical agents or work with hospitals and first responders to appropriately collect, store, and ship clinical samples to other LRN-C laboratories.

WMD/CBRN Coordination Mechanisms

- WMD Strategic Group (WMDSG)

When facing WMD terrorist threats, the FBI-led WMDSG, an interagency crisis action team, is activated within a Strategic Information Operations Center (SIOC). It supports information exchange and deconfliction of counterterrorism activities to prevent imminent WMD terrorist threats while simultaneously coordinating with the nationwide effort to save lives and protect property. The WMDSG, through its collection of interagency representatives, facilitates the application of real-time investigative information, intelligence, and technical analysis to WMD Counterterrorism (WMD-CT) law enforcement operations; facilitates the identification and acquisition of interagency assets that could support WMD-CT law enforcement operations; and enhances WMD-CT investigative information/intelligence sharing and synchronization of law enforcement operations with counterterrorism-related public health, homeland protection, and consequence management activities. The WMDSG, with its collaborative environment and through the dissemination of WMD Threat Profile products, contributes to the promotion of risk informed operations and decision making at all levels of the counterterrorism response, including local, state, tribal, territorial, and Federal law enforcement, public health, border security, and international partners. The WMDSG connects with the FBI field office(s) and appropriate local/regional partners through the Joint Operations Center(s) (JOC).

WMD Coordinators

The FBI has a WMD Coordinator assigned to each of its 56 field offices. WMD Coordinators manage the office's WMD program and serve as the point of contact for emergency responders and public health at the local, state, tribal, or territorial level in the event of a threat or incident potentially involving WMD. In the event of such an incident, the WMD Coordinator serves as a conduit for obtaining Federal assistance for operational response direction and threat evaluation support.

Note that CBRN-related facilities are listed as part of the NIPP in the Critical Infrastructure Annex above. CBRN equities primarily reside in the following NIPP 2013 annexes:

- Nuclear Reactors, Materials, and Waste Sector
- Healthcare and Public Health Sector
- Food and Agriculture Sector
- Chemical Sector.

R/N planning and assessment coordinating mechanisms:

- Countering Nuclear Threats Interagency Policy Committee (IPC)
- GNDA sub-IPC

- GNDA Interagency Working Group (IWG).

R/N analysis and reporting coordinating mechanisms:

- WMDSG.

Technical detection coordinating mechanisms:

- The Nuclear Defense Research and Development (NDRD) Working Group, convened by the White House Office of Science and Technology Policy (OSTP), facilitates the coordination of planning and information exchange for USG technical R/N detection research and development activities.
- Additional mechanisms such as the Combatting Terrorism Technical Support Office (CTTSO) Technical Support Working Group (TSWG) and the DNDO annual Industry Day exist to ensure coordination across departments and agencies for test and evaluation, systems development, and acquisition activities for R/N detection equipment.
- Four-party Memorandum of Understanding among DNDO, the Defense Threat Reduction Agency (DTRA), the NNSA, and ODNI.

Operational Support coordinating mechanisms:

- CBP LSSD-TC

CBP LSSD-TC is an operational entity which provides real time 24/7 R/N threat adjudications to all DHS components worldwide, and select state and local entities. LSSD-TC provides initial coordination with DOE and FBI during threat events which impact these entities.

- DHS DNDO Joint Analysis Center

The DNDO Joint Analysis Center facilitates the timely sharing and reporting of R/N incident and alarm data for Radiological Nuclear Detection (RND) agencies and meets the information requirements and crisis management capabilities of DHS for R/N threats.

- FBI SIOC

The FBI, through its JOC and FBI Headquarters (FBIHQ) SIOC, coordinates crisis action plan development for domestic counterterrorism activities with the ODNI National Counterterrorism Center (NCTC), DHS, DOD National Military Command Center (NMCC), and other Federal agency headquarters elements as appropriate. At the operational level, the JOC also coordinates planning for criminal investigations, law enforcement, and intelligence activities related to the threat.

- DHS NOC

The Secretary of Homeland Security's responsibilities in terrorism prevention and emergency response are supported by the NOC, which is the principal operations center for DHS. In the event of a terrorist threat or attack, the DHS NOC provides situational awareness and a common operating picture for the entire Federal Government and for local, state, tribal, territorial, and insular area governments and ensures that critical terrorism and disaster-related information reaches government decision makers. The DHS NOC consists of the following elements: NOC Watch; Intelligence Watch; Federal Emergency Management Agency (FEMA) National Watch Center (NWC) and NRCC; NICC; and a Planning Element. The NOC is also virtually linked to the operational centers of executive departments and agencies, DHS components, and local, state, and major urban area fusion centers.

- DOD NMCC

The DOD NMCC is a 24-hour operations center that maintains contact with other Federal operations centers. During terrorism incidents, if law enforcement resources are insufficient to provide an adequate response or specialized equipment and personnel are needed, the Attorney General may use available legal authorities to request support from DOD. In all incidents potentially requiring DOD support, the NMCC will serve as the operational coordination entry point for the DOJ/FBI at the national level. Communication and collaboration between the NMCC and SIOC is based on the specific requirements of the threat and requests for assistance from DOJ. If the FBI establishes a JOC, DOD may assign a representative to the JOC to facilitate support at the field level.

- NCTC

The NCTC leads the national effort to combat terrorism at home and abroad by analyzing threat information, sharing that information with partners, and integrating all instruments of national power. NCTC serves as the primary organization in the USG for integrating and analyzing all intelligence pertaining to terrorism possessed or acquired by the USG (except purely domestic terrorism); serves as the central and shared knowledge bank on known or suspected terrorists and international terror groups; and provides all-source intelligence support to government-wide counterterrorism efforts. NCTC also conducts the following activities:

- Produces integrated and interagency-coordinated analytic assessments on terrorism issues and publishes warnings, alerts, and advisories as appropriate.
- Leads secure video teleconferences with interagency partners and operational coordination structures to communicate real-time threat information on terrorist groups, capabilities, plans, and intentions, and emerging threats to U.S. interests at home and abroad in order to inform decision makers.
- Manages the ODNI National Counterterrorism Operations Center, which provides unique insight and situational awareness of developing terrorism-related worldwide issues and incidents.
- Operates a secure web-site, which serves as the primary dissemination mechanism for terrorism information produced by NCTC and other counterterrorism mission partners.
- Partners with DHS and FBI to provide terrorism-related interagency products to local, state, tribal, territorial, and insular area law enforcement and private sector partners. This is conducted by:
 - Partnering with analysts to create intelligence products for local, state, tribal, territorial, and insular area law enforcement.
 - Requesting classification downgrades for terrorism-related products suitable for first responders.
 - Facilitating briefing opportunities for intelligence analysts to interact with local, state, tribal, territorial, and insular area partners.

- WMDSG.

Communications coordinating mechanisms:

- Communications about implementation of R/N detection, analysis, and reporting activities are handled individually by departments and agencies in most cases. In situations where departments

and agencies must share information about R/N threats, each department or agency is aware of the appropriate channels to communicate with other USG departments and agencies and the appropriate White House officials. Additionally, the Countering Nuclear Threats IPC, or NSC, may intervene to coordinate interagency public affairs and messaging related to nuclear security, as needed.

Support to Other Coordinating Activities

The Defense Against WMD Threats coordinating activity provides support to the other *coordinating activities* in a variety of ways:

- It supports **Border Security** through intelligence and information sharing.
- It supports **Critical Infrastructure Security and Resilience** through the NIPP 2013 partnership structure that supports CBRN equities through sector coordination structures and SSA functions.
 - This includes SSPs for related sectors (Chemical Sector—DHS, Defense Industrial Base—DOD, Nuclear Reactors, Materials, and Waste Sector—DHS, Food and Agriculture Sector—USDA and HHS, Healthcare and Public Health Sector—HHS).
- It supports **Health Security** by developing medical countermeasures and nonpharmaceutical interventions to protect communities from and limit the adverse health impacts of WMD threats.
 - It also shares intelligence and health information to protect against threats.
- It supports **Immigration Security** through intelligence and information sharing.
- It supports **Maritime Security** efforts through intelligence and information sharing, as well as specific support actions by the USCG.
 - USCG security boarding/inspections are conducted routinely to detect or locate and report on R/N materials and devices or the transfer of terrorists into the U.S. who have the intent and capability to carry out WMD attacks.
 - USCG armed escorts of vessels carrying select certain dangerous cargoes are designed to protect the inhabitants of ports from the secondary consequences (i.e., death/injury, economic impacts, and environmental impacts) of a successful terrorist attack on such a vessel. In the event of a WMD attack in a port, the USCG provides remediation actions.
- It supports the **Protection of Key Leadership and Special Events** through intelligence and information sharing.
- It supports **Transportation Security** efforts through intelligence and information sharing.

Support from Other Coordinating Activities

The Defense Against WMD Threats coordinating activity receives support from the other *coordinating activities* in a variety of ways:

- It gets support from **Border Security** by providing shared intelligence and information, as Border Security operations support detection and interdiction efforts. Border security inspections are routinely conducted to detect or locate and report on R/N materials and devices.
 - ICE HSI special agents are assigned to JTTFs in support of the FBI's mission to prevent and protect against terrorist acts.

- Both CBP and ICE have WMD programs relating to the illegal import/export of either the precursors or actual WMD and therefore have a significant role in this area.
- HSI manages and operates the Export Enforcement Coordination Center, established by EO 13558, which strengthens the enforcement of U.S. export laws through the facilitation of partner agency communication and collaboration to keep our Nation safe.
- These counter proliferation efforts are executed by detecting, preventing, disrupting, investigating, and prosecuting violations of U.S. export control laws.
- It gets support from **Critical Infrastructure Security and Resilience** through cross-sector risk assessment, analysis, and impact modeling.
 - In particular, this includes assessments conducted through the DHS OCIA that inform impact assessment and planning efforts for WMD defense.
- It gets support from **Health Security** through health security activities that share information on potential threats and help gauge the potential impact of WMD.
 - These include coordination to help identify potential risk factors that could exacerbate a WMD incident.
- It gets support from **Immigration Security** through ICE HSI special agents who are assigned to JTTFs in support of the FBI's mission to prevent and protect against terrorist acts.
- It gets support from **Maritime Security** through the USCG, which provides defense activities to support our Nation's proliferation security initiative, while USCG Maritime Security Regime and MSRO includes sensors that detect WMD.
 - USCG maritime security boarding/inspections are conducted routinely to detect or locate and report on R/N materials and devices.
- It gets support from **Protection of Key Leadership and Special Events** through CBRN detection and analysis, including biosensor technology, radiation detection technology, and physical screening of attendees, vehicles, and equipment.
- It gets support from **Transportation Security** through valuable information and intelligence sharing to help maintain necessary situational awareness of potential threats to the transportation sector.
 - Transportation assets and systems are vulnerable to threats relating to WMD, as terrorist groups and criminals can use transportation assets and systems as targets or delivery methods for WMD attacks.
 - Information sharing can include sharing information on specific threats, as well as providing information on a general threat picture to help the sector as a whole develop effective protection strategies based on the current operating picture.

Support to Other Mission Areas

Prevention mission support

During responses to imminent WMD terrorist threats, the Protection mission area capabilities can be leveraged for Prevention mission activities, as appropriate. Further, the standing Protection WMD mission activities can serve as a means to identify specific, credible threats so that they may be resolved through Prevention efforts.

Response mission support

By working together and adopting the joint Criminal-Epidemiological (Crim-Epi) model, public health and law enforcement are able to achieve their separate but often overlapping objectives of determining an intentional versus unintentional event and protecting public health and safety. The Joint FBI/Centers for Disease Control and Prevention (CDC) Crim-Epi Investigations Initiative facilitates the establishment and sustainment of relationships between public health, law enforcement, and first responders at the local, state, tribal, territorial, and Federal levels. The Crim-Epi mission is primarily accomplished through Joint FBI/CDC Crim-Epi Workshops, which build relationships, share information, conduct joint threat assessments and investigations, and establish joint training and protocols to address potential bioterrorism threats.

Key Plans

- GNDAs Strategic Plan 2014
- GNDAs Domestic Implementation Plan 2015
- GNDAs International Implementation Plan 2012
- DHS GNDAs Implementation Plan 2012.

Key Authorities and References

The following laws, policy directives, strategies, and EOs are included in addition to the general authorities/references provided in the base plan for the Defense Against WMD Threats Coordinating Activity:

- EO 12333
- Federal Terrorist Use of Explosives (TUE), August, 2008
- Federal Improvised Nuclear Device, Strategic Guidance Statement (SGS), September 2008
- Federal Improvised Nuclear Device, Strategic Plan, January 2009
- Federal Biological Attack (BIO), SGS, January 2009
- Federal Radiological Attack (RDD), SGS, January 2009
- Federal Chemical Attack (CML), SGS, June 2009
- Federal RDD Attack, Strategic Plan, July 2009
- Federal BIO Attack, Strategic Plan, July 2009
- Global Initiative to Combat Nuclear Terrorism (GICNT) Model Guidelines Document for Nuclear Detection Architectures (2009)
- Global Threat Reduction Initiative
- GNDAs Strategic Plan 2014
- GNDAs Annual Report 2015
- Homeland Security Act of 2002, Section 1902, codified at 6 U.S.C. §592.
- HSPD-5: Management of Domestic Incidents
- HSPD-9: Defense of Food and Agriculture
- HSPD-10: Biological Weapons Defense

- HSPD-13: National Security Presidential Directive (NSPD)-41: Maritime Security
- HSPD-21: National Biodefense Strategy and National Strategy for Countering Biological Threats
- HSPD-22: Domestic Chemical Defense
- IAEA Nuclear Security Recommendations on Nuclear and Other Radioactive Materials out of Regulatory Control (IAEA Nuclear Security Series No. 15)
- Maritime Operational Threat Response Plan (2006)
- NRF
- NSPD-17/HSPD-4: National Strategy to Combat WMD (successor PPD document in draft)
- NSPD-43/HSPD-14: Domestic Nuclear Detection
- NSPD-38: National Strategy to Secure Cyberspace
- NSPD-54/HSPD-23: Cyber Security and Monitoring
- National Security Strategy (NSS) 2015
- National Strategy for Combating WMD (2006)
- National Strategy for Counterterrorism 2011
- National Strategy for Homeland Security 2007
- PPD-8: National Preparedness
- PPD-17: Countering Improvised Explosive Devices
- PPD-18: Maritime Security Policy
- PPD-21: Critical Infrastructure Security and Resilience
- PPD-25
- PPD-39: U.S. Counterterrorism Policy
- PRND Capability Development Framework
- PRND National Incident Management System (NIMS) Resource Typing
- QHSR, February 2014
- Quadrennial Defense Review (QDR), 2010 Strategy to Combat Transnational Organized Crime 2011
- United States Code Title 18: Illegal Use of WMD/CBRN
 - 18 U.S.C. § 175 – Prohibitions with Respect to Biological Weapons
 - 18 U.S.C. § 229 – Prohibited Activities
 - 18 U.S.C. § 545 – Smuggling Goods into the United States
 - 18 U.S.C. § 554 – Smuggling Goods from the United States
 - 18 U.S.C. § 831 – Prohibited Transactions Involving Nuclear Materials
 - 18 U.S.C. § 842 – Unlawful Acts
 - 18 U.S.C. § 2332 – Criminal Penalties

- United States Code Title 22 – Foreign Relations
 - 22 U.S.C. § 2778 – Control of Arms Exports and Imports.

This page intentionally left blank.

Appendix 4 to Annex C: Health Security

Before disaster strikes, people and their communities need to be prepared for the threats to health that come with disasters and emergencies. They need to be ready to protect themselves and remain resilient in the face of these threats. National health security is a state in which the Nation and its people are prepared for, protected from, and resilient in the face of incidents with health consequences. A future focus is important because the factors affecting national health security are continually evolving as health threats change and new threats emerge. Terrorist groups may develop novel ways to defeat our Nation's defenses; antibiotic resistance may reduce our ability to stop the spread of deadly diseases; and climate change may exacerbate the range, frequency, and destructive power of extreme weather incidents. The economic environment is also dynamic and unpredictable, affecting the resources available to strengthen national health security.

The Protection FIOP builds on the National Health Security Strategy 2015–2018 (NHSS), which provides a framework to build community resilience, strengthen and sustain health emergency response systems, improve capabilities, and prioritize resources on current and future budgets. This appendix to the Protection FIOP outlines roles and responsibilities for departments and agencies in Health Security and describes how the Federal Government delivers Protection core capabilities in order to secure the homeland from health-related threats and hazards.

Scope

This appendix focuses only on the Federal *coordinating activities* for Health Security. It specifically includes the Federal coordinating structures and mechanisms required to deliver the Protection core capabilities and achieve Health Security objectives.

Objectives

This appendix will accomplish the following:

- Provide a concept of operations for integrating existing Federal capabilities to strengthen and sustain communities' abilities to protect against incidents with negative health consequences.
- Describe Federal operational coordination mechanisms that integrate resources and personnel for Health Security.
- Lay the foundation for further department or agency Health Security planning, including integration among *coordinating activities*.

Concept of Operations

This appendix explains how Federal departments and agencies work together to deliver core capabilities required to secure the homeland against health-related threats and hazards. The concept of operations provides the common platform for ensuring that Federal actions operate in concert to achieve joint interagency objectives and serves as the vehicle for synchronizing Federal Health Security efforts in the Protection mission area. It serves to coordinate the delivery of Federal capabilities only.

Roles and Responsibilities

Health Security requires a unity of effort throughout the Federal Government. Several departments and agencies play a critical role in strengthening and sustaining communities' abilities to protect against incidents with health consequences. These departments and agencies include:

- HHS

- Administration on Aging, FDA
- Health Resources and Services Administration
- Indian Health Service
- Veterans Health Administration
- CDC
- FEMA
- DOS.

Each of these Federal partners support the delivery of the Protection core capabilities required for Health Security. The table below describes how the Federal Government delivers each Protection core capability in the Health Security mission space.

Table 18: Health Security Core Capabilities Critical Task Summary

Core Capability	Health Security Critical Task Summary
Access Control and Identity Verification	<ul style="list-style-type: none"> ▪ Support verification efforts to authorize, grant, or deny physical and cyber access to key assets.
Intelligence and Information Sharing	<ul style="list-style-type: none"> ▪ Set requirements for intelligence and information sharing across all sectors. ▪ Establish intelligence and information sharing processes between stakeholders at all levels of government and key private sector partners to share threat information, advisories, attack indicators, and corrective measures that can help address health security issues. ▪ Monitor, detect, and analyze threats to public health and security that could impact the health sector and work to develop education and awareness programs to help address those threats. ▪ Use intelligence and information to provide routine support for protection measures, training, and exercises for health security stakeholders. ▪ Support training and exercising of intelligence and information sharing of health threats and threats to health security systems.
Interdiction and Disruption	<ul style="list-style-type: none"> ▪ Disrupt terrorist financing and resource-acquisition activities by supporting improved security of potentially hazardous health sector assets. ▪ Ensure the capacity to detect CBRNE threats during health security screenings and resolve those threats prior to reaching their targets. ▪ Interdict conveyances, cargo, and persons to mitigate the spread of public health threats, CBRNE materials, and other threats to U.S. security. ▪ Coordinate with local, state, tribal, and territorial personnel and other Federal officials to address any threats identified by or detected within the health security system and effectively share information on how to interdict people and conveyances that could pose public health risks.

Core Capability	Health Security Critical Task Summary
<p>Screening, Search, and Detection</p>	<ul style="list-style-type: none"> ▪ Provide active screening and surveillance of people, baggage, mail, cargo, and conveyances to detect and identify any potentially threatening materials or persons using screening for health threats, CBRNE detection, and biosurveillance. ▪ Support intelligence and information sharing to help stakeholders identify potential threats and capability gaps, including coordinating local, state, tribal, territorial, and Federal efforts to drive risk assessment and awareness efforts. ▪ Establish coordinated efforts that help develop and train an engaged surveillance network from across all levels of government, the private sector, and the public at large to identify public health threats and develop measures to address public health threats at all levels of government. ▪ Support threat assessments, improvements in sensor technologies, testing, and intelligence gathering and analysis to improve the national capacity to detect, identify, locate, and address public health threats and hazards. ▪ Establish coordinated efforts among agencies (such as DOI, USDA, and HHS) that are charged with understanding and protecting wildlife, domesticated animal, human, and environmental health to significantly improve the ability to understand the potential for cross-species transmission and promote early detection of emerging pandemics.
<p>Physical Protective Measures</p>	<ul style="list-style-type: none"> ▪ Develop and implement risk-based physical security measures, including biosecurity and biosurveillance policies, as well as business continuity plans that address public health risks and threats to the delivery of health services. ▪ Develop training and acquisition programs that develop or deliver necessary skills and resources needed to address threats identified by risk assessments of the immigration security system and operations.
<p>Risk Management for Protection Programs and Activities</p>	<ul style="list-style-type: none"> ▪ Develop tools and community capacity for analyzing and assessing threats, risks, and vulnerabilities from threats to, or threats detected within, the health security system. ▪ Gather and share relevant information and deploy that collective information to develop risk assessments that incorporate changes to the physical environment, aging infrastructure, technological developments, and updated data. ▪ Use risk assessments to develop exercises and other work that can be used to validate and enhance future mitigation projects and initiatives that improve public health security and threats to the health sector.
<p>Cybersecurity</p>	<ul style="list-style-type: none"> ▪ Implement countermeasures, technologies, and policies to protect physical and cyber assets, networks, applications, and systems that support health security efforts and efforts to address public health threats.
<p>Supply Chain Integrity and Security</p>	<ul style="list-style-type: none"> ▪ Develop multilayer defense and planning efforts to safeguard necessary supplies for public health operations against asymmetrical and traditional threats and ensure the availability of key supplies during a public health crisis or national emergency. ▪ Use verification and detection capabilities to identify goods that are misrepresented or contaminated and prevent their entry into the health system. ▪ Support detection and identification of people who could pose a threat to supply chain operations or assets by sharing information and coordinating efforts in support of Protection efforts.

The NHSS 2015–2018 provides strategic direction to guide efforts to improve health security nationwide over the next four years with a common vision; base them on sound evidence; and carry them out in an efficient, collaborative manner. The Office of the Assistant Secretary for Preparedness and Response (ASPR) led the development of the NHSS in collaboration with a broad range of

stakeholders, including representatives from local, state, tribal, territorial, and Federal Government; community-based organizations; private-sector firms; and academia.

The NHSS recognizes health-related issues, specifically pandemic disease threats, as potential threats to national security. In addition, the NHSS incorporates concepts central to health security, including resilience, engaged communities and individuals, intergovernmental coordination, global public health cooperation, and strategic partnerships with NGOs. The strategy contributes to the strategic landscape in which the NHSS Implementation Plan operates and offers the Administration's vision, in partnership with Congress, with regards to national security. The NHSS Implementation Plan serves as a framework to help guide the Nation and facilitate collaboration and coordination among community organizations and businesses, as well as local, state, tribal, territorial, and Federal agencies in their pursuit of advancing national health security. HHS is responsible for meeting the Congressional requirement for developing the second quadrennial NHSS and Implementation Plan, but Federal and non-Federal stakeholders will carry out the steady state and emergency functions necessary to protect the Nation's health.

NHSS Strategic Objective 1: Build and Sustain Healthy, Resilient Communities

Community health resilience is a community's ability to use its assets to strengthen public health and healthcare systems and to improve the community's physical, behavioral, and social health to withstand, adapt to, and recover from adversity. Communities are facing an increasingly complex array of challenges. Human-caused and naturally occurring incidents are more frequent and costly and are influenced by global factors such as climate change, interconnected economies, and population shifts toward large, dense urban centers and megacities. A wider range of partners and capabilities must be brought together to address these heightened risks and to complement and expand available community, state, and Federal support. A community resilience approach does this by encouraging actions that improve the community's ability to withstand, adapt to, and recover from adversity while also promoting strong day-to-day systems and addressing the underlying social determinants of health.

The Nation will create a robust culture of health resilience, promoting physical and behavioral health and well-being, connecting communities, and championing volunteers. Across the Nation, communities, organizations, and individuals will all contribute through their unique resources and capabilities. A culture of resilience will equip them not only to address daily challenges, but also to prevent, prepare for, mitigate, respond to, and recover from large-scale emergencies. Individuals and households will know how to improve health and will act on that knowledge. They will be engaged with the healthcare system and understand how to support their neighbors and community. Households and communities will work together, with the support of local organizations, and will engage in training and planning that prepare them to fulfill their roles in health security. Communities will promote health in part by supporting community infrastructure, including secure housing, economically viable neighborhoods, quality healthcare facilities, and spaces for gathering and exercise. Public health, healthcare, behavioral health, and social service organizations will understand the needs of the people they serve and be ready to meet those needs before, during, and after an incident.

Risk Management for Protection Programs and Activities Core Capability

Using social connectedness through multiple mechanisms to promote community health resilience is a priority of the NHSS that aligns with the critical task involving capacity building within communities to analyze and assess risk and resilience. Community members are encouraged to use social networking sites and other methods designed to strengthen neighbor-to-neighbor ties and explore potential uses of such sites for emergency response.

NHSS Strategic Objective 2: Enhance the National Capability to Produce and Effectively Use Both Medical Countermeasures and Nonpharmaceutical Interventions

Countermeasures—Medical Countermeasures (MCM) and Nonpharmaceutical Interventions (NPIs)—are used to protect communities from and limit the adverse health impacts of CBRN attacks, outbreak of infectious disease, and other incidents. The NHSS Implementation Plan provides the guiding actions necessary to protect the Nation from a wide range of threats by creating a comprehensive suite of countermeasures for everyday public health and public health emergencies as well as a coordinated process for using them effectively. This objective encompasses the enhancement of the successful Public Health Emergency Medical Countermeasures Enterprise (PHEMCE) and the range of actions related to enhancing the Nation’s capacity to develop, manufacture, evaluate, and use MCMs and NPIs both for routine public health purposes and during emergencies, from research, to development and acquisition, to effective use or implementation of countermeasures, to assessing the intended and unintended consequences of the countermeasures.

The Nation has made progress in developing and preparing countermeasures through the active involvement of many agencies and organizations. PHEMCE has facilitated and strengthened interaction among Federal stakeholders and between Federal and non-Federal stakeholders. It provides an integrated vision of the entire MCM enterprise, which is necessary to ensure the maximum health benefit and most efficient use of public and private resources.

CDC has invested significantly in procuring and maintaining materiel for the Strategic National Stockpile (SNS), the Nation’s repository of antibiotics, vaccines, antidotes, antitoxins, and other critical medical equipment and supplies. Local, state, tribal, and territorial capacity to receive, distribute, and dispense MCMs has improved since 2009. Such programs as the CDC Division of State and Local Readiness provide distribution and dispensing technical assistance, while the Cities Readiness Initiative (CRI) provided funding and technical assistance to local, state, tribal, and territorial health departments.

Supply Chain Integrity and Security Core Capability

Federal partner efforts centered on this objective support the Supply Chain Integrity and Security core capability and the associated critical task of analyzing supply operation dependencies through the priority to expand and improve the national capacity to research, develop, manufacture, obtain, distribute, and dispense medical countermeasures. Within this priority, Federal partners will develop a coordinated communication approach that shares timely and accurate information on supply and the challenges associated with the production and dissemination of emerging and existing MCMs, specifically if the product is in limited supply and high demand. Federal partners will also develop strategies to maintain, and where appropriate, expand, advanced development pipelines replete with medical countermeasures and platforms to address unmet public health needs, emphasizing innovation, flexibility, multipurpose and broad spectrum application, and long-term sustainability.

Physical Protective Measures Core Capability

In support of the Physical Protective Measures capability, Federal partners will develop an agile, robust, and sustainable U.S. manufacturing infrastructure capable of rapidly producing vaccines and other biologics against pandemic influenza and other emerging threats. Federal partners will also create or sustain overarching capabilities to rapidly mature promising candidate drugs, vaccines, therapeutics, and diagnostics using public-private ventures and other collaborative opportunities. The intersection of the Physical Protective Measures core capability and Supply Chain Integrity and Security core capability involves NPIs. The availability and efficiency of physical protective measures like medical countermeasures will be enhanced, and NPIs can ensure supply chain security.

The objective addresses this through the priority to focus research and translation on NPIs. Within this priority, Federal partners will and academia can identify situations through research and evaluation in which NPIs can be prioritized because of delay in MCM production or when MCMs are determined to be infeasible.

NHSS Strategic Objective 3: Ensure Comprehensive Health Situational Awareness (HSA) to Support Decision Making Before Incidents and During Response and Recovery Operations

National situational awareness includes all sectors and relevant actors nationally and globally across the Prevention, Protection, Mitigation, Response, and Recovery mission areas and uses a process that involves an active, continual, and timely information-gathering loop that relies on existing assets, networks, and systems. Active and timely situational awareness provides the foundation for decisions and actions that, in turn, can result in better resource utilization, successful prevention and mitigation of emerging threats, and improved security for the Nation. HSA contributes to overall situational awareness by providing information that includes data regarding health threats, population health, health system and human services resources, health-related response assets, and other considerations to inform decision making.

Intelligence and Information Sharing Core Capability

Improving HSA and data-sharing with respect to integrating human health, environmental, zoonotic, and other relevant information to mitigate immediate-, short-, and long-term health effects is a priority in Strategic Objective 3 that corresponds with critical tasks related to the Intelligence and Information Sharing core capability. By developing HSA processes that actively gather information about resource allocation, risk analysis, forecasting, response, and other actions that might affect health security, decision makers will have the support needed before incidents and during response and recovery operations. The breadth of the collected information needs to include not only health-related data but also non-health-related data that may be required to make sound operational decisions (e.g., transportation data, power-grid status, active intelligence from law enforcement, real-time weather and climate information). Federal partners will work with local, state, tribal, and territorial stakeholders to innovate and improve functional compatibility of their systems across all sectors and among all levels of government. State health departments can work with professional associations to conduct an inventory of regional health information organizations (RHIO) and electronic health information exchanges (HIEs) and determine the potential for inclusion in a national HSA capability. Higher education centers can develop partnerships, curricula, and cross-degree programs (e.g., joint public health and veterinary medicine degrees) to aid in developing a workforce that understands the language of human, animal, and environmental health. Local, state, tribal, and territorial health, environment, law enforcement, and agriculture agencies can strengthen joint health, intelligence, agricultural, and law enforcement capabilities for prevention and mitigation of animal or human disease incidents.

Cybersecurity Core Capability

The growth of social media not only increases opportunities for individuals and organizations to connect with each other and to access and use information, but also facilitates the spread of potentially dangerous rumors and misinformation—with significant consequences for public health. To address these communication challenges, health security leaders and other stakeholders must ensure proper cybersecurity, understand how to frame communications effectively, and know how to optimally manage and use social media as sources of “big data,” especially with respect to differentiating useful and erroneous information. Federal partners will conduct cybersecurity risk assessments of healthcare systems, with the goal of developing contingency plans for continuity of

operations in the event of a cyber incident that leverages existing cybersecurity risk assessment resources.

NHSS Strategic Objective 4: Enhance the Integration and Effectiveness of the Public Health, Healthcare, and Emergency Management Systems

Communities are making contributions to national health security every day. For example, the Public Health Emergency Preparedness (PHEP) and the Hospital Preparedness Program (HPP) cooperative agreements, administered by HHS' CDC and ASPR, respectively, are key Federal investments in national health security. The programs provide both financial and technical assistance to help awardees strengthen public health and medical response systems and enhance community preparedness.

Emergency services involve first-responder organizations that have the specialized training and equipment to support a national-level health incident through response, treatment, or stabilization, transportation through fire services and EMS, and decontamination of personnel and equipment through hazardous material services. Components of the emergency management system are also essential to establishing and maintaining incident command and incident management operations. A skilled workforce is the foundation of these systems. The workforce is made up of paid and volunteer staffs employed by governments and other organizations, as well as interim employees, volunteers, and bystanders who just happen to be at the scene of an incident and seek to contribute.

The integration of utilities (such as power, water, and wastewater) public health, healthcare, and emergency management systems means that they can work together day to day, mutually supporting one another so that they can seamlessly scale up to handle increased requirements or demands during the mitigation, response, and recovery phases of the incident life cycle.

Alignment of the PHEP and HPP programs has included such efforts as working with a common set of preparedness capabilities, aligning the grant application process, and use of common performance indicators that support the implementation of national health security initiatives.

Supply Chain Integrity and Security Core Capability

Protecting key assets, infrastructures, and support systems through risk management principles is one of the critical tasks for this capability and requires investments prior to an emergency. The NHSS also calls for partners to build upon and improve routine systems and services as a foundation for incident response and risk reduction, focusing on common elements that leverage the alignment of routine capabilities with those needed during an incident. Federal partners will work with non-Federal stakeholders (e.g., Joint Commission) to support the widespread application of principles of disaster risk reduction and mitigation.

NHSS Strategic Objective 5: Strengthen Global Health Security

The health of the American people and that of the people around the world are more closely linked than ever before. Greater movement of people, animals, and goods across international borders increases the risk of exposure to health threats originating outside one's own country. In such an interconnected environment, the best way for a country to protect its population is to prevent a health threat from emerging and spreading in the first place. By working together with international partners to develop global capacities and operational capabilities to prevent epidemics, detect threats early, rapidly respond to incidents, and support integrated recovery efforts, the United States will also protect the health of the American people from global health security threats.

The USG uses a variety of mechanisms to strengthen national and global health security. Domestically, several national strategies highlight U.S. health security, including the National

Strategy for Countering Biological Threats, the National Strategy for Pandemic Influenza, the National Strategy for Combating Antibiotic-Resistant Bacteria, and the National Strategy for Biosurveillance.

On an international level, the United States works within multiple bilateral and multilateral agreements and frameworks to protect the American people from global health security threats. USG agencies, including CDC, DOD, DOS, USAID, and others, are supporting implementation and advancement of the Global Health Security Agenda to help countries improve capacity to prevent, detect, and respond to infectious disease threats. For example, the United States is a signatory to the 2005 International Health Regulations (IHR), a legally binding agreement among 196 state parties, which obligates member states to develop and maintain the capability to detect, assess, notify, and respond to public health threats, especially those of international concern. Under the IHR, the USG works both domestically and internationally to ensure that health security capabilities are in place. The United States is also a party to the Global Health Security Initiative, an international partnership that arose in the immediate aftermath of the 2001 terrorist attacks among like-minded countries to strengthen health preparedness and response globally, encompassing CBRN threats and pandemic influenza. The North American Plan for Animal and Pandemic Influenza and the health security work under the U.S.-Canada Beyond the Border initiative are other examples of regional efforts in which the United States plays a part to promote global health security.

Interdiction and Disruption Core Capability

Strengthening national capacities and capabilities globally to prevent the global spread of public health threats and diseases is a global health security priority.

Screening, Search, and Detection Core Capability

Detection is an important aspect of national health security that should not be understated. Detection refers to the timely identification of a threat or incident with negative health consequences. Strengthening national capacities and capabilities globally to detect diseases in a timely manner is a priority contributing to critical tasks of the Screening, Search, and Detection capability. Specific, related actions are strengthening laboratory systems, linking regional and global networks for biosurveillance, improving sample sharing, and improving global efforts to develop and widely deploy novel diagnostics.

Supply Chain Integrity and Security Core Capability

Federal partners and the private sector will help provide or improve training for supply chain professionals.

Coordination Structures

Health Security is a complex Protection activity requiring extensive Federal coordination. The main Health Security coordinating structures include:

- **DHS NOC**
The DHS NOC, which operates 24 hours a day, seven days a week, and 365 days a year, coordinates information sharing to help deter, detect, and prevent terrorist acts and to manage domestic incidents. Information on domestic incident management is shared with Emergency Operations Centers at all levels through the Homeland Security Information Network (HSIN).
- **FEMA NWC**

The FEMA NWC's mission is to maintain uninterrupted, 24-hour-a-day, 365-day-a-year situational awareness of FEMA response capabilities, readiness postures, and all incidents and special events—natural or manmade—that may require a coordinated Federal disaster response. Through a variety of formal presentations and written reports, the NWC provides shared situational understanding aimed at supporting effective decision making at all levels—from the local emergency manager to the President of the United States. Additionally, the NWC plays a critical role in coordinating the rapid deployment and management of national emergency response teams and resources in response to disasters, special events, field operations, and other incidents as required.

- HHS Secretary's Operations Center (SOC)

The HHS SOC serves as the central HSA hub through which HHS monitors public health and medical indicators and warnings, both domestically and internationally, and coordinates integrated response and recovery operations related to ongoing incidents of public health significance. The SOC maintains HSA on a 24-hour-a-day, 365-day-a-year basis and oversees all phases of the information management process, including collection, analysis, integration, and dissemination. Dissemination of information is conducted under a phased reporting structure that mirrors the structure used by the DHS NOC and the FEMA NWC and allows for the sharing of information with both internal and external partners. Additionally, the SOC works with other local, state, tribal, territorial, and Federal operations centers to share information and coordinate appropriate responses for public health and medical consequences. The SOC works internally to coordinate all department and agency activities across the HHS spectrum.

Support to Other Coordinating Activities

The Health Security coordinating activity provides support to the other *coordinating activities* in a variety of ways:

- It supports **Border Security** through health security activities that provide information and intelligence to support border-based screening and detection of health security threats.
 - Border security activities can play a key role in supporting quarantine, tracking, and monitoring efforts to reduce potential public health risks.
 - This includes sharing key information on potential hazards and threats, indicators, and symptoms to watch for.
 - Border security teams share information on potential health security threats they encounter or track.
- It supports **Critical Infrastructure Security and Resilience** through the work supporting the critical infrastructure sectors.
 - Healthcare and Public Health is a critical infrastructure sector.
 - HHS is the SSA for this sector.
- It supports **Defense Against WMD Threats** through health security activities that share information on potential threats and help gauge the potential impact of WMD.
 - These include coordination to help identify potential risk factors that could exacerbate a WMD incident.
- It supports **Immigration Security** efforts by ensuring public health is maintained during activities related to immigration.

- Information sharing and coordination activities to maintain situational awareness of potential risk factors presented during immigration activities include potential pathogen exposure or disease monitoring, identification of necessary public health resources, and tracking and monitoring for particular symptoms.
- This is particularly important to ICE Enforcement and Removal Operations (ERO), which works with the interagency to coordinate the planning and response to unexpected migration crises, and is responsible for the custody and removal of priority aliens.
- To this end, the Public Health Service (PHS) assists in the guidance of health policy regarding the custody of unaccompanied children and assists in providing health services to all detainees in ICE custody. The safe care and custody of unaccompanied children, whom DHS transfers to the custody of HHS, and ICE detainees is viewed as promoting the health, safety, and well-being of the American public.
- It supports **Maritime Security** efforts by coordinating information and threat-hazard sharing to combat the introduction of hazardous agents that could introduce public health challenges into the United States.
 - The USCG supports and assists the CDC in carrying out quarantine regulations.
- It supports the **Protection of Key Leadership and Special Events** by ensuring the protection of sufficient health capacity to effectively address any challenges.
 - Information sharing supports preparedness to address any potential incidents, safeguard against the introduction of any public health threats during a major event, and provide sufficiently robust health services during the event.
 - Information sharing should also ensure that parties are fully aware of potential interdependencies and changes in the risk picture in the planning and delivery of operations during a major event that may place unique stressors on existing health infrastructure.
 - State and local disability organizations can serve as subject matter experts and connect protection officials to local people with disabilities and others with access and functional needs.
- It supports **Transportation Security** efforts through intelligence and information sharing of relevant health security information that helps transportation officials monitor for potential health sector risks and threats as people and goods pass through transportation sector operations.
 - That information sharing also includes notifications from health officials to transportation officials to ensure they maintain situational awareness on any public health risks that could endanger the effective operation of the transportation sector.

Support from Other Coordinating Activities

The Health Security coordinating activity receives support from the other *coordinating activities* in a variety of ways:

- It gets support from **Border Security** by maintaining awareness of health security priorities, information and intelligence to support border-based screening and detection of health security threats.

- It provides support during humanitarian crises, for example, by assessing health, safety, and security of at-risk populations, such as unaccompanied children along the southwest U.S. border.
- It gets support from **Critical Infrastructure Security and Resilience** by supporting the SSA, as delineated by NIPP 2013.
 - HHS serves as the SSA for the Healthcare and Public Health Sector (HPH Sector), supporting the public-private partnership focused on enhancing the HPH Sector’s security and resilience.
 - This includes managing risks, promoting cybersecurity, sharing information, and coordinating response and recovery efforts.
- It gets support from **Defense Against WMD Threats** by developing medical countermeasures and nonpharmaceutical interventions to protect communities from, and limit the adverse health impacts of, WMD threats.
 - It also shares intelligence and health information to protect against threats.
- It gets support from **Immigration Security** by leveraging public health systems to share information and intelligence and support immigration activities as needed.
- It gets support from **Maritime Security** through the USCG, which works with HHS to quarantine ships suspected of being a health hazard.
- It gets support from **Protection of Key Leadership and Special Events** through public health monitoring that includes systematic examinations and assessments, sensor technologies, disease surveillance, laboratory testing, or physical investigation and intelligence.
- It gets support from **Transportation Security** through coordination and information sharing.
 - Transportation systems and assets support public health as a lifeline function on which public health systems depend.
 - Transportation Systems Sector assessments of public health and safety identify potential threats or risks that impact transportation protection measures. They support risk management information sharing that addresses public health and pandemic threats to determine potential impacts to transportation systems.

Support to Other Mission Areas

The National Preparedness Goal, developed within the National Preparedness System to strengthen our Nation’s security and resilience, outlines core capabilities organized into the five mission areas (Prevention, Protection, Mitigation, Response, and Recovery). The NHSS drives actions that communities must take to address five key mission areas before, during, and after an incident. These mission areas align with those found in the National Preparedness Goal. Moreover, the NHSS follows these strategies, policies, and doctrine and supports their overarching objectives.

Key Plans

- NHSS and Implementation Plan 2015–2018
- Public Health and Medical Situational Awareness Strategy and Implementation Plan
- PHEMCE Implementation Plan

- HHS All Hazards Plan.

Key Authorities and References

The following laws, policy directives, strategies, and EOs are included in addition to the general authorities/references provided in the base plan for the Health Security Coordinating Activity.

- Pandemic and All-Hazards Preparedness Act
- Pandemic and All-Hazards Preparedness and Reauthorization Act
- Public Health Service Act.

Appendix 5 to Annex C: Immigration Security

Purpose

In support of national preparedness, the Nation's immigration system secures America's promise and responds rapidly to changes and demand for immigration services by providing accurate and useful information to customers, granting immigration and citizenship benefits, promoting awareness and understanding of citizenship, and ensuring the integrity, safety, and security of the process. The Federal Government protects national security, public safety, and the integrity of our borders through the criminal and civil enforcement of Federal law governing border control, customs, trade, and immigration.

Scope

This appendix includes only the Federal *coordinating activities* for Immigration Security. It specifically includes the Federal coordinating structures and mechanisms required to deliver the Protection core capabilities and achieve Immigration Security objectives. While Immigration Security efforts overlap with Border Security efforts, these *coordinating activities* are distinct and are addressed in separate Protection FIOP appendices.

Objectives

This appendix will accomplish the following:

- Provide a concept of operations for integrating existing Federal capabilities to secure the Nation's immigration system.
- Describe Federal operational coordination mechanisms that integrate resources and personnel for Immigration Security.
- Lay the foundation for further department or agency Immigration Security planning, including integration among *coordinating activities*.

Concept of Operation

The Federal Government protects America and promotes national security, public safety, and the integrity of U.S. borders through criminal and civil enforcement of Federal law governing border control, customs, trade, and immigration. This objective will be achieved by prioritizing efforts toward the first four homeland security missions identified in the DHS QHSR. These are:

- **Prevent Terrorism and Enhance Security.** The Federal Government's objective is to identify, investigate, and interdict threats as early as possible to protect against terrorist attacks against the United States before they materialize. To address these vulnerabilities, DHS works in coordination with the Departments of State, Defense, Justice and others to prevent the entry of people and materials that pose a threat to national security, investigate and arrest or remove suspected terrorists or their supporters from the United States, and prevent the export of weapons and sensitive technologies that could be used to harm the Nation, the population, and allies.
- **Secure and Manage our Borders to protect against Illicit Trade, Travel, and Finance.** The Federal Government will develop a layered approach to border security that focuses on minimizing disruption to and facilitating safe and secure inbound and outbound legal flows of people and goods and prioritizing efforts to counter illicit finances, travel, and trade through targeted interdiction and other activities, while continuing to increase efficiencies in operations.

- **Enforce and Administer the Immigration Laws of the United States** by protecting against the unlawful entry of aliens and arresting, detaining, and removing criminals, fugitives, and other dangerous foreign nationals from the United States, while promoting the integration of lawful immigrants into American society. This mission includes actions overseas, at and between POEs, and throughout the interior of the United States. The Federal Government will also pursue an effective worksite enforcement and student visa program to reduce the incentive for aliens to enter the U.S. and remain unlawfully.
- **Safeguard and Secure Cyberspace.** The Federal Government will develop a collaborative approach to work with sector partners to strengthen cybersecurity protections, investigate those who engage in cybercrime, and take full advantage of technological innovations in machine intelligence and communications that enhance detection and security. The DHS will also promote security and risk reduction approaches that are driven by the needs of our stakeholders, provide assistance to impacted entities, coordinate the national response to significant cyber incidents, and investigate those responsible in conjunction with other law enforcement partners.

Roles and Responsibilities

Immigration Security requires a unity of effort throughout the Federal Government. Several departments and agencies play a critical role in protecting national security, public safety, and the integrity of our borders through the criminal and civil enforcement of Federal law governing border control, customs, trade, and immigration. These departments and agencies include:

- DHS
- CBP
- ICE
- USCG
- USCIS
- DOS
- DOJ
- HHS
- ATF
- FBI
- FLETC
- DOS.

Each of these Federal partners supports the delivery of the Protection core capabilities required for Immigration Security. The table below describes how the Federal Government delivers each Protection core capability in the Immigration Security mission space.

Table 19: Immigration Security Core Capabilities Critical Task Summary

Core Capability	Immigration Security Critical Task Summary
Access Control and Identity Verification	<ul style="list-style-type: none"> ▪ Control and limit access to critical locations and systems. ▪ Support verification efforts to authorize, grant, or deny physical and cyber access to key assets.
Intelligence and Information Sharing	<ul style="list-style-type: none"> ▪ Set requirements for intelligence and information sharing across all sectors. ▪ Establish intelligence and information sharing processes between stakeholders at all levels of government and key international and private sector partners to share threat information, advisories, attack indicators, and corrective measures that can help address immigration security issues. ▪ Monitor, detect, and analyze threats to public safety, health, and security that could be introduced through the immigration system and work to develop education and awareness programs to help address those threats. ▪ Use intelligence and information to provide routine support for protection measures, training, and exercises for immigration security stakeholders.
Interdiction and Disruption	<ul style="list-style-type: none"> ▪ Deter movement of terrorists into and within the U.S. and disrupt financing and logistical support from reaching potential threats in the U.S. ▪ Ensure the capacity to detect CBRNE threats during immigration security screenings and resolve those threats prior to reaching their targets. ▪ Interdict conveyances, cargo, and persons to mitigate the spread of public health threats, CBRNE materials, and other threats to U.S. security. ▪ Coordinate with local, state, tribal, and territorial personnel and other Federal officials to address any threats identified by or detected within the immigration security system. ▪ Focus on smart and effective immigration enforcement, which prioritizes the removal of convicted criminal aliens, threats to national security, recent border crossers, illegal re-entrants, those who have significantly abused the visa or visa waiver program, and immigration fugitives, utilizing the latest technology through coordination with science and technology on all fronts.
Screening, Search, and Detection	<ul style="list-style-type: none"> ▪ Provide active screening and surveillance of people, baggage, mail, cargo, and conveyances to detect and identify any potentially threatening materials or persons using CBRNE detection, biosurveillance, and screening for health threats. ▪ Support intelligence and information sharing to help stakeholders identify potential threats and capability gaps, including coordinating local, state, tribal, territorial, and Federal efforts to drive risk assessment and awareness efforts. ▪ Establish coordinated efforts that help develop and train an engaged surveillance network from across all levels of government, the private sector, and the public at large to identify WMD threats. ▪ Support threat assessments, improvements in sensor technologies, testing, and intelligence gathering and analysis to improve national capacity to detect, identify, locate, and address WMD threats and hazards.
Physical Protective Measures	<ul style="list-style-type: none"> ▪ Develop and implement risk-based physical security measures, policies, and procedures, including business continuity plans and physical protective measures needed to safeguard key operational activities and infrastructure. ▪ Develop training and acquisition programs that develop or deliver necessary skills and resources needed to address threats identified by risk assessments of the immigration security system and operations.
Risk Management for Protection Programs and Activities	<ul style="list-style-type: none"> ▪ Develop tools and community capacity for analyzing and assessing threats, risks, and vulnerabilities from threats to or threats detected within the immigration security system. ▪ Gather and share relevant information and deploy that collective information to develop risk assessments that incorporate changes to the physical environment, aging infrastructure, technological developments, and updated data.

Core Capability	Immigration Security Critical Task Summary
	<ul style="list-style-type: none"> ▪ Use risk assessments to develop exercises and other work that can be used to validate and enhance future mitigation projects and initiatives.
Cybersecurity	<ul style="list-style-type: none"> ▪ Implement countermeasures, technologies, and policies to protect physical and cyber assets, networks, applications, and systems that support immigration security efforts. ▪ Safeguard against the introduction of people or materials that could impact the cyber or physical security of cyber assets in the U.S.
Supply Chain Integrity and Security	<ul style="list-style-type: none"> ▪ Develop multilayer defense and planning efforts to safeguard necessary supplies for immigration security operations against asymmetrical and traditional threats. ▪ Use verification and detection capabilities to identify goods that are misrepresented or contaminated and prevent their entry into the U.S. or the U.S. supply chain. ▪ Support detection and identification of people who could pose a threat to supply chain operations or assets by sharing information and coordinating efforts in support of Protection efforts.

- Fraud Detection and National Security Directorate (FDNS):
 - FDNS determines whether individuals or organizations filing for immigration benefits pose a threat to national security, public safety, or the integrity of the Nation’s legal immigration system. Benefits may include adjustment of immigration status (granting lawful permanent residence), naturalization (granting United States citizenship), asylum and refugee status, and other immigrant and nonimmigrant benefits. FDNS officers serve as the primary liaison between USCIS and the law enforcement and intelligence community. These efforts ensure criminals, terrorists, and other individuals who pose a threat to national security and/or public safety are not able to exploit the immigration system to gain access to, or remain in, the United States. In addition, FDNS reviews cases of suspected fraud and where the security vetting process has indicated possible national security or public safety-related concerns. FDNS Immigration Officers are located at all USCIS service centers, field offices, asylum offices, and some overseas offices.
 - The Fraud Detection and National Security Data System (FDNS-DS) is FDNS’ central data repository that FDNS Immigration Officers use to record, track, and manage the background check process related to immigration applications and petitions, as well as information related to beneficiary applications with suspected or confirmed fraud, criminal activity, public safety, and/or national security concerns, and cases randomly selected for benefit fraud assessments.
- NTC-P:
 - Starting with the earliest indications of potential travel, including U.S.-bound travel reservations, Electronic System for Travel Authorization (ESTA) applications, visa applications, passenger and cargo manifests, and continuing through the inspection or arrivals process, the NTC is continually analyzing information gleaned from these sources. At the NTC, CBP leverages all available advance passenger data including Passenger Name Records (PNR) and manifest data from the Advance Passenger Information System (APIS), previous crossing information, intelligence, and law enforcement information, as well as open source data in its antiterrorism efforts. This advanced targeting is designed to interdict high-risk passengers at foreign departure locations before they can board or be loaded on a conveyance destined to the United States. Subsequent to attempted in-flight bombings, CBP re-examined its passenger targeting strategy and as a result re-engineered its operations with a greatly increased emphasis on pre-departure targeting and interdiction.

- A major part of the new targeting emphasis was the creation of the Pre-Departure Program. This targeting program utilizes PNR data and Advance Passenger Information (API), in conjunction with ATS-P, to identify high-risk passengers and/or other inadmissible aliens in an effort to prevent them from boarding commercial carriers bound for the United States from overseas locations that do not have an IAP team presence.
- The IAP and the Joint Security Program:
 - Officers are posted at eleven overseas airports in nine countries whose function is to screen passengers to identify targets referred from NTCP and assist airlines in determining if passengers are legitimate travelers and have the proper documents to enter the United States. IAP officers will recommend that the carrier not board suspect or possible high-risk passengers.
- CBP Regional Carrier Liaison Groups (RCLG):
 - These groups, located in Miami, New York, and Honolulu play an important role in the Pre-Departure targeting program by acting as a conduit between NTC and the airlines when mala fide passengers at overseas departure locations are identified and a denial of boarding request is made by NTC.
 - NTC conducts pre-vetting for Trusted Traveler Programs (TTP) and ESTA applications. The TTP application process includes rigorous vetting and compliance checks, including biographic queries of criminal history databases and an interview process which is tantamount to a border inspection at a POE.
- United States Visitor and Immigrant Status Indicator Technology (US-VISIT):
 - USCIS, CBP, and ICE, in coordinating with NPPD's Office of Biometric Identity Management, cross-check a person's biometrics against a watch list of known or suspected terrorists, criminals, and immigration violators. Those biometrics are also used to determine if a person is using an alias or attempting to use fraudulent identification. This information allows for the establishment, then verification, of a person's identity before crossing U.S. borders.
- USCIS Refugee, Asylum and International Operations (RAIO):
 - USCIS may provide humanitarian relief to foreign nationals who have been persecuted or fear they will be persecuted on account of race, religion, nationality, and/or membership in a particular social group or political opinion. Through coordination with USCIS FDNS, USCIS refugee officers and asylum officers adjudicate applications and ensure applicants do not pose a threat to national security.
- E-Verify:
 - This is an electronic program through which employers verify the employment eligibility of their employees after hire. Employers submit information through E-Verify to the Social Security Administration and USCIS to determine whether the information matches government records and whether the new hire is authorized to work in the United States.
- Visa Hot List:
 - Designed for re-vetting previously issued U.S. visas against lookout records to identify persons whose eligibility for a visa or entry to the U.S. has changed since the issuance of the visa. Matches to such records are referred to DOS for possible visa revocation.

- ICE, the DOS, and NTC-P have developed an automated visa screening process that will enable DHS entities to identify derogatory information relating to visa applicants prior to the adjudication of their application. Screening pre-adjudicated visa applications and Consular Electronic Application Center (CEAC) data by leveraging current IT platforms, such as the ATS-P, will enhance the USG's antiterrorism efforts by adding another layer of security to the visa issuance process and will further extend our borders outward, denying mala fide travelers access to the United States.
- Passenger Analytic Units:
 - Passengers are continually assessed, as they travel by air or sea to the United States, by local Passenger Analytical Units to identify travelers who may be at high risk for customs or immigration violations, such as confirmed overstays, prior removals, prior deportations, and criminal convictions.
 - CBP officers at the POEs inspect all arriving persons to determine identity, alienage, and whether they are subject to the grounds of inadmissibility or removability per Immigration and Nationality Act sub-sections 212(a) and 237(a).
- Criminal Administrative Inquiries:
 - While other specialty units are responsible for advanced review, observation, and interview of targeted travelers encountered at the POEs, the CBP Enforcement Officer conducts criminal and administrative inquiries regarding individuals suspected of criminal activity, to include violations under Title 8 of the U.S. Code. CBP Enforcement Officers conduct follow-up criminal casework as directed by the United States Attorney's Office (USAO) for cases brought by CBP for prosecution, including but not limited to obtaining certified documents needed for criminal court proceedings; arranging for forensic examination of travel documents, cell phones, computers, and electronic documents' participating in debriefs and proffers; and serving subpoenas, warrants, and other official orders. For those persons that require formal determination hearings due to administrative violations of law, the immigration process then proceeds to ICE.
- Other security mechanisms for border protection include:
 - PNR agreement:
 - CBP's IAP; air, land, cyber, and maritime craft/equipment with support command/control structures. The ICE ERO LESC provides real-time information and assistance to local, state, tribal, and territorial LEOs who encounter suspected aliens, fugitives, etc., in the course of their official duties.
 - Organizational risk management analysts and supervisors; MOTR, MACCs, DHS PLCY, and DOJ; training for insider threats.
 - Risk analysis tools; information sharing networks, OCIA; deployed Federal officers, THIRA, JTTFs, MSRAM; NTAS; NTC; DHS/USCG Maritime Security (MARSEC) Levels.
 - Counterterrorism and Criminal Exploitation Unit
 - Export Enforcement Coordination Center.

Coordination Structures

- Counterterrorism and Criminal Exploitation Unit

- Export Enforcement Coordination Center
- USCIS FDNS
- CBP IAP
- ICE ERO LESC
- FLETC
- BIFS
- ACTTs
- GMCC
- DHS JTFs (East, West, Investigations)
- DHS IPTs.

Support to Other Coordinating Activities

The Immigration Security coordinating activity provides support to the other *coordinating activities* in a variety of ways:

- It supports **Border Security** through ICE HSI, which is the investigative arm of ICE and ICE ERO, which focuses its resources on individuals who pose the greatest risk to public safety, national security, and border security within the interior of the United States and those apprehended by CBP at or between POEs.
 - ICE HSI conducts border related investigations for a myriad of offenses involving illicit trade, travel, and finance crossing our borders and the enforcement of certain Federal laws for DHS and on behalf of other government agencies.
 - ICE HSI mission includes narcotics, alien smuggling and human trafficking, contraband smuggling, endangered species smuggling, and bulk cash smuggling.
 - ICE ERO identifies, arrests, and removes aliens who present a danger to national security or are a risk to public safety, as well as those who enter the United States illegally or otherwise undermine the integrity of our immigration laws and our border control efforts.
- It supports **Critical Infrastructure Security and Resilience** through ICE HSI, which conducts insider threat investigations under its Title 8 authorities to identify foreign nationals and aliens employed at critical infrastructure who may pose a threat to national security.
 - HSI also conducts investigations into IPR, trade transparency, money laundering, general smuggling, and cybercrime investigations that cross silos with almost all critical infrastructure sectors.
 - Additionally, ICE HSI conducts sensitive investigations into the counter proliferation and illegal export of nuclear materials, munitions systems, weapons, technology, and other critical manufacturing and defense related industries, as well as investigations into dual use chemicals and compounds imported and exported contrary to law.
- It supports **Defense Against WMD Threats** through ICE HSI special agents, who are assigned to JTTFs in support of the FBI's mission to prevent and protect against terrorist acts.
 - Both CBP and ICE have WMD interdiction programs relating to the illegal import/export of either the precursors or actual WMD and therefore have a significant role in this area.

- HSI manages and operates the Export Enforcement Coordination Center, established by EO 13558, which strengthens the enforcement of U.S. export laws through the facilitation of partner agency communication and collaboration to keep our Nation safe.
- These counter proliferation efforts are executed by detecting, preventing, disrupting, investigating, and prosecuting violations of U.S. export control laws.
- It supports **Health Security** by leveraging public health systems to share information and intelligence and support immigration activities as needed.
- It supports **Maritime Security** efforts through the use of interagency coordination, information sharing, and investigations.
 - HSI has stood up 37 BESTs throughout the Nation, composed of many local, state, and Federal agencies. BEST teams are led by HSI special agents and address a myriad of maritime and transportation security issues, including contraband smuggling, safety violations to aircraft and marine vessels, and security and access to restricted areas at airports/seaports.
 - In coordination with CBP, ICE also conducts investigations related to Customs Broker backgrounds, as well as facilities and physical security inspections of all functional equivalents of the border (FEB) including Customs Bonded Warehouses, Foreign Trade Zones and Container Freight stations.
 - The HSI mission therefore intertwines with several Federal agencies in many areas relating to maritime transportation security.
- It supports the **Protection of Key Leadership and Special Events** through the work of ICE HSI as a secondary agency in support of DHS for this responsibility and provides protection to SEAR 1 and SEAR 2 special events.
- It supports **Transportation Security** efforts through ICE HSI's work as the lead investigative agency for all immigration offences against the United States.
 - HSI has stood up 37 BESTs throughout the Nation, composed of many local, state, and Federal agencies. BEST teams are led by HSI special agents and address a myriad of border related transportation security issues, including contraband smuggling, safety violations to aircraft and marine vessels, and security and access to restricted areas at airports/seaports.
 - In coordination with CBP, ICE also conducts investigations related to Customs Broker backgrounds, as well as facilities and physical security inspections of all functional equivalents of the border (FEB) including Customs Bonded Warehouses, Foreign Trade Zones and Container Freight stations.
 - The HSI mission therefore intertwines with TSA, USCG, and CBP in many areas relating to transportation security.

Support from Other Coordinating Activities

The Immigration Security coordinating activity receives support from the other *coordinating activities* in a variety of ways:

- It gets support from **Border Security** by aligning intelligence to drive border security and immigration security practices for both border and internal immigration security.

- ICE ERO works cooperatively with local, state and federal agencies within the United States to identify, locate, and arrest priority removable aliens and focus on gathering and disseminating intelligence.
- It gets support from **Critical Infrastructure Security and Resilience** by supporting robust national infrastructure across multiple infrastructure sectors, especially Transportation Systems.
 - SSPs and the sector partnership structure support immigration security efforts through planning and strategic assessment.
- It gets support from **Defense Against WMD Threats** through intelligence and information sharing.
- It gets support from **Health Security** efforts by ensuring public health is maintained during activities related to immigration.
 - Information sharing and coordination activities maintain situational awareness of potential risk factors presented during immigration activities, including potential pathogen exposure or disease monitoring, identification of necessary public health resources, and tracking and monitoring for particular symptoms.
 - ICE ERO coordinates with the interagency community on the planning and response to unexpected migration crises and is responsible for the custody and removal of priority aliens.
 - The Public Health Service (PHS) also plays an important role in immigration security by providing health-related guidance for unaccompanied children in HHS custody, and assisting in providing health services to all detainees in ICE custody.
- It gets support from **Maritime Security** through intelligence and information sharing.
- It gets support from **Protection of Key Leadership and Special Events** through intelligence and information sharing.
- It gets support from **Transportation Security** through sharing of key threat and risk information to maintain situational awareness of potential hazards that would impact transportation system operations or security.
 - Immigration facilities are often located at key transportation hubs, including airports, ports, rail stations, and road inspection sites.
 - The sectors also conduct joint assessments to identify potential dependencies and interdependencies caused by those co-locations.
 - Immigration Security assets also provide updated information that supports passenger and cargo screening efforts on transportation systems.

Support to Other Mission Areas

Starting with the earliest indications of potential travel, including U.S.-bound travel reservations, ESTA applications, visa applications, passenger manifests, and continuing through the inspection or arrivals process, the NTCP is continually analyzing information gleaned from these sources using CBP's ATS. ATS is a decision support tool for CBP officers that compares information on travelers arriving in, transiting through, and exiting the country against law enforcement and intelligence databases to identify individuals that require additional scrutiny. This information is also matched against targeting rules developed by CBP subject matter experts. Targeting rules are based on actionable intelligence derived from current IC reporting or other law enforcement information

available to CBP. NTCP analyzes each traveler's risk before departure to identify possible matches to the USG's consolidated terrorist watch list, Interpol lost and stolen passports, criminal activity, fraud, or otherwise mala fide travelers, including U.S. citizens.

Through direct networks with commercial airlines, including CBP RCLGs and connections to CBP officers overseas as part of the IAP, NTCP officials are able to issue no-board recommendations to the airlines to keep suspected high-risk passengers from traveling to the United States. The NTCP vetting process for international passengers continues even while the flight is en route to the United States to identify any travelers who, although they may not be national security risks, may need to be referred for a more thorough inspection at the first POE upon arrival in the U.S. for other potential violations.

A major part of the new targeting emphasis was the creation of the Pre-Departure Program. This targeting program utilizes PNR data and API, in conjunction with ATS-P, to identify high-risk passengers and/or other inadmissible aliens in an effort to prevent them from boarding commercial carriers bound for the United States from overseas locations that do not have an IAP team presence.

The IAP and the Joint Security Program have officers posted at eleven overseas airports in nine countries whose function is to screen passengers to identify targets referred from NTCP and assist airlines in determining if passengers are legitimate travelers and have the proper documents to enter the United States. IAP officers will recommend that the carrier not board suspect or possible high-risk passengers.

The LESC serves as a single national point of contact that provides timely immigration status, identity information, and real-time assistance to local, state, and Federal law enforcement agencies regarding aliens suspected, arrested, or convicted of criminal activity. The LESC protects and defends the United States by sharing timely and relevant ICE information with law enforcement partners around the world. The LESC serves as a national enforcement operations center, responding to inquiries from local, state, and Federal criminal justice agencies concerning aliens under investigation or arrest. The LESC operates 24 hours a day, 7 days a week, and 365 days a year. The primary users of the LESC are local, state, and Federal LEOs seeking information regarding aliens encountered in the course of their daily enforcement activities. During Fiscal Year 2015, the LESC processed 1,465,900 Immigration Alien Queries (IAQ) in support of local, state, tribal, Federal, and international law enforcement agency requests for information.

CBP RCLGs in Miami, New York, and Honolulu play an important role in the Pre-Departure targeting program by acting as a conduit between NTC and the airlines when mala fide passengers at overseas departure locations are identified and a denial of boarding request is made by NTC.

NTC conducts pre-vetting for TTPs and ESTA applications. The TTP application process includes rigorous vetting and compliance checks, including biographic queries of criminal history databases and an interview process which is tantamount to a border inspection at a POE.

The Visa Hot List is designed for re-vetting previously issued U.S. visas against lookout records to identify persons whose eligibility for a visa or entry to the U.S. has changed since the issuance of the visa. Matches to such records are referred to DOS for possible visa revocation.

ICE, DOS, and NTCP have developed an automated visa screening process that will enable DHS entities to identify derogatory information relating to visa applicants prior to the adjudication of their application. Screening pre-adjudicated visa applications and CEAC data by leveraging current IT platforms, such as the ATS-P, will enhance the USG's antiterrorism efforts by adding another layer of security to the visa issuance process and will further extend our borders outward, denying mala fide travelers access to the United States.

The Student and Exchange Visitor Information System (SEVIS) collects, maintains, analyzes, and provides information so only legitimate foreign students or exchange visitors can gain entry into the United States, while protecting the Nation's security. The result is an easily accessible information system that provides timely information to DOS, CBP, USCIS, and ICE, as well as a number of other Federal law enforcement agencies who have a vested interest in F, M and J visa-holding nonimmigrants.

The ICE Mutual Agreement between Government and Employers (IMAGE) program was created in 2006 to minimize vulnerabilities that help unauthorized workers gain unlawful employment. The goal of the IMAGE program is to reduce the employment through outreach, education, and training. Participating in the IMAGE program reduces unauthorized employment and minimizes the use of fraudulent identity documents. It also protects workforce integrity by helping to ensure employees are who they represent themselves to be. Improving company hiring practices will help avoid negative exposure due to unauthorized workers in the workplace and as a result will create an enhanced corporate image.

The ICE ERO Criminal Alien Program (CAP) provides ICE-wide direction and support in the biometric and biographic identification, arrest, and removal of priority aliens who are incarcerated within local, state, and Federal prisons and jails, as well as at-large criminal aliens who have circumvented identification. It is incumbent upon ICE to ensure that all efforts are made to investigate, arrest, and remove individuals from the United States that ICE deems priorities by processing the alien expeditiously and securing a final order of removal for an incarcerated alien before the alien is released to ICE custody. The identification and processing of incarcerated criminal aliens before release from jails and prisons decreases or eliminates the time spent in ICE custody and reduces the overall cost to the Federal Government.

Additionally, integral to the effective execution of this program is the aggressive prosecution of criminal offenders identified by ERO officers during the course of their duties. ERO, in conjunction with the Offices of the United States Attorneys, actively pursues criminal prosecutions upon the discovery of offenses of the nation's criminal code and immigration laws. This further enhances public safety and provides a significant deterrent to recidivism.

The ICE ERO National Fugitive Operations Program (NFOP) is responsible for the identification, location, and arrest of at-large criminal and previously removed aliens. The 129 Fugitive Operations Teams (FOT) prioritize cases on those aliens who pose a serious threat to national security and community safety, including members of transnational street gangs, child sex offenders, and aliens with prior convictions for violent crimes. ERO also prioritizes the apprehension and removal efforts of convicted criminal aliens through a coordinated effort with state and local probation and parole offices.

Key Plans

- Counter-Proliferation Investigations Program
- Illicit Pathways Attack Strategy
- Law Enforcement Assistance Corner
- Project Shield America
- Visa Security Program.

Key Authorities and References

- Homeland Security Act of 2002 (Public Law 107–296), as amended

This page intentionally left blank.

Appendix 6 of Annex C: Maritime Security

Purpose

Maritime Security is a subsector or mode of the Transportation Systems Sector, one of the sixteen critical infrastructure sectors established by PPD-21: Critical Infrastructure Security and Resilience (PPD-21). USCG is the lead component in DHS for maritime homeland security and is the designated SSA for the maritime transportation mode.

The modal focus is upon our Nation's maritime transportation system, which is formally titled the Marine Transportation System (MTS) by the 2008 DOT National Strategy for the MTS. The MTS consists of waterways, ports, and intermodal landside connections that allow the various modes of transportation to move people and goods to, from, and on the water. The MTS includes the following: 25,000 miles of navigable channels; 238 locks at 192 locations; Great Lakes and St. Lawrence Seaway; over 3,700 marine terminals; and over 1,400 designated intermodal connections.³⁶ Ninety-nine percent of the volume of overseas trade (62 percent by value) enters or leaves our Nation by ship. The MTS includes approximately 70 deep-draft port areas along U.S. coasts. Approximately 40 of those ports each handle 10 million tons or more of cargo per year. Most of these terminals are owned by port authorities and are operated by the private sector. Maritime critical infrastructure includes facilities, structures, systems, assets, or services so vital to the port area and its economy that their disruption, incapacity, or destruction could potentially have a debilitating impact on defense, security, the environment, long-term economic prosperity, public health, or the safety of the port.³⁷

Elements of the MTS include marine terminals and their associated berths, which are often specialized to serve specific types of cargo or passenger movements. Terminals handling bulk cargo such as petroleum, coal, ore, and grain are frequently located outside the boundaries of organized public port authorities. These facilities are often the origin and destination points for bulk commodities and thus differ from terminals often found in public ports, where shipments are transferred from one transportation mode to another. Terminals handling containerized cargo tend to be located within larger public port complexes with significant warehousing, storage, and intermodal transportation connectivity. The U.S. Exclusive Economic Zone contains offshore facilities used for U.S. crude oil and natural gas production. These "intermodal" facilities are a key component of the Energy Sector but are also inextricably linked to the maritime transportation mode of the Transportation Systems Sector.

Vessels of all types, sizes, descriptions, and capabilities are also key elements of the MTS. An estimated 17 million small vessels—both commercial and recreational—use the MTS. These vessels operate in close proximity to larger vessels and critical infrastructure. Major classes of oceangoing vessels are tankers, container ships, dry bulk and general cargo freighters, and specialized ships such as the roll-on/roll-off carriers used to transport motor vehicles. Cruise ships are elements of the MTS that serve the recreation and tourism industries and operate on a regular basis from U.S. ports. Ferries of varying sizes carry automobiles, trucks, and passengers that are received from or passed to other transportation modes.

³⁶ MARAD 2012 web site fact sheet.

³⁷ 33 C.F.R. § 101.105, Navigation and Navigable Waters.

Although the deep oceans are the primary means of moving cargo internationally, the U.S. inland river, coastal, and Great Lakes waterways are critical for moving cargo domestically and for providing outbound feeder traffic for overseas shipping:

- **Inland River Systems.** By far the largest and busiest inland waterway system in our Nation is the Mississippi River system, which includes the Ohio River, the Illinois River, the Missouri River, and their tributaries. This system extends for more than 12,000 miles and encompasses navigable waterways on more than a dozen lesser tributary systems passing through numerous States to the Gulf of Mexico. Barges are loaded and unloaded at shallow-draft terminals situated along the riverbanks. There are more than 1,800 shallow-draft terminal facilities in the United States.
- **Coastal and Intracoastal Waterways.** The main coastal shipping activity in the United States occurs along the Gulf coast and, to a lesser extent, along the Atlantic coast. The Atlantic Intracoastal Waterway, which is maintained by the U.S. Army Corps of Engineers (USACE), extends from Norfolk, Virginia, to Miami, Florida, and offers pleasure boaters and commercial shippers with a protected inland channel. The Gulf Intracoastal Waterway, which is maintained by the USACE, spans 1,300 miles from Texas to Florida and is used for moving grain, coal, refinery products, and chemicals domestically and for supplying feeder traffic to seaports.
- **Great Lakes System.** Approximately 350 terminals are situated along the U.S. shoreline of the Great Lakes. A half-dozen lake ports, including Duluth–Superior, Chicago, Detroit, and Cleveland, rank among the top 50 U.S. ports in terms of tonnage. The terminals in these ports, as well as most others on the Great Lakes, primarily handle dry bulk cargo, led by iron ore, grain, coal, sand, stone, and lumber. Access to and transit within the Great Lakes system requires close international cooperation with Canada and a critical dependency upon the St. Lawrence Seaway.
- **Arctic System.** The potential effects of climate change on ice free days have resulted in an increased focus on development in the Arctic region and associated MTS. The U.S. Arctic from the Bering Strait northward, at the present time, lacks the infrastructure and resources to support the Arctic MTS beyond its current demand. The USCG and its Federal and international partners are conducting studies to support a potential expansion of the use of the Arctic that will require a detailed risk-based security assessment and other resilience efforts.
- **America’s Marine Highways.**³⁸ The Secretary of DOT has designated specific navigable waterways that have demonstrated the ability to provide additional capacity to relieve congested landside routes serving freight and passenger movement. The America’s Marine Highway Program is a U.S. Maritime Administration (MARAD)-led initiative to expand the use of the MTS while relieving landside congestion and reducing carbon emissions. The program is designed to integrate America’s Marine Highways into the Nation’s surface transportation system (highways/freight rail), providing seamless transition across all modes by leveraging marine services to complement landside surface transportation routes. America’s Marine Highways consist of over 29,000 nautical miles of navigable waterways including rivers, bays, channels, the Great Lakes, Saint Lawrence Seaway System, and coastal routes. The America’s Marine Highway system is a robust and efficient means of moving freight in terms of cost per ton-mile, and yet it is the most underutilized of our transportation modes.

³⁸ MARAD 2012 web based Fact Sheet, America’s Marine Highways.

Scope

This appendix focuses only on the Federal *coordinating activities* for Maritime Security. It specifically includes the Federal coordinating structures and mechanisms required to deliver the Protection core capabilities and achieve Maritime Security objectives.

Objectives

This appendix will accomplish the following:

- Provide a concept of operations for integrating existing Federal capabilities in Maritime Security.
- Describe Federal operational coordination mechanisms that integrate resources and personnel for Maritime Security.
- Lay the foundation for further department or agency Protection planning for Maritime Security, including integration among *coordinating activities*.

Concept of Operations

As the DHS-designated lead for the maritime mode of the Transportation Systems Sector,³⁹ the USCG promotes alignment and coordination of risk reduction programs and activities with modal partners. A variety of risk mitigation activities address scenarios across the risk spectrum. The USCG and its Federal and international partners have extensive statutory authority, presence, command and control capability, and experience in maritime safety and security.

Roles and Responsibilities

Maritime Security requires a unity of effort throughout the Federal Government. Several departments and agencies play a critical role in safeguarding our Nation's waterways, ports, and intermodal landside connections. These departments and agencies include:

- USCG
- DHS IPTs
- CBP
- DHS
- FLETC
- DOD
- DOJ
- DOT
- ICE
- DOS.

Each of these Federal partners supports the delivery of the Protection core capabilities and the continued defense of our Nation's waterways, ports, and intermodal landside connections. The table below describes how the Federal Government delivers each Protection core capability in Maritime Security.

³⁹ NIPP 2013.

Table 20: Core Capabilities Critical Task Summary

Core Capability	Critical Task Summary
Intelligence and Information Sharing	<ul style="list-style-type: none"> ▪ The National Maritime Intelligence Center allows for the synthesis of real time maritime information and intelligence regarding threats to U.S. ports and vessels
Interdiction and Disruption	<ul style="list-style-type: none"> ▪ The USCG drug interdiction, migrant interdiction and PWCS activities provide a layered approach that support border security and immigration security.
Screening, Search, and Detection	<ul style="list-style-type: none"> ▪ Robust maritime screening processes and initiatives, including the CSI, identify potential threats and alerts.
Physical Protective Measures	<ul style="list-style-type: none"> ▪ Physical measures and countermeasures throughout the maritime system enhance the maritime security regime framework.
Risk Management for Protection Programs and Activities	<ul style="list-style-type: none"> ▪ A layered, risk-based approach is designed to detect, deter, and disrupt threats and provide resilience through the maritime security system.
Cybersecurity	<ul style="list-style-type: none"> ▪ Vessel navigation and related infrastructure and services are dependent on cyber- and communications-supported systems managed by various public and private owners and operator.
Supply Chain Integrity and Security	<ul style="list-style-type: none"> ▪ Maritime supply chain and global supply chain security are reflected in AMSP and operations.

The USCG will lead its maritime security partners to conduct the legislated PWCS mission⁴⁰ to prevent, protect against, respond to, and recover from terrorist attacks, sabotage, espionage, or subversive acts in the maritime domain and the MTS. PWCS includes the establishment and oversight of Maritime Security Regimes, employment of MDA, and the execution of MSRO activities.

The DOT serves as a co-SSA for the Transportation Systems Sector and coordinates with a broad base of stakeholders to develop an approach to manage the security and resilience of transportation systems and assets. In addition, the Department works with industry stakeholders to develop overarching transportation systems sector goals and objectives.

PWCS is conducted through the use of a layered security strategy that “pushes out the borders” in an effort to reduce the terrorist threat to the MTS. This approach maximizes early warning of emerging maritime related threats originating from foreign ports, routing through the “global commons” of the high seas, into the approaches and waterways of our Nation. The layered approach employs a maritime governance model that shares responsibilities with many partners, both domestic and international. The maritime governance model consists of a three-element system of maritime security regimes, MDA, and MSRO to create an overlapping domestic and international safety net, layers of security, and effective stewardship. Descriptions of the three elements of the maritime governance model follow:

1. Maritime Security Regimes comprise the rules and protocols that enhance collaboration on all-hazard maritime infrastructure resilience and recovery planning, exercises, and operations. This element of layered security implements domestic and international statutes, regulations, and agreements that coordinate partnerships and establish maritime security standards. Examples of initiatives that enhance the maritime security regime framework include:

⁴⁰ Homeland Security Act of 2002 and Title 14 U.S.C.

- The MTSA requires the USCG to collaborate with vessel owners and port facilities to assess their vulnerabilities and develop measures to reduce them. MTSA also requires the identification of threats to maritime critical infrastructure and key resources to periodically assess the effectiveness of antiterrorism measures in both U.S. and foreign ports and take action in cases where effective antiterrorism measures are not in place. Commensurate with the provisions of the MTSA, the USCG coordinated closely with the International Maritime Organization develop an international security regime, designated the International Ship and Port Facility Security (ISPS) Code. It contains security-related requirements for all signatory governments, port authorities, and shipping companies, together with a series of guidelines and recommendations for meeting those requirements. The USCG's International Port Security Program engages with foreign governments and visits foreign ports to assess their compliance with the ISPS Code and to improve security through dialogue and targeted capacity building.
- The CSI was launched in 2002 in response to the September 11, 2001, terrorist attacks.⁴¹ It is part of the CBP layered cargo security strategy. CSI addresses the threat to border security and global trade posed by the potential terrorist use of maritime containers. CBP deploys multidisciplinary teams to foreign seaports. They target and examine high-risk cargo before it is placed on vessels bound for the United States. CSI operates in over 55 ports worldwide. Currently, over 80 percent of all maritime cargo imported into our Nation is subject to prescreening. CBP has also deployed NII and Radiation Portal Monitor technology to identify contraband and weapons of mass effect.

TSA's TWIC regulations are now implemented in the maritime domain for workers requiring unescorted access to secure area of port facilities, Outer Continental Shelf facilities, and vessels regulated under the MTSA. TSA and the USCG implement the TWIC program to help ensure only vetted individuals have access to secure areas. The TWIC program furthers the multilayered approach to safeguarding the MTS and port critical infrastructure.

2. MDA includes detection, monitoring, and information sharing activities occurring within the maritime domain. Together, regimes and MDA inform decision makers and allow them to identify trends, anomalies, and activities that threaten or endanger U.S. interests. Sharing information in the maritime environment regarding vessels, activities, and operators is a critical component in DHS mission success. Through a number of operational, technological, programmatic, and policy-related initiatives, DHS continues to improve information sharing among departmental components and other local, state, tribal, territorial, Federal, international, and private sector partners. The following examples illustrate initiatives that support information sharing efforts and MTSA requirements for maritime intelligence:
 - The National Maritime Intelligence Center is an interagency facility housing ODNI's National Maritime Intelligence-Integration Office (NMIO); the U.S. Navy's Office of Naval Intelligence (ONI); and the USCG's Intelligence Coordination Center (CG-ICC). Collectively, this center and other Federal information sharing mechanisms synthesize real-time maritime information and intelligence regarding threats to U.S. ports and vessels. Other information hubs that support maritime transportation security include the USCG Maritime Intelligence Fusion Centers (MIFCs), the CBP NTC, and the DHS NICC.

⁴¹ U.S. CBP website, CSI Fact Sheet, May 2011.

- The USCG and its partners have established Interagency Operation Centers (IOC) at 35 large ports (per requirements of the 2006 SAFE Port Act). A port's IOC is the foundation for a coalition of federated agencies and local, state, tribal, and territorial government first responders that conduct risk-based operational planning for improved port security. The IOC helps establish the framework necessary to synchronize and sequence single-agency mission planning with a more holistic interagency operational planning and monitoring effort. The IOCs at all major ports are enhanced by a Federal Maritime Operations Coordination Plan (MOC-P). The DHS Science and Technology Directorate aids IOC development by evaluating sensor and information sharing technologies to improve data sharing between port partners.
3. MSRO is the third element of the maritime governance model. MSRO provides the collaborative, coordinated, integrated, and layered operations conducted by the USCG and its local, state, tribal, territorial, and Federal maritime partners to deny use and exploitation of the maritime domain by criminal or hostile actors. These operations are risk-based and MDA-informed. MSRO also allows the safe and sustainable day-to-day use of the maritime domain and rapid system stabilization and recovery of basic functions of the maritime infrastructure from natural or manmade hazards.
- MSRO elements include coastal and waterway deterrence patrols of maritime critical infrastructure and marinas, armed escorts of high-risk vessels, response to threats, and recovery from attacks or natural disasters that may occur. MSRO also encompasses security support of DOD military out-loads; enforcement of fixed security zones; and control of port access, activity, and movement. MSRO includes waterborne security boarding by law enforcement agencies; underwater port security; canine explosives detection; deliberate and contingency planning and exercises; and focused regional surge operations.
 - A key element of MSRO is persistent offshore multimission operations. This consists of USCG and CBP vessels and aircraft, often supported by DOD and international partners, continuously conducting at-sea awareness, interdiction, and enforcement patrols to execute the offshore portion of the layered security system. MSRO forces are equipped to conduct operations in hostile environments, including responding to a CBRN or high-yield explosive threat. For field commanders to determine resource levels appropriate for specific terrorism prevention and response, risk-informed decision making is based upon potential terrorist courses of action within the maritime domain. These courses of action, comparable to the DHS Transportation Sector Security Risk Assessment (TSSRA) scenarios, have been categorized in 15 meta-scenarios, grouped into three attack modes: transfer, direct attack and exploitation.⁴² Examples include: transfer of WMD into our Nation to support terrorist operations using exploited vessels en route from foreign countries; waterborne explosive attacks delivered against high-value assets; and forces taking control of a vessel of opportunity to be used as a weapon against other targets.
 - MSRO also includes the immediate and short-duration salvage and recovery from all-hazards damage crucial to ensuring resilience of our Nation's maritime and associated cross-modal transportation systems. Of significant importance to all-hazard maritime resilience and recovery is the development, maintenance, exercise, and management of the Salvage Response Plans (SRP) required by the SAFE PORT Act and the MTS recovery protocols required by the MTSA. The USCG and its local, state, tribal, territorial, Federal, and private

⁴² USCG MSRO Manual (U//SSI) COMDTINST M16600.6A.

sector port partners are required to maintain an expertise in the salvage and recovery organizations, essential elements of information, and equipment of their particular area of responsibility. They effectively coordinated multipartner waterways salvage and recovery efforts in the Gulf of Mexico after Hurricane Katrina and the New York/New Jersey area after Super Storm Sandy provided the proof of the importance of recovery and salvage planning and exercises. Each of the 43 Captain of the Port (COTP) MTS Recovery plans support coordinated recovery activities and operations for all our port areas. The USCG's Common Assessment Reporting Tool (CART) is a database which facilitates real-time sharing of MTS information and infrastructure status during response and recovery to an incident.

4. The MOTR Plan aims for coordinated U.S. Government response to threats against the United States and its interests in the Maritime Domain by establishing roles and responsibilities, which enable the government to respond quickly and decisively.

USACE. The USACE operates and maintains 12,000 miles of commercial inland navigation channels and 239 navigation lock chambers. In addition, it maintains 926 coastal, Great Lakes, and inland harbors.⁴³ The USACE helps mitigate the damage and losses from severe flooding in the inland rivers system by controlling dams and the construction and maintenance of levees. The USACE waterway maintenance role also includes dredging of the same river system during periods of severe drought-caused low water conditions by excavating channels deep and wide enough to allow unimpeded movement of commercial vessel traffic.

USACE's responsibility is complemented by the National Oceanic and Atmospheric Administration, which charts, preserves, enhances, and monitors the condition of the Nation's waterways.

CBP and ICE are responsible for helping protect our Nation from the entry of dangerous goods and people. This includes ensuring that all persons and cargo enter legally, safely, and efficiently through official air, land, and sea POEs. CBP and ICE partners with local, state, tribal, territorial, Federal, and private sector and international stakeholders to perform its mission. CBP processes millions of vessel-borne passengers and crew members and millions of sea containers arriving by vessel from foreign origin. ICE HSI is the primary investigative arm of DHS and the investigative sister agency for CBP. In conjunction with these responsibilities, ICE HSI created Border Enforcement Security Task Forces to coordinate investigations and intelligence related to the entry of dangerous goods and people.

Coordination Structures

No single government agency possesses the responsibility for, the resources required, or the awareness needed to ensure the security of the MTS. The security of the mode depends on the cooperative actions of multiple local, state, tribal, territorial, Federal, and private entities, including owners and operators or their representative organizations; regional organizations and coalitions; academic and professional entities; and international organizations. The following is a list of the coordinating structures in Maritime Security:

- National Maritime Security Advisory Committee (NMSAC)

The MTSA mandated the creation of the NMSAC to provide advice to the Secretary of the DHS via the Commandant of the USCG on matters such as national security strategy and policy, actions required to meet current and future all hazard threats, international cooperation on

⁴³ USACE website, Mission Overview and 7/19/12 Engineer Update.

protection and security issues, and the Protection concerns of the maritime transportation industry.

▪ **Maritime Government Coordinating Council (MGCC)**

In 2006, the MGCC stood up as an element of the Transportation Systems Sector Government Coordinating Council (TSSGCC). Primary membership consists of representatives from DHS, CBP, DOT/MARAD, DOD, Department of Commerce (DOC), USCG, and the FBI. The responsibilities of the MGCC are derived from the NIPP and the charter of the TSSGCC. The MGCC collaborates with the Maritime Sector Coordinating Council, which represents private sector maritime critical infrastructure owners and operators.

▪ **Maritime Security Interagency Policy Committee (MSIPC)**

The membership consists of representatives from numerous government departments, offices, and agencies. It coordinates U.S. Government maritime security policy and recommends maritime security actions.

▪ **CBP/USCG Joint Protocols for the Expeditious Recovery of Trade**

The CBP/USCG joint protocols establish a process for collaborative recovery of maritime trade. For the purposes of these joint protocols, recovery is defined as activities related to the resumption of the basic functionality of the MTS in that period commencing with response to an incident and continuing into the initial phase of restoration of full capability. The actual recovery time period will vary, but generally starts within three days of the incident and may continue for an extended period. Joint protocols specify actions to be taken at the national level to assist in recovering MTS functionality and include:

- Establish communications at the national level to be used by the USCG, CBP, other Federal agencies, and the maritime industry prior to or after an incident.
- Consider the collateral impacts on international commerce due to MTS disruption.
- Support Federal decision making and the protection of Federal interests.
- Establish how the USCG and CBP will interact with other agencies to jointly facilitate the expeditious recovery of the MTS and resumption of commerce.
- Support NSPDs and HSPDs to protect our Nation and its economy.
- Support the SAFE Port Act mandate to develop protocols for the resumption of trade in the event of a transportation disruption.

▪ **Area Maritime Security Committee (AMSC)**

There are 43 COTPs covering all port areas of the U.S. Within their respective COTP Zones, they are charged with enforcing port safety and security and marine environmental protection regulations, including, without limitation, regulations for the protection and security of vessels, harbors, and waterfront facilities; anchorages; security zones; safety zones; regulated navigation areas; deep water ports; water pollution; and ports and waterways safety.⁴⁴ The MTSA and its implementing regulation, 33 C.F.R. § 101, also designate that the COTP serves as the Federal Maritime Security Coordinator (FMSC) for their respective COTP zone. The FMSC is authorized to establish and direct an AMSC and appoint its members, as well as to develop, maintain, and

⁴⁴ 33 C.F.R. § 1.01–30.

exercise, in coordination with the AMSC, the Area Maritime Security Plan (AMSP) for the COTP Zone. In the event of an emergency, the COTP has broad authority to act as necessary without additional authorization and acts as coordinator among other major Federal agencies in the maritime area of responsibility. Each of the 43 Coast Guard COTPs oversees an AMSC that provides a primary means of Federal Government collaboration and communication with the port-level private sector maritime transportation industry.

The MTSA mandated the development of a new regulatory scheme for maritime security that set forth requirements to establish AMSCs to foster government/private collaboration. Each AMSC is active at the local port level and is instrumental in achieving and sustaining a robust maritime security and information sharing regime to protect and increase the resilience of the Nation's MTS from all hazards. The MTSA implementing regulation, 33 C.F.R. § 101, tasks the AMSCs with ensuring that a detailed portwide risk-based Area Maritime Security Assessment is conducted in their respective Area of Responsibility. AMSCs contribute to the establishment of a maritime common operating picture that permits decision makers to access critical and time-sensitive information. AMSCs help define and address national and port-level priorities for all-hazards critical infrastructure security and resilience through the sharing of relevant and actionable information and the identification and exchange of best practices. AMSC annual reports document meetings, activities, training, accomplishments, best practices, and challenges and recommendations and support MSRAM improvements to increase AMSC overall effectiveness.

- **MTS Waterways Management Services**

The USCG's responsibility for waterways management includes coordinating and controlling vessel operations and scheduling on the waterways with Federal agencies, local pilot associations, private marine exchanges, port authorities, and individual vessel operators. The USCG maintains nearly 50,000 aids to navigation, ranging from lighted buoys and beacons to radio navigation systems. Vessel navigation and related infrastructure and services are dependent on cyber- and communications-supported systems managed by various public and private owners and operators; these systems include Global Positioning Systems (GPS), Geographic Information Systems (GIS), Automatic Identification Systems, and Long-Range Identification and Tracking. In addition, the USCG port-specific Vessel Traffic Services (VTS) provide the mariner with information related to the safe navigation of a waterway and report suspicious activity to law enforcement. This information contributes to the safe routing of vessels through congested waterways or waterways that contain a particular hazard.

- **HSI BEST**

HSI BEST was created to combat emerging and existing Transnational Criminal Organizations (TCO) by employing the full range of local, state, tribal, Federal, and international law enforcement resources in the fight to identify, investigate, disrupt, and dismantle these organizations at every level of operation. BEST is a comprehensive response to the growing threat to border security, public safety, and national security. BESTs eliminate the barriers between local and Federal investigations (access to both state and Federal prosecutors), close the gap with international partners in multinational criminal investigations, and create an environment that minimizes the vulnerabilities in our operations that TCOs have traditionally capitalized on to exploit our Nation's land and sea borders.

- **DHS JTFs**

The Secretary of Homeland Security established three JTFs to coordinate the SBA Campaign. On behalf of the Secretary, the JTFs coordinate establishing operational priorities to synchronize capabilities to achieve SBA Campaign objectives and lead coordinating efforts for their respective JTF. Two JTFs have responsibilities in the maritime security coordinating activity: JTF-East and JTF-West.

- JTF-East's joint operating area includes Puerto Rico, the U.S. Virgin Islands, the coastline along the Gulf of Mexico and Florida (excluding the littorals under JTF-West control), international waters of the Caribbean Sea and the Eastern Pacific Ocean southward to the north coast of South America, the airspace spanning U.S. territorial land and waters, and international airspace in the approaches.
- JTF-West's joint operating area includes the land border with Mexico from California to the Gulf of Mexico and the land approaches to this border, the littorals in the Gulf of Mexico off Texas and Pacific off California, and the airspace spanning U.S. territorial land and waters.
- DHS IPTs
 - Senior leaders regularly identify and assess gaps in Protection mission capabilities and capacities. These assessments should be coordinated with the component-led Integrated Product Teams (IPT) managed by the DHS Science and Technology Directorate (S&T), which identifies capability gaps and coordinates and prioritizes DHS research and development efforts to address the identified gaps.

- MARAD

Pursuant to the Defense Production Act of 1950, MARAD has authority⁴⁵ delegated from the Secretary of Transportation to require priority use of commercial port facilities and services by DOD ahead of commercial port contractual obligations. MARAD also has in place standby Federal Port Controller (FPC) service agreements with key executives at strategic U.S. ports.⁴⁶ Each FPC is responsible for prioritizing and controlling the use of port facilities, equipment, and services to ensure that military deployment cargo movement timelines are met, while minimizing congestion and disruption to the movement of commercial cargo. The National Port Readiness Network (NPRN) comprises seven Federal agencies or organizations with missions supporting the secure movement of military cargo during deployments or other national emergencies. Readiness and coordination are accomplished through the local NPRN Port Readiness Committees, which are chaired by the Coast Guard COTP, in the designated strategic seaports. In addition to managing the America's Marine Highways, MARAD seeks to ensure that our Nation maintains adequate shipbuilding and repair services, efficient ports, effective intermodal water and land transportation systems, and reserve shipping capacity for use in time of national emergency. MARAD operates and maintains the National Defense Reserve Fleet (NDRF). The NDRF is available, among other uses, to support the deployment of the armed forces of the United States and for civil contingency operations upon orders from the National Command Authority. The MARAD also has authority to purchase, charter, operate, or otherwise acquire the use of any documented vessel. MARAD assists DHS in the granting of Jones Act waivers of the Merchant Marine Act of 1920 by determining whether Jones Act waivers are necessary, as well as the extent and duration of such waivers, by identifying available U.S. flagged sealift capacity.

⁴⁵ 46 C.F.R. § 340.3.

⁴⁶ The Maritime Administration and the U.S. Marine Transportation System: A Vision for the 21st Century, 2007.

- Saint Lawrence Seaway Development Corporation

The Saint Lawrence Seaway Development Corporation (SLSDC) may halt traffic through those portions of the Saint Lawrence Seaway subject to the jurisdiction of the United States, if required for safety or security of the Seaway or for national security (e.g., deepwater vessels could be barred from entering or leaving the Seaway).

- DHS DNDO

The mission of DNDO is to prevent nuclear terrorism by continuously improving capabilities to deter, detect, respond to, and attribute attacks, in coordination with domestic and international partners.⁴⁷ DNDO's maritime mission area addresses the scanning of people, cargo, vessels, and other conveyances at seaports of entry and on seas, oceans, or other navigable waterways within local, state, tribal, territorial, and Federal enforcement jurisdiction. DNDO, in coordination with the USCG, has deployed over 1,400 radiation portal monitors at U.S. POEs.⁴⁸ These monitors alarm when they detect radiation emissions; this is followed by detailed CBP inspections. DNDO also helps prioritize efforts towards addressing the gaps in MDA, unresolved small vessel security countermeasures, and commercial noncontainer maritime cargo security.

- Private sector facility and vessel owners and operators.

The maritime industry carries out the security and resilience initiatives mandated by MTSA per their independent and industry-shared best practices. Private sector partners also work with international and domestic private and government partners to help enhance layered security regimes, increase MDA, and collaborate on response and recovery operations. The private sector works closely with government regulatory bodies to provide feedback to improve legislation or regulation designed to enhance maritime security. Our Nation's maritime industry owners and operators, or their representative associations, participate in a myriad of forums including port level AMSCs and related exercises, Harbor Safety Committees, domain awareness and reporting programs, the NMSAC, the Maritime Information Sharing and Analysis Centers, and modal Sector Coordinating Councils (SCC).

- Port Security Grant Program (PSGP)

FEMA's PSGP provides funding to maritime partners. PSGP funds, as appropriated, are directed towards preventing or reducing the effects of a marine Transportation Security Incident (TSI) through the implementation of AMSPs and Facility Security Plans. PSGP investments address identified vulnerabilities in maritime security that support the prevention, detection, response, and mitigation factors captured within these plans and support maritime security zone requirements for salvage and recovery. In 2013, over \$93 million in PSGP funding were provided.⁴⁹ Emphasis is placed in building and sustaining capabilities that address high-consequence marine TSIs that pose the greatest risk to the maritime economic security and can be used locally and regionally. These efforts improve the overall maritime resilience of the United States.

- USCG HOMEPORT

⁴⁷ DHS Connect website entry: <https://collaborate.st.dhs.gov/dndo/Intranet/SitePages/AboutUsDNDO.aspx>.

⁴⁸ DHS 2012 Annual Performance Report.

⁴⁹ FEMA PSGP website, updated May 2013.

This is a publicly accessed and secure enterprise internet portal that supports collaborative port information sharing and resilience functionality for operational use. It also serves as the USCG's primary communications tool to share, collect, and disseminate Sensitive but Unclassified information, including Sensitive Security Information, For Official Use Only, and Law Enforcement Sensitive information. HOMEPORT meets critical information sharing mission requirements in support of MTSA and is a primary means for day-to-day management and communication of port security matters between public and private stakeholders from the national to the local levels, including coordination and collaboration between FMSCs and AMSC members, commercial vessel and facility owners and operators, government partners, and the public. HOMEPORT includes the Alert Warning System function, which provides time-sensitive status updates (e.g., maritime security level changes). The COTP routinely uses HOMEPORT to provide port security advisories, port closure status, post hurricane and other contingency plans, and provide other maritime domain information relevant to its port partners.

- The Homeland Security Information Network–Critical Infrastructure (HSIN-CI)

HSIN-CI enables DHS and the critical infrastructure sector stakeholders to communicate, coordinate, and share information in support of the Sector Partnership Framework. HSIN-CI users communicate information pertaining to threats, vulnerabilities, security, response, and recovery activities affecting sector and cross-sector operations by receiving, submitting, and discussing timely, actionable, and accurate information. DHS has designated HSIN-CI to be its primary information sharing platform between and within the critical infrastructure sectors and state and local fusion centers.

Support to Other Coordination Activities

The Maritime Security coordinating activity provides support to the other *coordinating activities* in a variety of ways:

- It supports **Border Security** through the USCG, which performs drug interdiction, migrant interdiction and PWCS activities to provide a layered approach that supports border security and immigration security.
 - Maritime Security initiatives (e.g., PWCS and CSI) reduce threats to border security.
 - Maritime Security operations work in concert with Border Security operations to share intelligence and information and conduct joint security initiatives.
- It supports **Critical Infrastructure Security and Resilience** through work supporting the critical infrastructure sectors.
 - The maritime transportation mode is a subsector or mode of the Transportation Systems Sector, one of the critical infrastructure sectors.
 - Maritime critical infrastructure includes facilities, structures, systems, assets, or services vital to the port area and its economy.
 - USCG Maritime Security Regimes comprise the rules and protocols that enhance collaboration on all-hazard maritime infrastructure resilience and recovery planning, exercises, and operations.
 - This element of layered security implements domestic and international statutes, regulations, and agreements that coordinate partnerships and establish maritime security standards. For example, MTSA requires the identification of threats to maritime critical infrastructure and

key resources, periodic assessment of the effectiveness of antiterrorism measures in both U.S. and foreign ports, and action in cases where effective antiterrorism measures are not in place.

- USCG and CBP AMO MDA comprise a collaborative effective understanding of objects and activities in or near the marine environment that could affect the security, safety, economy, or environment of the U.S.
- The USCG and CBP AMO conduct a diverse set of MSRO activities designed to reduce risks associated with terrorist attack scenarios on critical infrastructure. These include security boardings of various vessels; waterborne, air, and shoreside patrols; and enforcement of fixed security zones at maritime critical infrastructure.
- This layered, risk-based approach is designed to detect, deter, and disrupt terrorist attacks against maritime critical infrastructure.
- It supports **Defense Against WMD Threats** through the USCG, which provides defense activities to support our Nation's proliferation security initiative, while the USCG Maritime Security Regime and MSRO includes sensors that detect WMD.
 - USCG and CBP AMO Maritime security boarding/inspections are conducted routinely to detect or locate and report on R/N materials and devices.
- It supports **Health Security** through the USCG, which works with HHS to quarantine ships suspected of being a health hazard.
- It supports **Immigration Security** efforts through intelligence and information sharing.
- It supports the **Protection of Key Leadership and Special Events** through PWCS activities that protect Key Leadership and Special Events.
- It supports **Transportation Security** by using USCG ice breakers and aids to navigation to provide support.

Support from Other Coordinating Activities

The Maritime Security coordinating activity receives support from the other *coordinating activities* in a variety of ways:

- It gets support from **Border Security** by aligning protective efforts at POEs, coordinating operations and sharing intelligence.
 - The USCG also conducts a diverse set of protective activities designed to reduce human trafficking and contraband smuggling. These include waterborne, air, and shore patrols and security boarding of suspect vessels. This layered, risk-based approach is designed to detect, deter, and disrupt human trafficking.
 - In coordination with CBP, ICE conducts investigations related to Customs Broker backgrounds, as well as facilities and physical security inspections of all functional equivalents of the border (FEB) including Customs Bonded Warehouses, Foreign Trade Zones and Container Freight stations.
- It gets support from **Critical Infrastructure Security and Resilience** through efforts to promote and protect maritime critical infrastructure.
 - Maritime critical infrastructure includes facilities, structures, systems, assets, or services vital to the port area and its economy.

- Some maritime critical infrastructure, predominantly shoreside facilities that transfer cargo (passengers, bulk liquids and solids, packaged goods, and containers) warrant USCG security visits only when vessels carrying such cargoes are present.
- Some maritime critical infrastructure have relatively high likelihood and consequence scores for a particular terrorist attack mode when their risks are compounded by the presence of a high-risk ship or barge that is engaged or about to engage in transfer operations.
- USCG Maritime Security Regimes comprise the rules and protocols that enhance collaboration on all-hazard maritime infrastructure resilience and recovery planning, exercises, and operations. This element of layered security implements domestic and international statutes, regulations, and agreements that coordinate partnerships and establish maritime security standards.
- MTSA requires the identification of threats to maritime critical infrastructure and key resources, periodic assessment of the effectiveness of antiterrorism measures in both U.S. and foreign ports, and action in cases where effective antiterrorism measures are not in place.
- USCG MDA comprises the effective understanding of objects and activities in or near marine critical infrastructure that could affect their security or safety.
- The USCG conducts a diverse set of MSRO activities designed to reduce risks associated with terrorist attack scenarios on critical infrastructure. These include security boardings of vessels suspected of supporting terrorism or other illegal activities that may pose a threat to critical infrastructure; waterborne, air, and shoreside patrols; and enforcement of fixed security zones at maritime critical infrastructure.
- This layered, risk-based approach is designed to detect, deter, and disrupt terrorist attacks against maritime critical infrastructure.
- It gets support from **Defense Against WMD Threats** efforts through intelligence and information sharing, as well as specific support actions by the USCG.
 - USCG security boarding/inspections are conducted routinely to detect or locate and report on R/N materials and devices or the transfer of terrorists into the U.S. who have the intent and capability to carry out WMD attacks.
 - USCG armed escorts of vessels carrying select certain dangerous cargoes are designed to protect the inhabitants of ports from the secondary consequences, i.e., death/injury, economic impacts, and environmental impacts, of a successful terrorist attack on such a vessel. In the event of a WMD attack in a port, the USCG provides remediation actions.
- It gets support from **Health Security** efforts by coordinating information and threat-hazard sharing to combat the introduction of hazardous agents that could introduce public health challenges into the United States.
 - The USCG supports and assists the CDC in carrying out quarantine regulations.
- It gets support from **Immigration Security** efforts through the use of interagency coordination, information sharing, and investigations.
- It gets support from **Protection of Key Leadership and Special Events** through intelligence and information sharing.

- The USCG conducts a diverse set of MSRO activities that are designed to reduce risks associated with terrorist attack scenarios on key leadership and special events.
- These include security boardings of various vessels by waterborne, air, and shoreside patrols; escorts of vessels carrying key leaders, and enforcement of fixed security zones around key leaders and special events.
- This layered, risk-based approach is designed to detect, deter, and disrupt maritime terrorist attacks against key leadership and special events.
- It gets support from **Transportation Security** when Maritime Security personnel and assets provide direct support to Transportation Security through joint physical and planning security teams.
 - Transportation and maritime security personnel conduct joint security planning exercises and development of security programs like the TWIC program, which helps safeguard maritime transportation systems through more robust security screenings.
 - Maritime Security offices and personnel also provide risk analysis modeling and information sharing that helps identify interdependences and opportunities for coordination of effort.
 - Those coordinated efforts include sharing information, sharing risk reduction tools and methods, and conducting joint planning and response operations. Once a Notice of Arrival from a vessel bound for the U.S. has been received, Federal counterterrorism, criminal, and immigration databases screen the crew and passengers onboard. This screening process identifies potential threats and alerts USCG field units, who board the vessel, if necessary.
 - HSI has stood up 37 BESTs throughout the Nation, composed of many local, state, and Federal agencies. BEST teams are led by HSI special agents and address a myriad of maritime and transportation security issues, including contraband smuggling, safety violations to aircraft and marine vessels, and security and access to restricted areas at airports/seaports.
 - Investigations related to Customs Broker backgrounds, as well as facilities and physical security inspections of all functional equivalents of the border (FEB) including Customs Bonded Warehouses, Foreign Trade Zones and Container Freight stations, are also part of the HSI mission set.
 - The HSI mission therefore intertwines with several Federal agencies in many areas relating to Transportation Security.

Support to Other Mission Areas

Maritime Security supports other national preparedness missions. USCG maritime security includes antiterrorism and counterterrorism activities (escorts of vessels; enforcement of fixed security zones; patrols of harbors; randomly assigning armed personnel aboard ferries and other vessels; approval of area, vessel, and facility security plans; random security boardings of vessels; and the international port security program) that support Prevention. The USCG provides search and rescue, specialized HAZMAT teams, and vessel inspections help prevent, mitigate, respond, and recover from natural or manmade disasters. The USCG maintains aids to navigation that prevent vessel groundings or collisions and, after natural disasters, restore navigation aids.

Maritime Security supports other *coordinating activities*. The USCG drug interdiction, migrant interdiction, and PWCS activities provide a layered approach that supports Border Security and

Immigration Security. PWCS activities protect critical infrastructure and Key Leadership and Special Events. USCG defense activities support our Nation's proliferation security initiative, while PWCS includes sensors that detect WMD. The USCG works with HHS to quarantine ships suspected of being a health hazard. USCG ice breakers and aids to navigation support Transportation Security.

Key Plans

- **MTSA of 2002.** This legislation was enacted to address port and waterway security. MTSA directs the Secretary of DHS to identify high-risk vessel types and port facilities and their vulnerabilities and establish maritime safety and security teams.
- **SAFE Port Act of 2006.** This legislation codified into law a number of programs to improve security of U.S. ports including additional security requirements for maritime facilities, creation of the TWIC, establishment of IOCs for port security, and periodic assessments of foreign nation ports conducting trade with the U.S.
- **AMSP.** AMSPs are required for each COTP zone per the National Maritime Transportation Security Plan (NMTSP), and MTSA implementing regulations and must be based on a valid risk-based Area Maritime Security Assessment of the COTP Zone. AMSPs include protocols and procedures for awareness, preparedness, prevention, security response, communications, and port recovery coordination, making them essential elements of the layered security of our Nation's ports. In 2006, following Hurricanes Katrina and Rita, Congress passed the SAFE Port Act which mandated that each AMSP include a post-TSI SRP. The SRP serves as a pre-incident coordination plan to assist the COTP and port partners with clearing navigable waterways as expeditiously as possible following a TSI. Additionally, to satisfy the requirements of the Coast Guard Authorization Act of 2010 and MTSA implementing regulations, each AMSP contains an MTS Recovery (MTSR) Plan. The MTSR Plan contains pre-incident coordination procedures to facilitate short-term stabilization of the MTS and stabilization of the supply chain.
- **Facility Security Plans (FSPs).** The USCG maintains security oversight for more than 3,100 facilities subject to MTSA, 2,564 of which must maintain and implement USCG-approved security plans. Every FSP is reviewed by the Coast Guard in preparation for the annual facility compliance inspection mandated by the SAFE Port Act. These facilities also receive an unannounced inspection during the course of the year.⁵⁰
- **Vessel Security Plans (VSPs).** The USCG maintains security oversight for all vessels subject to MTSA. Approximately 13,000 vessels (including U.S. and foreign commercial vessels that operate in U.S. waters) must maintain and implement USCG-approved security plans. Every VSP is reviewed by the USCG in preparation for the annual MTSA compliance verification inspection mandated by the SAFE Port Act.⁵¹
- **MOTR.** This presidentially approved plan coordinates Federal Government response to threats against the United States and its interests in the maritime domain. The MOTR Plan contains operational coordination requirements to ensure quick and decisive action to counter maritime threats. In its first five years, the MOTR Plan has been utilized in more than 1,000 maritime events ranging from migrant interdictions and drug seizures to terrorism and piracy.

⁵⁰ Threat of Terrorism to U.S. Ports and Vessels Report to Congress, dated Sept 2012.

⁵¹ Ibid.

- **The Maritime Infrastructure Recovery Plan (MIRP).** The MIRP is one of eight plans supporting the National Strategy for Maritime Security. It was developed in collaboration with public and private sector stakeholders, as directed by NSPD-41/HSPD-13. Its development was also coordinated with other supporting plans, especially the MTS Security Recommendations and the Maritime Commerce Security Plan, because of their importance to the secure flow of commerce. The MIRP is intended to protect the American economy by facilitating the restoration of passenger and cargo flow, specifically container cargo, in the event of an attack or similarly disruptive event. Container cargo is more likely to hold perishable items in immediate need of unloading, or items that are key components in the production of consumer goods. The MIRP includes an exercise plan to maintain a level of preparedness within the maritime community. This plan recommends periodic tabletop and field exercises, which align with existing related plans such as the NRF and the DHS National Exercise Program.
- **MTS Recovery Units (MTSRU).** The MTSRU is managed by the COTP and has representatives from local, state, tribal, territorial, Federal, and industry port partners. During MTS recovery operations, the MTSRU is an element under the Planning Section of the Incident Command System (ICS) organization and functions to:
 - Track and report the status of the MTS in an accurate and timely manner
 - Develop a clear understanding of critical recovery pathways
 - Develop courses of action to support MTS Recovery
 - Provide an avenue of input to the response organization for all MTS stakeholders
 - Identify and communicate long-term restoration issues for the Incident Commander.
- **DHS Maritime Migration Plan (DMMP) DHS Operation Plan—VIGILANT SENTRY (OVS)**
- **National Maritime Domain Awareness Plan (NMDAP).** Establishes the foundation for the effective understanding of potential and actual maritime threats and challenges by promoting favorable conditions for integrating and sharing information, including intelligence, to inform decision makers.

Key Authorities and References

The following laws, policy directives, strategies, plans, and EOs are included in addition to the general authorities/references provided in the base plan for the Maritime Security Mission Activity.

- AMSPs
- DHS Small Vessel Security Strategy Implementation Plan, 2011
- DHS Small Vessel Security Strategy (2008)
- DMMP (2011)
- Maritime Operational Threat Response for the National Strategy for Maritime Security (2006)
- Maritime Security Operations Program Performance Plan 2014–2019 (2013)
- Maritime Transportation System Security Plan
- MIRP (2006)
- MTSA of 2002

- National Plan to Achieve MDA (2005)
- National Strategy for Global Supply Chain Security
- National Strategy for Maritime Security (2005)
- National Strategy for Physical Protection of Critical Infrastructure and Key Assets (February 2003)
- National Strategy for the MTS: A Framework for Action (2008)
- NIPP 2013
- NMTSP, Annex B: Maritime.
- Outer Continental Shelf Facility Security Plans
- OVS, (2012)
- Plans to Re-establish Cargo Flow after TSI, 2005 SSI only
- QDR, 2010
- QHSR, 2014
- The 2010 National Drug Control Strategy.
- The DOJ Strategy for Combating Mexican Cartels, 2009.
- The MOC-P
- The National Interdiction Command and Control Plan (NICCP), 2010
- The National Southwest Border Counternarcotics Strategy, 2009
- The NSS, 2010
- The Partnership for 21st Century U.S. Southwest Border Security, 2010
- The USCG Strategy for Maritime Safety, Security, and Stewardship, (2007)
- Transportation Systems SSP (TS SSP)
- Underwater Terrorism Preparedness Plans
- Vessel and Facility Security Plans.

(U//FOUO) Appendix 7 to Annex C: Protection of Key Leadership and Special Events

This Annex is Unclassified and For Official Use Only. Because this document is sensitive, it will not be posted electronically on unclassified systems. Copies may be requested by contacting FEMA at PPD8-NationalPreparedness@fema.dhs.gov.

This page intentionally left blank.

Appendix 8 to Annex C: Transportation Security

Purpose

The Nation's transportation network is an expansive, open, and accessible set of interconnected systems of airways, roads, tracks, terminals, and conveyances that provide services essential to our way of life. Given the complexity and interconnectivity of these networks, Transportation Security requires structured collaboration across the Federal Government. In accordance with PPD-21: Critical Infrastructure Security and Resilience (PPD-21) and NIPP 2013, DHS and DOT are the SSAs for the Transportation Systems Sector. As outline in NIPP 2013, DHS delegates TSA to serve as the executive agent for transportation counterterrorism security, and USCG serves as the executive agent for maritime security. TSA and the USCG, in collaboration with the DOT coordinate the preparedness activities among the sector's partners to prevent, protect against, respond to, and recover from all hazards that could have a debilitating effect on homeland security, public health and safety, or economic well-being.

The co-SSA agencies coordinate the leadership and implementation of the Transportation Systems Sector's mission, which is to continuously improve the security and resilience posture of the Nation's transportation systems to ensure the safety and security of travelers and goods. The co-SSA agencies also coordinate cross-sector issues between/among interdependent sectors, such as the Energy Sector. Coordination among these partners is critical, as the Transportation Systems Sector is considered a lifeline function. Critical transportation infrastructure supports everything from national security and economic stability to public health and safety.

Scope

This appendix focuses only on the Federal *coordinating activities* for Transportation Security. It specifically includes the Federal coordinating structures and mechanisms required to deliver the Protection core capabilities and achieve Transportation Security objectives. The Federal Government will deliver, synchronize, and integrate Protection core capabilities needed to keep our Nation's transportation networks secure and resilient.

Objectives

This appendix will accomplish the following:

- Provide a concept of operations for integrating existing Federal capabilities needed for Transportation Security.
- Describe Federal operational coordination mechanisms that integrate resources and personnel for Transportation Security.
- Lay the foundation for further department or agency planning for Transportation Security, including integration among *coordinating activities*.

Concept of Operations

The concept of operations for delivery of Federal protection capabilities is built on a foundation of local, regional, state, tribal, and territorial situational awareness, including an understanding of the critical dependencies of other sectors on Transportation Services. Transportation infrastructure development involves extensive community engagement and planning, including the consideration of design standards for safety and probable threats, current and future land use, demographic trends and plans, supply needs of industries and utilities, and other vital issues. Federal grant programs

supporting transportation development provide a means for regional and state authorities to meet minimum Federal protection standards. DHS and DOT maintain a field presence in the Federal regions and with the state departments of transportation to provide more effective channels of communication in the steady state and during emergencies. Pre-emergency and emergency operations are augmented through additional Federal coordinating personnel and organizations.

Roles and Responsibilities

Transportation Security requires a unity of effort throughout the Federal Government. Several departments and agencies play a critical role in this mission, including:

- DHS NOC
- TSA
- USCG
- DOT
- CBP.

Each of these Federal partners support the delivery of the Protection core capabilities required for Transportation Security. The table below describes how the Federal Government delivers each Protection core capability in this mission space.

Table 22: Transportation Security Core Capabilities Critical Task Summary

Core Capability	Transportation Security Critical Task Summary
Access Control and Identity Verification	<ul style="list-style-type: none"> ▪ Control and limit access to critical locations and systems ▪ Support verification efforts to authorize, grant, or deny physical and cyber access to key assets
Intelligence and Information Sharing	<ul style="list-style-type: none"> ▪ Setting requirements for intelligence and information sharing across all sectors ▪ Monitoring, detecting, and analyzing threats to public safety, health and security and providing sufficient safeguards to prevent their interaction with transportation systems or key assets. ▪ Gathering and analyzing information to identify potential threats and determine appropriate strategies to address those threats before they can interact with transportation systems or key assets.
Interdiction and Disruption	<ul style="list-style-type: none"> ▪ Deter movement of terrorists into or within the U.S. and disrupt financing and logistical support from reaching potential threats in the U.S. ▪ Coordinate efforts with local, state, tribal, and territorial partners to detect threats and prevent them from reaching their targets. ▪ Ensure transportation security stakeholders have the ability to detect CBRNE devices and resolve CBRNE threats by interdicting conveyances, cargo, and persons associated with a potential threat or act.
Screening, Search, and Detection	<ul style="list-style-type: none"> ▪ Provide active screening and surveillance of people, baggage, mail, and cargo being conveyed through transportation sector assets to detect and identify any potentially threatening materials or persons prior to their interaction with key transportation sector assets. ▪ Provide CBRNE screening of persons, baggage, mail, cargo, and conveyances to prevent their entry into U.S. transportation systems. ▪ Support intelligence and information sharing to help stakeholders identify potential threats and capability gaps. ▪ Screen persons, baggage, mail, cargo, and conveyances using technical, nontechnical, intrusive, and nonintrusive means without unduly hampering the flow of legitimate commerce and transportation.

Core Capability	Transportation Security Critical Task Summary
Physical Protective Measures	<ul style="list-style-type: none"> ▪ Develop and implement physical security measures to support transportation security efforts and enhance transportation security stakeholders' abilities to safeguard against potential threats to transportation security personnel and assets. ▪ Use risk assessments to identify physical protective measures and security training that would support improved protection of key activities and assets. ▪ Identify and prioritize transportation assets, systems, networks, and functions that need to be protected.
Risk Management for Protection Programs and Activities	<ul style="list-style-type: none"> ▪ Develop and use appropriate tools to identify and assess threats, vulnerabilities, and consequences that could impact transportation security efforts. ▪ Develop and implement risk assessments to look at physical environment, infrastructure, new technologies, and improved methodologies to determine appropriate risk mitigation measures that can increase transportation security stakeholders' ability to protect against threats to transportation systems or key assets. ▪ Use risk assessments to design exercises and determine the feasibility of introducing mitigation projects and initiatives to support transportation security.
Cybersecurity	<ul style="list-style-type: none"> ▪ Implement countermeasures, technologies, and policies to protect physical and cyber assets, networks, applications, and systems that support transportation security efforts. ▪ Safeguard against the introduction of people or materials that could impact the cyber or physical security of cyber assets into transportation systems or to areas where they could access key transportation assets.
Supply Chain Integrity and Security	<ul style="list-style-type: none"> ▪ Analyze transportation security assets and networks to identify key dependencies and risks, and implement physical and cyber protection measures to secure and make resilient the key nodes, transportation hubs and modes, and materials needed for transportation security operations. ▪ Develop multi-layer defense and planning efforts to safeguard necessary supplies for transportation security operations against asymmetrical and traditional threats. ▪ Incorporate verification and detection capabilities to identify goods that are misrepresented or contaminated as part of transportation security screenings, and prevent their introduction into U.S. supply chains. ▪ Prevent cargo and supplies from being misdirected or compromised as it through or along transportation systems.

Coordination Structures

Legislation and interdepartmental agreements require DOT and DHS, with TSA and USCG as its agents, to consult with one another when their activities may impact the other. Coordination of Prevention, Protection, Mitigation, Response, and Recovery operations occurs in numerous forums and processes, formal and informal, during steady state operations. During emergencies, formal coordinating processes through the NRF and the National Disaster Recovery Framework provide the coordinating mechanism for the return of transportation services.

- NOC
- NIPP sector coordination (see Critical Infrastructure Security and Resilience coordination structures)
- HSI BESTs
- DHS JTFs (East, West, Investigations)
- DHS IPTs

- FLETC.

Support to Other Coordination Activities

The Transportation Security coordinating activity provides support to the other *coordinating activities* in a variety of ways:

- It supports **Border Security** through coordination and support activities, including a wide range of resource sharing efforts, support for advanced research, and the development of new detection and security measures that can help protect key transportation systems and assets.
 - Border security systems provide support by helping protect against the introduction of threats and hazards into transportation systems, including screening for terrorists, criminals, HAZMAT, and illicit materials.
 - These measures include new biometric screening tools, joint operations to monitor for threats in all sectors (particularly aviation and maritime transportation measures), and improved support for quickly and reliably screening cargo at the border or in foreign countries before it enters into U.S. transportation networks.
 - Integrated teams of border and transportation security personnel can quickly identify risks and corrective measures.
 - Support activities also include safeguarding transportation systems and personnel through improved information sharing and awareness.
 - Border security assets share information about particular threats or hazards to help develop corrective measures.
 - Information sharing can take place in formal environments that work to perform awareness operations and monitoring, such as the AMO Center.
- It supports **Critical Infrastructure Security and Resilience** through work supporting the SSAs, as delineated by NIPP 2013, particularly with regard to coordination efforts.
 - The co-SSAs for Transportation Systems under NIPP 2013 are DHS (USCG and TSA) and DOT.
 - Transportation security supports intelligence and information sharing on cross-sector issues between/among interdependent sectors, such as the Energy Sector.
 - Coordination among these partners is critical, as the Transportation Systems Sector is considered a “lifeline function” within the NIPP construct—as critical transportation infrastructure supports everything from national security and economic stability to public health and safety.
 - It further supports Critical Infrastructure Security and Resilience through the Transportation Systems Sector Cyber Working Group, which has put into place a strategy that encompasses a security methodology that identifies risks and mitigation activities and plans for identifying implementation elements and supports periodic assessments of system capabilities.
 - Transit, passenger and cargo rail, aviation, and other transportation systems rely on computerized networks to facilitate operations, enable communication, provide safety measures, and enhance efficient service delivery. This makes them vulnerable to network failure and cyber attacks.

- The result of attacks on primary or peripheral components or networks could include loss of operational capability or communications.
 - Cybersecurity personnel provide support by sharing information regarding cyber threats and risks, as well as sharing cybersecurity practices that can help protect cyber systems.
 - Cybersecurity assets also help to support research and development of cybersecurity measures that help reduce the risk posed by persistent cyber attacks on transportation networks.
- It supports **Defense Against WMD Threats** through valuable information and intelligence sharing to help maintain necessary situational awareness of potential threats to the transportation sector.
 - Transportation assets and systems are vulnerable to threats relating to WMD, as terrorist groups and criminals can use transportation assets and systems as targets or delivery methods for WMD attacks.
 - Information sharing can include sharing information on specific threats, as well as providing information on a general threat picture to help the sector as a whole develop effective protection strategies based on the current operating picture.
 - It supports **Health Security** through coordination and information sharing.
 - Transportation systems and assets support public health as a lifeline function on which public health systems depend.
 - Transportation Systems Sector assessments of public health and safety identify potential threats or risks that impact transportation protection measures. They support risk management information sharing that addresses public health and pandemic threats to determine potential impacts to transportation systems.
 - It supports **Immigration Security** efforts through sharing of key threat and risk information to maintain situational awareness of potential hazards that would impact transportation system operations or security.
 - Immigration facilities are often located at key transportation hubs, including airports, ports, rail stations, and road inspection sites.
 - The sectors also conduct joint assessments to identify potential dependencies and interdependencies caused by those co-locations.
 - Immigration Security assets also provide updated information that supports passenger and cargo screening efforts on transportation systems.
 - It supports **Maritime Security** efforts when Maritime Security personnel and assets provide direct support to Transportation Security through joint physical and planning security teams.
 - Transportation and maritime security personnel conduct joint security planning exercises and the development of security programs like the TWIC program, which helps safeguard maritime transportation systems through more robust security screenings.
 - Maritime Security offices and personnel also provide risk analysis modeling and information sharing that helps identify interdependences and opportunities for coordination of effort.
 - Those coordinated efforts include sharing information, sharing risk reduction tools and methods, and conducting joint planning and response operations. Once a Notice of Arrival

from a vessel bound for the U.S. has been received, Federal counterterrorism, criminal, and immigration databases screen the crew and passengers onboard.

- This screening process identifies potential threats and alerts USCG field units who board the vessel if necessary.
- It supports the **Protection of Key Leadership and Special Events** by supporting Transportation Security measures that use information and resource sharing relating to key event protection planning.
 - Given the risks that can be posed to transportation systems during a major event, as well as the risk that incidents relating to transportation systems can pose to key events, maintaining strong situational awareness of all potential threats and hazards is key to safeguarding the transportation systems.
 - Coordination and support can also include efforts to conduct joint planning and strategy efforts that help identify new threats, determine roles and responsibilities for security efforts, and share key resources to maximize Protection efforts.

Support from Other Coordinating Activities

The Transportation Security coordinating activity receives support from the other *coordinating activities* in a variety of ways:

- It gets support from **Border Security** through the provision of operational coordination and shared intelligence, especially where transportation systems and POEs operate jointly.
 - In coordination with CBP, ICE conducts investigations related to Customs Broker backgrounds, as well as facilities and physical security inspections of all functional equivalents of the border (FEB) including Customs Bonded Warehouses, Foreign Trade Zones and Container Freight stations.
- It gets support from **Critical Infrastructure Security and Resilience** through the promotion of interagency efforts on protecting critical transportation infrastructure.
 - DOT, TSA, and USCG work jointly to support the Transportation Systems Sector, and the NIPP 2013 partnership structure supports security coordination and planning for the Transportation Systems Sector.
- It gets support from **Defense Against WMD Threats** through intelligence and information sharing.
- It gets support from **Health Security** through intelligence and information sharing of relevant Health Security information that helps transportation officials monitor for potential health sector risks and threats as people and goods pass through Transportation Sector operations.
 - That information sharing also includes notifications from health officials to transportation officials to ensure they maintain situational awareness on any public health risks that could endanger the effective operation of the Transportation Sector.
- It gets support from **Immigration Security** through ICE HSI's work as the lead investigative agency for all immigration offenses against the United States.
- It gets support from **Maritime Security** through the use of USCG ice breakers and aids to navigation to provide support.

- HSI has stood up 37 BESTs throughout the Nation, composed of many local, state, and Federal agencies. BEST teams are led by HSI special agents and address a myriad of border-related Transportation Security issues including contraband smuggling, safety violations to aircraft and marine vessels, and security and access to restricted areas at airports/seaports.
- It gets support from **Protection of Key Leadership and Special Events** through intelligence and information sharing.

Support to Other Mission Areas

Transportation Security provides support to other mission areas, as set forth in the National Preparedness Goal. One of the biggest areas where transportation security protection activities provide support is in response capabilities. Transportation security stakeholders work to ensure that transportation systems and key assets are protected from threats across the threat spectrum, helping ensure that those systems and assets are available in the aftermath of an incident or emergency. Maintaining access and functionality of those systems and assets establishes essential lifelines for both the delivery of response services and the safe and fully accessible transit or evacuation of affected persons. Protecting transportation systems and assets also supports recovery efforts by establishing a reliable mechanism for delivering recovery services to impacted areas and ensuring effective movement of recovery personnel and affected persons in the impacted area. Protection activities from within Transportation Security also support mitigation efforts by helping reduce the potential impact of the full spectrum of threats to key transportation systems and assets. Similarly, Transportation Security supports screenings, threat information sharing, and establishment of security measures that support Prevention mission tasks by reducing risks and helping limit the ability of threats to access or impact key transportation assets.

Key Plans

- Transportation Systems Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan.
- United States Department of Transportation Roadway Safety Plan.
- Maritime Transportation System Security Recommendations.

Key Authorities and References

The following laws, policy directives, strategies, and EOs are included in addition to the general authorities/references provided in the base plan for Transportation Security.

By statute, the Secretary of Transportation shall, under the direction of the President, exercise leadership in transportation matters, including those matters affecting national defense and those matters involving national or regional emergencies. The following is an overview of select authorities of the department that may be of interest in the response to an emergency situation. These are authorities that the Department and operating administrations already have and are available any time the situation warrants, but may be called upon during an emergency situation. Part I below contains a summary of Departmental emergency authorities for key components of the transportation system, including air, rail, mass transit, highway, pipeline, HAZMAT, and maritime transportation. Part II contains a summary of select waiver authorities of the Department.

Part I—DOT Authorities

Air. Any movement in the navigable airspace of the United States can be stopped, redirected, or excluded by the FAA, regardless of the commodity involved (49 U.S.C. § 40103). Additionally, the

FAA can order U.S. flag air carriers not to enter designated airspace of a foreign country (e.g., to keep airspace clear for rescue operations). If the FAA determines that an emergency exists related to safety in air commerce that requires immediate action, the FAA may prescribe regulations and issue orders immediately to meet that emergency (49 U.S.C. § 46105(c)).

Rail. Any movement in the United States by rail carrier (including commuter rail but excluding urban rapid transit not connected to the general system of rail transportation) may be stopped, redirected, or limited by the combined authority of the Surface Transportation Board (STB) and the Federal Railroad Administration (FRA), irrespective of commodity involved. FRA may issue, without providing prior notice and an opportunity for comment, an emergency order imposing any restrictions or prohibitions necessary to abate what FRA determines is an emergency situation involving a hazard of death, personal injury, or significant harm to the environment caused by unsafe conditions or practices (49 U.S.C. § 20104). While FRA may stop rail traffic, it may not redirect the movement of the traffic; only STB may do that. In addition, FRA safety inspectors may immediately order a locomotive out of service if it is not safe to operate without unnecessary danger of personal injury (e.g., noncompliance with FRA regulations) until either repair of the defect or further inspection and a finding of compliance (49 U.S.C. § 20702(b)).⁵³ Further, an FRA safety inspector may immediately order freight cars and railroad passenger equipment (both cars and locomotives) out of service if they violate certain FRA regulations and are unsafe to operate, until they are repaired or found to be in compliance (49 U.S.C. §§ 20111(b), 20702(b)).⁵⁴

The STB can direct for a period of 270 days the movement, preferences, and prioritization of freight traffic necessary to alleviate an emergency situation involving the failure of traffic movement having substantial adverse impacts on shippers or on rail service in any region of the United States (49 U.S.C. § 11123), and may also order that preference be given to certain traffic when the President so directs in time of war or threatened war (49 U.S.C. § 11124).

Mass Transit. In general, DOT is forbidden from regulating the operation, etc., of public transportation system grantees of the Federal Transit Administration (FTA). However, Section 49 U.S.C § 5334 creates an express exception to the above prohibition when needed for national defense or in the event of a national or regional emergency, or for purposes of establishing and enforcing a program to improve the safety of U.S. public transportation systems.

Highway. DOT's Federal Highway Administration (FHWA) possesses no authority to operate the Nation's highway system during times of emergency. Local governments, states, other Federal agencies, and private parties own, control, and operate the Nation's roads and bridges.

Pipeline. The Pipeline and Hazardous Materials Safety Administration (PHMSA) has authority to issue an administrative order suspending or restricting operation of a gas or hazardous liquid pipeline facility without prior notice and hearing if it determines that: (1) continued operation of the pipeline facility is or would be hazardous; and (2) failure to issue the order expeditiously will result in likely serious harm to life, property or the environment (49 U.S.C. § 60112). PHMSA may issue a special permit on an emergency basis temporarily waiving compliance with any part of the Federal safety regulations applicable to a pipeline without prior notice and hearing on terms PHMSA considers appropriate, if PHMSA determines that: (1) it is in the public interest to grant the special permit; (2) the special permit is not inconsistent with pipeline safety; and (3) the special permit is necessary to address an actual or impending emergency involving pipeline transportation, including an emergency

⁵³ 49 C.F.R. § 216.13, 216.17.

⁵⁴ 49 C.F.R. § 216.11, 216.15, 216.17, June 25, 2013.

caused by a natural or manmade disaster. Emergency special permits may be issued for a period of not more than 60 days but may be renewed upon application after notice and opportunity for a hearing (49 U.S.C. § 60118(c) (2)).

Hazardous Materials. Any aspect of HAZMAT transportation by any mode that presents an “imminent hazard” may be halted by court order (49 U.S.C. § 5122(b)). An “imminent hazard” is a condition that presents a substantial likelihood that death, serious illness, severe personal injury, or a substantial endangerment to health, property, or the environment may occur before the reasonable foreseeable completion date of a formal proceeding begun to lessen the risk of that death, illness, injury, or endangerment (49 U.S.C. § 5102). DOT may issue or impose emergency restrictions, prohibitions, recalls, or out-of-service orders involving HAZMAT without notice or an opportunity for a hearing, but only to the extent necessary to abate an imminent hazard (49 U.S.C. § 5121(d)).⁵⁵

Maritime. The SLSDC may halt traffic through those portions of the Saint Lawrence Seaway subject to the jurisdiction of the United States, if required for safety or security of the seaway or for national security (e.g., deepwater vessels could be barred from entering or leaving the Seaway) (33 U.S.C. §§ 984 & 1226). Also, June 25, 2013, the Ports and Waterways Safety Act of 1972 (Pub. L. 92-340, 86 Stat. 424), as amended by the Port and Tanker Safety Act of 1978 (Pub. L. 95-474, 92 Stat. 1471), provides the SLSDC authority over vessel operations in the Saint Lawrence Seaway.

During a national emergency declared by the President, DOT, through MARAD, can enhance U.S. sealift capacity by taking control of vessels, containers, and chassis through requisitioning (46 U.S.C. § 56301); Emergency Foreign Vessels Acquisition Act (50 U.S.C. §§ 196–198)). When the United States is at war or during a national emergency declared by the President, MARAD can also restrict the transfer of shipyards, among other properties, to foreign ownership (46 U.S.C. § 56102(a)). MARAD can prevent the transfer of vessel ownership to foreign ownership or control (46 U.S.C. § 56101), and, working with the DOD, can allocate landside access and space in ports for the more efficient movement of military cargo (see discussion below regarding the Defense Production Act, and MARAD’s regulations at 46 C.F.R. Parts 340, 345–47).

MARAD operates and maintains the NDRF (50 U.S.C. App. § 1744). The NDRF is available, among other uses, to support the deployment of the armed forces of the United States and for civil contingency operations upon orders from the National Command Authority (50 U.S.C. App. § 1744(b)). MARAD also has authority to purchase, charter, operate, or otherwise acquire the use of any documented vessel (46 U.S.C. § 57533).

Part II—Select Waiver Authorities of DOT

DOT has specific authorities to waive certain safety regulations. The following is an overview of DOT’s more significant or useful authorities that may apply in an emergency situation. Each authority is heavily fact-driven.

Aviation (FAA and OST)

Safety: FAA has authority to grant exemptions from FAA regulations (49 U.S.C. § 40109(b)).⁵⁶

Economic: The Office of the Assistant Secretary for Aviation and International Affairs (OST-X) may issue emergency exemptions on a temporary basis to permit foreign-flag airlines to carry passengers and freight in support of a designated relief effort, such as a hurricane (49 U.S.C.

⁵⁵ For DOT’s regulations implementing this statutory authority, see 49 C.F.R. part 109.

⁵⁶ For FAA’s exemption procedures see 14 C.F.R. § 11.61 et seq.

§ 40109(g)), and may issue emergency exemptions to permit air carriers normally licensed only for private air transportation to offer their services to the public at large, including government and private relief organizations, to assist in relief efforts (49 U.S.C. § 40109(c)).

Commercial Motor Vehicles (CMV) (Federal Motor Carrier Safety Administration [FMCSA]):

Upon declaration of a regional or local emergency, either by the President, designated FMCSA officials, or appropriate local, state, tribal, and territorial officials, FMCSA regulations automatically provide temporary relief from specific safety regulations to any motor carrier or driver operating a CMV to provide direct emergency assistance during the emergency (49 C.F.R. § 390.23); no application by the carrier or driver is needed. This regulatory relief covers 49 C.F.R. § 390–399 of the Federal Motor Carrier Safety Regulations, which include hours of service requirements; driver qualification requirements; CMV operation, inspection, repair and maintenance requirements; and employee safety and health standards. Section 390.23 does not provide relief from the requirements for a Commercial Driver’s License (49 C.F.R. § 383), controlled substances and alcohol testing (49 C.F.R. § 382), or motor carrier financial responsibility/insurance (49 C.F.R. § 387).^{57,58}

Highway (FHWA): DOT’s FHWA possesses no authority to operate the Nation’s highway system during times of emergency. Local, state, tribal, and territorial governments, other Federal agencies, and private parties own, control, and operate the Nation’s roads and bridges. Additionally, waivers of size and weight restrictions may be issued by the states in the event of a Presidential Declaration of Emergency.

Hazardous Materials (PHMSA): Pursuant to 49 U.S.C. § 5117(a)(1), PHMSA may issue special permits authorizing a variance of specified HAZMAT transportation safety regulations for transportation of HAZMAT in a way that achieves a safety level at least equal that required under existing law, or that is consistent with the public interest and Chapter 51, Title 49, if a required safety level does not exist.

Maritime—Jones Act: Although DHS, not DOT, issues waivers of the Merchant Marine Act of 1920 (the “Jones Act”), MARAD assists DHS in determining whether such waivers are necessary, as well as the extent and duration of such waivers, by identifying available U.S. flagged sealift capacity (46 U.S.C § 501).

War Risk Insurance: Under 46 U.S.C. § 53905, with approval of the President, DOT issues war risk insurance without payment of the insurance premium at the request of the DOD upon an agreement of indemnifying DOT against loss covered by the insurance.

Transporting Military Freight: Under 10 U.S.C. § 2631, DOD, not DOT, may waive the vessel requirements of transporting military freight when DOD determines that such waiver is critical to U.S. national security.

Public Transit: FTA is prohibited from regulating operations, routes, or schedules of public transportation except for purposes of national defense or in the event of a national or regional emergency, or for purposes of establishing and enforcing a program to improve the safety of U.S. public transportation systems (49 U.S.C. 5334(b)(1)). FTA generally does not have authority to

⁵⁷ The definition of “direct assistance” in 49 C.F.R. § 390.23 is “transportation and other relief services provided by a motor carrier or its driver(s) incident to the immediate restoration of essential services (such as electricity, medical care, sewer, water, telecommunications, and telecommunication transmissions) or essential supplies (such as food and fuel). It does not include transportation related to long-term rehabilitation of damaged physical infrastructure or routine commercial deliveries after the initial threat to life and property has passed.”

⁵⁸ For PHMSA’s special permit procedures, see 49 C.F.R. Part 107, subpart B.

waive statutory requirements. However, when making a grant under FTA's Public Transportation Emergency Relief Program, authorized by Moving Ahead for Progress in the 21st Century Act (MAP-21), grants are subject to terms and conditions FTA considers are necessary. In addition, FTA's charter rule (49 C.F.R. Part 604) provides that evacuations and emergency services are not considered charter service. Grantees may provide emergency services that might otherwise be considered charter to a community for up to 45 days before notifying FTA (49 C.F.R. § 604.2(f)). In addition, FTA may waive the prohibition against use of FTA-funded assets for school bus service during or in the aftermath of an emergency (49 U.S.C. § 5323, 49 C.F.R. Part 605). FTA may also waive the requirement that FTA-assisted property be used for transit purposes and allow, for example, transit systems to use buses as barricades or to use transit facilities as shelters (49 C.F.R. Part 18). Additionally, FTA may waive the requirement to reimburse FTA for damage to FTA-funded property due to misuse if, during an emergency, the transit system needs to subject its assets to dangerous conditions (FTA Master Agreement § 19). Finally, FTA may waive requirements for driver drug and alcohol testing, competitive procurement, and Buy America requirements, if drivers or assets need to be quickly obtained to respond to an emergency (49 U.S.C. § 5331; 49 C.F.R. Part 655; 49 C.F.R. Part 18, 49 U.S.C. § 5323; and 49 C.F.R. Part 661).^{59,60}

Pipeline: PHMSA may issue a special permit on an emergency basis temporarily waiving compliance with any part of the Federal safety regulations applicable to a pipeline without prior notice and hearing on terms PHMSA considers appropriate, if PHMSA determines that: (1) it is in the public interest to grant the special permit; (2) the special permit is not inconsistent with pipeline safety; and (3) the special permit is necessary to address an actual or impending emergency involving pipeline transportation, including an emergency caused by a natural or manmade disaster. Emergency special permits may be issued for a period of not more than 60 days but may be renewed upon application after notice and opportunity for a hearing (49 U.S.C. § 60118(c) (2)).

Railroads (FRA and STB)

FRA: FRA may issue waivers of certain safety regulations or orders during an emergency situation or event (49 U.S.C. § 20103(d)). Such waivers may include temporary postponement of required maintenance, repair, or inspection related to railroad equipment, track, and signals; temporary relief from certain recordkeeping or reporting requirements; or short-term relief from various operational requirements.

STB: STB has broad authority to exempt persons, transactions, or services—either individually or as a class—from almost all parts of the statute that it administers, pursuant to 49 U.S.C. § 10502 (rail provisions), § 13541 (motor and water carrier provisions), and § 15302 (pipeline provisions). Similarly, STB has broad authority to waive its regulations, so long as the waiver is reasonable and explained.

⁵⁹ For FTA's emergency relief provisions, see 49 C.F.R. Part 601.

⁶⁰ For FRA's emergency waiver procedures, see 49 C.F.R. § 211.45.

This page intentionally left blank.

Annex D: Selected Glossary

Capability Targets: The performance threshold(s) for each core capability.

Coordinating Activities: The existing means of coordinating Protection activity within distinct and established domains of operation.

Core Capabilities: Distinct critical elements necessary to achieve the National Preparedness Goal.

Critical Infrastructure: Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. The Nation's critical infrastructure is composed of 16 sectors: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, material, and waste; transportation systems; and water and wastewater systems.

Cybersecurity: The process of protecting information by preventing, detecting, and responding to attacks. It encompasses the cyberspace global domain of operations consisting of the interdependent network of information technology infrastructures, and includes the internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. The cybersecurity core capability is the means for protecting cyberspace from damage, unauthorized use, or exploitation of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability.

Mission Areas: Groups of core capabilities, including Prevention, Protection, Mitigation, Response, and Recovery.

Mitigation: The term "mitigation" refers to those capabilities necessary to reduce loss of life and property by lessening the impact of disasters. Mitigation capabilities include, but are not limited to, community-wide risk reduction projects; efforts to improve the resilience of critical infrastructure and key resource lifelines; risk reduction for specific vulnerabilities from natural hazards or acts of terrorism; and initiatives to reduce future risks after a disaster has occurred.

National Health Security: Securing the Nation and its people to be prepared for, protected from, and resilient in the face of incidents with health consequences.

National Preparedness: The actions taken to plan, organize, equip, train, and exercise to build and sustain the capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from those threats that pose the greatest risk to the security of the Nation.

Performance Measure: The metrics used to ascertain actual performance against target levels identified for each core capability; by design, they are clear, objective, and quantifiable.

Prevention: The term "prevention" refers to those capabilities necessary to avoid, prevent, or stop a threatened or actual act of terrorism. Prevention capabilities include, but are not limited to, information sharing and warning; domestic counterterrorism; and preventing the acquisition or use of WMD. For purposes of the prevention framework called for in this directive, the term "prevention" refers to preventing imminent threats.

Protection: The term "protection" refers to those capabilities necessary to secure the homeland against acts of terrorism and manmade or natural disasters. Protection capabilities include, but are not limited to, defense against WMD threats; defense of agriculture and food; critical infrastructure

security and resilience; protection of key leadership and special events; border security; maritime security; transportation security; immigration security; and cybersecurity.

Recovery: The term “recovery” refers to those capabilities necessary to assist communities affected by an incident to recover effectively, including, but not limited to, rebuilding infrastructure systems; providing adequate interim and long-term housing for survivors; restoring health, social, and community services; promoting economic development; and restoring natural and cultural resources.

Resilience: The ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies.

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

Risk Assessment: A product or process that collects information and assigns a value to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision making.

Security: The protection of the Nation and its people, vital interests, and way of life.

Stabilization: The process by which the immediate impacts of an incident on community systems are managed and contained.

Steady State: A condition where operations and procedures are normal and ongoing. Communities are considered to be at a steady state prior to disasters and after recovery is complete.

Terrorism: Any activity that involves an act that is dangerous to human life or potentially destructive of critical infrastructure or key resources and is a violation of the criminal laws of the United States or of any state or other subdivision of the United States; and appears to be intended to intimidate or coerce a civilian population, or to influence the policy of a government by intimidation or coercion, or to affect the conduct of a government by mass destruction, assassination, or kidnapping. (Note that although the definition of terrorism includes both domestic and international acts of terrorism, the scope of the planning system is the prevention and protection against acts of terrorism in the homeland.)

Weapon of Mass Destruction: Materials, weapons, or devices that are intended or capable of causing death or serious bodily injury to a significant number of people through release, dissemination, or impact of toxic or poisonous chemicals or precursors, a disease organism, or radiation or radioactivity, to include, but not limited to, biological devices, chemical devices, improvised nuclear devices, radiological dispersion devices, and radiological exposure devices.

Whole Community: A focus on enabling the participation in national preparedness activities of a wide range of players from the private and nonprofit sectors, including NGOs and the general public, in conjunction with the participation of all levels of government in order to foster better coordination and working relationships. Whole community contributors include children; older adults; individuals with disabilities and others with access and functional needs; those from religious, racial, and ethnically diverse backgrounds; people with limited English proficiency; and owners of animals including household pets and service animals. Used interchangeably with “all-of-Nation.”

Annex E: List of Acronyms

AMO	Air and Marine Operations Center
AMSC	Area Maritime Security Committee
AMSP	Area Maritime Security Plans
API	Advance Passenger Information
APIS	Advance Passenger Information System
ASPR	Assistant Secretary For Preparedness and Response
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
ATS	Automated Targeting System
ATS-P	Automated Targeting System–Passenger
BEST	Border Enforcement Security Task Force
BIFS	Border Intelligence Fusion Section
CAP	Criminal Alien Program
CART	Common Assessment Reporting Tool
CBP	U.S. Customs and Border Protection
CBRN	Chemical, Biological, Radiological, and Nuclear
CBRNE	Chemical, Biological, Radiological, Nuclear, and Explosive
CDC	Centers for Disease Control and Prevention
CEAC	Consular Electronic Application Center
CFATS	Chemical Facility Anti-Terrorism Standards
CFR	Code of Federal Regulations
CG-ICC	U.S. Coast Guard Intelligence Coordination Center
CI	Critical Infrastructure
CII	Critical Infrastructure Information
CIPAC	Critical Infrastructure Partnership Advisory Council
CIRG	Critical Incident Response Group
CMU	Crisis Management Unit
CMV	Commercial Motor Vehicle
COOP	Continuity of Operations Plan
COTP	Captain of the Port
CRI	Cities Readiness Initiative
CSG	Counterterrorism Security Group
CSI	Container Security Initiative

CST	Civil Support Team
CTAB	Counter Terrorism Advisory Board
CTTSO	Combatting Terrorism Technical Support Office
CWMD	Counter-Weapons of Mass Destruction
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DMMP	DHS Maritime Migration Plan
DNDO	Domestic Nuclear Detection Office
DOC	Department of Commerce
DOD	Department of Defense
DOE	Department of Energy
DOI	Department of the Interior
DOJ	Department of Justice
DOS	Department of State
DOT	Department of Transportation
DTRA	Defense Threat Reduction Agency
E2C2	ICE HSI Export Enforcement Coordination Center
EMS	Emergency Medical Services
EO	Executive Order
EPA	Environmental Protection Agency
ERO	Enforcement and Removal Operations
ESS	Emergency Services Sector
ESTA	Electronic System For Travel Authorization
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FBIHQ	FBI Headquarters
FDA	Food and Drug Administration
FEMA	Federal Emergency Management Agency
FHWA	Federal Highway Administration
FIOP	Federal Interagency Operational Plan
FLETC	Federal Law Enforcement Training Centers
FMCSA	Federal Motor Carrier Safety Administration
FMSC	Federal Maritime Security Coordinator
FPC	Federal Port Controller

FPS	Federal Protective Service
FRA	Federal Railroad Administration
FSIS	USDA Food Safety and Inspection Service
FSLC	Federal Senior Leadership Council
FSP	Facility Security Plans
FTA	Federal Transit Administration
FTTTF	Foreign Terrorist Tracking Task Force
GCC	Government Coordinating Councils
GMCC	Global MOTR Coordination Center
GNDA	Global Nuclear Detection Architecture
GSA	General Services Administration
HAZMAT	Hazardous Materials
HHS	Health and Human Services
HPH	Healthcare and Public Health
HPP	Hospital Preparedness Program
HSA	Health Situational Awareness
HSI	Homeland Security Investigations
HSIN	Homeland Security Information Network
HSIN-CI	Homeland Security Intelligence Network – Critical Infrastructure
HSPD	Homeland Security Presidential Directive
I&A	Office of Intelligence and Analysis
IAC	Integrated Analysis Cell
IAEA	International Atomic Energy Agency
IAP	Immigration Advisory Program
IAQ	Immigration Alien Queries
IC	Intelligence Community
ICE	Immigration and Customs Enforcement
ICS	Incident Command System
IFSO	Integrated Federal Support Overview
IHR	International Health Regulations
IMAGE	ICE Mutual Agreement Between Government and Employers
IOC	Interagency Operation Center
IPC	Interagency Policy Committee
IPR	Intellectual Property Rights

IPT	Integrated Product Teams
ISPS	International Ship and Port Facility Security
IWG	Interagency Working Group
JOC	Joint Operations Center
JTF	Joint Task Force
JTTF	Joint Terrorism Task Force
LEO	Law Enforcement Officer
LESC	Law Enforcement Support Center
LRN	Laboratory Response Network
LRN-B	Laboratory Response Network for Biological Threats
LRN-C	Laboratory Response Network for Chemical Threats
LSIS	Large Scale Inspection System
LSSD-TC	CBP Laboratories and Scientific Services Directorate Teleforensic Center
MACC	Multi-Agency Coordination Center
MAP-21	Moving Ahead for Progress in the 21st Century Act
MARAD	U.S. Maritime Administration
MARSEC	Maritime Security
MCM	Medical Countermeasures
MDA	Maritime Domain Awareness
MDDP	Mobile Detection Deployment Program
MGCC	Maritime Government Coordinating Council
MIRP	Maritime Infrastructure Recovery Plan
MOC-P	Maritime Operations Coordination Plan
MOTR	Maritime Operations Threat Response
MPF	Migrant Processing Facility
MSRAM	Maritime Security Risk Analysis Model
MSRO	Maritime Security and Response Operations
MTS	Marine Transportation System
MTSA	Maritime Transportation Security Act
MTSR	Marine Transportation System Recovery
MTSRU	Marine Transportation System Recovery Unit
NBIC	National Biosurveillance Integration Center
NCCIC	National Cybersecurity and Communications Integration Center
NCTC	National Counterterrorism Center

NDRD	Nuclear Defense Research and Development
NDRF	National Defense Reserve Fleet
NGO	Nongovernmental Organizations
NHSS	National Health Security Strategy
NICC	National Infrastructure Coordinating Center
NICCP	National Interdiction Command and Control Plan
NII	Non-Intrusive Inspection
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NLR	National Level Reporting
NMCC	National Military Command Center
NMIO	National Maritime Intelligence-Integration Office
NMSAC	National Maritime Security Advisory Committee
NMTSP	National Maritime Transportation Security Plan
NNSA	National Nuclear Security Administration
NOC	National Operations Center
NPPD	National Protection and Programs Directorate
NPRN	National Port Readiness Network
NRC	Nuclear Regulatory Commission
NRCC	National Response Coordination Center
NRF	National Response Framework
NSC	National Security Council
NSPD	National Security Presidential Directive
NSS	National Security Strategy
NSSE	National Special Security Events
NTAS	National Terrorism Advisory System
NTC	National Targeting Center
NTC-C	National Targeting Center-Cargo
NTC-P	National Targeting Center-Passenger
NWC	National Watch Center
OCIA	Office of Cyber and Infrastructure Analysis
ODNI	Office of the Director of National Intelligence
OHA	DHS, Office of Health Affairs
ONI	Office of Naval Intelligence

OST	Department of Transportation Office of the Secretary
OSTP	White House Office of Science and Technology Policy
OST-X	Office of the Assistant Secretary for Aviation and International Affairs
OVS	DHS Operation Plan—VIGILANT SENTRY
PHEMCE	Public Health Emergency Medical Countermeasures Enterprise
PHEP	Public Health Emergency Preparedness
PHMSA	Pipeline and Hazardous Materials Safety Administration
PHS	Public Health Service
PNR	Passenger Name Record
POE	Ports of Entry
PPD	Presidential Policy Directive
PRND	Preventive Radiological/Nuclear Detection
PSGP	Port Security Grant Program
PWCS	Ports, Waterways, and Coastal Security
QDR	Quadrennial Defense Review
QHSR	Quadrennial Homeland Security Review
R/N	Radiological and Nuclear
RAP	Radiological Assistance Program
RCLG	Regional Carrier Liaison Groups
RND	Radiological Nuclear Detection
RNSO	Radiological/Nuclear Search Operations
S&T	DHS Science and Technology Directorate
SBA	Southern Border and Approaches Campaign
SCC	Sector Coordinating Councils
SDR	National Science and Technology Council Subcommittee On Disaster Reduction
SEAR	Special Event Assessment Rating
SEVIS	Student and Exchange Visitor Program
SEWG	Special Events Working Group
SGS	Strategic Guidance Statement
SIOC	Strategic Information Operations Center
SLB	Senior Leader Brief
SLSDC	Saint Lawrence Seaway Development Corporation
SLTTGCC	State, Local, Tribal, and Territorial Government Coordinating Council
SNRA	Strategic National Risk Assessment

SNS	Strategic National Stockpile
SOC	Health and Human Services Secretary's Operations Center
SRP	Salvage Response Plans
SSA	Sector Specific Agencies
SSP	Sector Specific Plans
STB	Surface Transportation Board
SWAT	Special Weapons and Tactics
TCE	Threat Credibility Evaluation
TCO	Transnational Criminal Organizations
THIRA	Threat and Hazard Identification and Risk Assessment
TSA	Transportation Security Administration
TSDB	Terrorist Screening Database
TSI	Transportation Security Incident
TSSGCC	Transportation Systems Sector Government Coordinating Council
TSSRA	Transportation Sector Security Risk Assessment
TSWG	Technical Support Working Group
TTP	Trusted Traveler Programs
TUE	Terrorist Use of Explosives
TWIC	Transportation Worker Identification Credential
UCG	Unified Coordination Group
USACE	U.S. Army Corps of Engineers
USAO	United States Attorney's Office
USC	United States Code
USCG	U.S. Coast Guard
USCIS	U.S. Citizenship and Immigration Services
USDA	U.S. Department of Agriculture
USG	U.S. Government
USSS	U.S. Secret Service
VIPR	Visible Intermodal Prevention and Response
VSP	Vessel Security Plans
VTS	Vessel Traffic Services
WMD	Weapons of Mass Destruction
WMD-CT	WMD Counterterrorism
WMDSG	WMD Strategic Group

This page intentionally left blank.