

THE INTEGRATED PLANNING SYSTEM

January 2009

Intentionally Left Blank

CONTENTS

FOREWORD	iii
CHAPTER 1: INTRODUCTION AND OVERVIEW	1-1
CHAPTER 2: PLANNING DOCTRINE.....	2-1
CHAPTER 3: PLANNING ROLES AND RESPONSIBILITIES	3-1
CHAPTER 4: VERTICAL AND HORIZONTAL PLANNING INTEGRATION	4-1
CHAPTER 5: FEDERAL PLAN DEVELOPMENT PROCESS.....	5-1
ANNEX A: FEDERAL STRATEGIC GUIDANCE STATEMENT FORMATS.....	A-1
ANNEX B: FEDERAL STRATEGIC PLAN FORMAT.....	B-1
ANNEX C: FEDERAL CONCEPT PLAN FORMAT	C-1
ANNEX D: FEDERAL OPERATIONS PLAN FORMAT.....	D-1
ANNEX E: RISK MANAGEMENT OVERVIEW AND THE IPS	E-1
ANNEX F: RELATED AUTHORITIES.....	F-1
ANNEX G: SELECTED GLOSSARY OF IPS TERMS	G-1
ANNEX H: SELECTED ABBREVIATIONS AND ACRONYMS	H-1

Intentionally Left Blank

FOREWORD

The purpose of the Integrated Planning System (IPS) is to further enhance the preparedness of the United States¹ by formally establishing a standard and comprehensive approach to national planning. It is meant to provide guidance for conducting planning in accordance with the Homeland Security Management System (HSMS), described in the *National Strategy for Homeland Security of 2007*. The *Strategy* calls for a national effort to create and transform homeland security principles, systems, structures and institutions across four key pillars of homeland security:

- Prevent and disrupt terrorist attacks
- Protect the American people, our critical infrastructure, and key resources
- Respond to and recover from incidents that do occur
- Continue to strengthen the foundation to ensure our long-term success.

The fourth pillar of the *Strategy* calls for the Federal Government to:

“Establish a more deliberate and comprehensive system that will ensure unity of effort and help maximize success as we work to prevent and disrupt terrorism, protect the American people, critical infrastructure and key resources, and respond to and recover from incidents that do occur. This new Homeland Security Management System will involve a continuous, mutually reinforcing cycle of activity across four phases: Guidance; Planning Execution; and Assessment and Evaluation.”

To execute the direction set forth in the *Strategy*, the President issued Annex I (*National Planning*) to *Homeland Security Presidential Directive 8 (HSPD-8) (National Preparedness)*. Annex I directs the Secretary of Homeland Security to, among other tasks, develop the IPS.

By introducing a standardized approach to national homeland security planning, the IPS is an important step in enhancing our national preparedness. As this system is implemented over time, it will align and synchronize our Federal planning efforts and serve as a model for planning at all levels of government—Federal, State², local, and Tribal. IPS incorporates lessons learned from both the development of the National Planning and Execution System³ and the planning process and doctrine elements of the *Interim Comprehensive Preparedness Guide 101 (CPG-101)*.

Understanding several key fundamental concepts is important to ensure effective use and implementation of the IPS:

1. The IPS has been developed recognizing that homeland security planning is based on coordination and synchronization rather than command and control. In the Executive Branch, only the President of the United States has directive authority over Federal departments

¹ Public Law 107–296—NOV. 25, 2002 116 STAT. 2141, Section 2 “Definitions.” The term “United States,” when used in a geographic sense, means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, any possession of the United States, and any waters within the jurisdiction of the United States.

² Public Law 107–296—NOV. 25, 2002 116 STAT. 2141, Section 2 “Definitions” and STAT. 2255 “Facilitating Homeland Security Information Sharing Procedures” The term “State” means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States. The term “State” includes the District of Columbia and any commonwealth, territory, or possession of the United States.

³ The IPS replaces the National Planning and Execution System (NPES).

and agencies. Effective planning in this situation can only occur through Federal departments and agencies actively coordinating and synchronizing their planning with each, as required by the situation.

2. The IPS applies to Federal departments and agencies with a role in homeland security when conducting scenario-based planning. The IPS was developed for those departments and agencies that do not have existing planning systems and to standardize plans across the Federal Government to facilitate integration of plans and planning. IPS accommodates most existing Federal planning systems and thus is largely consistent with the planning systems currently in use across the Federal Government. Federal departments and agencies will not be required to discontinue use of successful planning systems or re-draft existing plans to ensure compliance with the IPS. However, those agencies with existing planning systems and plans must ensure the planning products produced with their existing system are compatible with the products produced with the IPS. Those agencies without existing planning processes shall adopt the IPS. Further, the IPS does not replace, but rather complements, the planning process used as part of the Incident Command System (ICS) established in the *National Incident Management System* (NIMS).

3. State, local, and Tribal governments are encouraged to comply with IPS by using the Comprehensive Preparedness Guide (CPG) 101. CPG 101 meets the Annex I requirement that IPS include a “guide for all-hazards planning ... that can be used at Federal, State, local, and Tribal levels to assist the planning process.” The IPS is flexible enough to accommodate the many planning formats, styles, and processes used by State, local, and Tribal governments. Over time, using IPS is expected to facilitate standardization of plans across the United States at all levels of government and enhance preparedness. Together, IPS and CPG 101 support national vertical integration by clearly articulating Federal planning procedures to State, local, and Tribal governments and by establishing a consistent planning process across all levels of government.

4. The IPS establishes a process for developing Federal plans. Initial requirements are based on the current list of National Planning Scenarios (NPS). (These scenarios will change over time.) The Secretary of Homeland Security has been tasked by the President to work in coordination with other agencies with a role in homeland security to develop a Strategic Guidance Statement (SGS),⁴ Strategic Plan,⁵ and a Concept Plan⁶ (CONPLAN) for each NPS.⁷ Every Federal agency with responsibilities enumerated in a CONPLAN shall be required to develop an Operations Plan (OPLAN)⁸ for that scenario, to be approved by the head of that

⁴ Strategic Guidance Statements (SGS), which are required for each NPS, establish the foundation for the development of each Strategic Plan. An SGS will be developed by DHS in coordination with Federal agencies with a role in homeland security and issued by the Secretary of Homeland Security.

⁵ Strategic Plans are required for each SGS; they will define specific Federal interagency roles, responsibilities, mission essential tasks, capabilities, and supporting metrics; and provide strategic guidance to support the development of interagency operational level CONPLANS. Strategic Plans will be developed by DHS in coordination with Federal agencies with a role in homeland security and issued by the Secretary of Homeland Security.

⁶ CONPLANS are developed and issued by the Secretary in coordination with Federal agencies with a role in homeland security. CONPLANS, which are required for each Strategic Plan, will describe the concept of operations for integrating and synchronizing existing Federal capabilities to accomplish mission essential tasks; describe how Federal capabilities will be integrated into and support regional, State, local, and tribal plans; and provide the operational level guidance to support development of each Federal department and agency OPLAN.

⁷ The current list of 15 NPSs has been grouped into 8 scenario sets (see p.75, National Response Framework). An SGS, Strategic Plan, CONPLAN, and agency OPLANs will be required for each of the eight designated scenario sets. The list of NPSs will be updated at least every 2 years.

⁸ OPLANs are developed by each Federal department and agency with responsibilities under a CONPLAN. An OPLAN identifies detailed resource, personnel, and asset allocations to execute the objectives of the strategic plan and turn strategic priorities into operational execution. An OPLAN contains a full description of the concept of operations, including specific roles and responsibilities, tasks, integration, and actions

agency or a designated representative. Federal agencies are not required to re-write their existing plans based on one or more of the NPSs if those documents are compatible with the requirements established in the SGS, Strategic Plan, and CONPLAN. Over time, as existing plans are routinely updated and improved, it is expected that agencies may modify their existing plans for compatibility with the formats established in the IPS.

5. The IPS is not designed to solve every planning problem. The IPS lays the initial foundation necessary to implement the HSMS. It is a major step in establishing common Federal planning doctrine, providing a means for synchronizing operations across the spectrum of homeland security operations (i.e., prevent, protect, respond, and recover) and integrating national planning efforts both horizontally across the Federal Government and vertically among Federal and State, local, and Tribal entities. However, further work is necessary to successfully integrate existing Federal guidance, policies, strategies, plans, and legislation with the HSMS. Through future IPS refinement and the development of other *HSPD-8* Annex I deliverables such as the National Homeland Security Plan (NHSP), the Federal Government remains committed to addressing the following key issues in follow-on efforts:

- A mechanism to inform National Homeland Security planning efforts through a U.S. Government-wide risk-based analysis process
- A consistent and standard process to update the NPSs
- A standardized methodology to define, develop, and assess the required national capabilities and capacity necessary to execute IPS-generated plans
- A standardized methodology that ensures the success of IPS-generated plans by integrating the Federal budgeting and resourcing processes necessary to execute IPS-generated plans.

In summary, the IPS is the first step in standardizing homeland security planning. This will be a dynamic and iterative process for years to come. This document shall be updated 1 year after approval and then every 2 years after that. Constructive feedback will continue to be an integral component of the refinement of this key planning document.

Intentionally Left Blank

CHAPTER 1: INTRODUCTION AND OVERVIEW

“For the Homeland Security Management System to be effective and address long-range challenges across multiple disciplines, all homeland security partners should develop a planning capability that may also be employed during times of crisis.”

National Homeland Security Strategy, October 2007

1. Introduction

a. Annex I (National Planning) to *Homeland Security Presidential Directive-8 (HSPD-8) (National Preparedness)* requires the development and maintenance of a standardized approach to national planning. Effective plans are the product of a comprehensive planning process that supports effective implementation and assessment of operations to achieve an objective.

b. To be successful, national planning must integrate policy and operational objectives and be composed of:

(1) An effective and standardized planning process, including a system for integrating plans among all levels or jurisdictions of government;

(2) National planning doctrine;

(3) Resourced operational and tactical planning capabilities at the Federal and State, local, and Tribal levels;

(4) Levels of planning that capture strategic, operational, and, as appropriate, tactical considerations; and

(5) A structure to fill the capability gaps and shortfalls of State and local governments adequately and effectively.

2. Purpose

a. The Integrated Planning System (IPS) fulfills the requirement for a standardized national planning process and integration system as directed by Annex I to *HSPD-8*. It provides a basic, general framework for developing a series of products leading to a synchronized Federal plan. The IPS is a “how-to” guide for Federal departments and agencies (henceforth “agencies”) to develop contingency planning documents that support State, local, and Tribal governments.

b. Ultimately, the IPS provides a common Federal planning process composed of three levels of planning: strategic, operational, and tactical. The IPS supports the development of a family of related planning documents: Strategic Guidance Statements (SGSs), Strategic Plans, Concept Plans (CONPLANS), Operations Plans (OPLANS), and tactical plans.

3. Scope and Applicability

a. The target audience for the IPS is those Federal agencies with a role in homeland security operations requiring significant complex planning.⁹ Particular focus is on agencies that rely on or provide assistance to other agencies.

b. The IPS applies to Federal agencies with a role in homeland security when developing plans based on the National Planning Scenarios (NPSs). Agencies with existing

⁹ *HSPD-8*, Annex I, National Planning, identifies Federal agencies with a role in homeland security.

planning processes are required to ensure their systems are capable of producing plans consistent with plans produced using the IPS.¹⁰ Federal agencies with no existing planning processes are required to adopt the IPS. The IPS does not replace, but rather complements, the planning process established in the *National Incident Management System (NIMS)*. The IPS also provides a method for Federal agencies to maintain *NIMS* compliance because it is tied to the Preparedness component of *NIMS*.

c. Existing Federal planning processes can be better aligned through standardized planning, shared nomenclature, transparency, and agreed upon allocations of capabilities to achieve common objectives. The intent is not to disrupt ongoing Federal efforts but to introduce a standardized planning methodology that best supports the Nation’s homeland security priorities.

d. The IPS does not supersede any existing State, local, and Tribal planning processes. However, it is the standard general planning system the Federal Government will use for scenario-based planning. It is designed to highlight commonalities among most planning processes because planners often apply the same fundamentals, principles, and processes to developing plans regardless of the objective or desired effect of the plan being developed. As such, the IPS is compatible with many existing planning systems.

e. While State, local, and Tribal governments are not required to adopt IPS, they are the foundation of the homeland security planning process; their participation in integrated planning and understanding of this document is crucial. State, local, and Tribal governments will also participate in the review, development, exercise, and training activities built on this document, as appropriate. *Comprehensive Prepared Guide (CPG) 101* meets the Annex I requirement that IPS include a “guide for all-hazards planning ... that can be used at Federal, State, local, and Tribal levels to assist the planning process.” It is expected that State and local jurisdictions will, over a period of time, align their existing planning processes with those in *CPG-101*. Using shared planning processes helps ensure consistent planning across the Nation at all levels of government, provides a better understanding of the process the Federal Government uses to produce contingency plans, and provides a better understanding of the capabilities and limitations of State, local, and Tribal planning entities. It will also foster greater understanding of the plans themselves.

4. Overview

a. Annex I to *HSPD-8* directs the Secretary of Homeland Security (hereafter “the Secretary”) to develop an IPS that provides a common plan development process, and includes:

(1) National planning doctrine and planning guidance, instruction, and process to ensure consistent planning across the Federal Government;

(2) A mechanism that provides for concept development to identify and analyze the mission and potential courses of action;

(3) A description of the process that allows for plan refinement and proper execution to reflect developments in risk, capabilities, or policies, as well as to incorporate lessons learned from exercises and specific events;

¹⁰ The IPS replaces the National Planning and Execution System (NPES).

(4) A description of the process that links regional, State, local, and Tribal plans, planning cycles, and processes, and allows these plans to inform the development of Federal plans;

(5) A process for fostering vertical and horizontal integration of Federal, State, local, and Tribal plans and allows for State, local, and Tribal capability assessments to feed into Federal plans; and

(6) A guide for all-hazards planning, with comprehensive, practical guidance and instruction on fundamental planning principles that can be used at Federal, State, local, and Tribal levels to assist the planning process.

b. The IPS meets the planning requirements articulated in the *National Strategy for Homeland Security* (2007), which called for the development of a Homeland Security Management System to “ensure unity of effort and help maximize success as we work to prevent and disrupt terrorism, protect the American people, critical infrastructure, and key resources, and respond to and recover from incidents that do occur.”¹¹ Further, these efforts will be complementary and mutually reinforcing to those efforts underway in support of the *National Strategy for Combating Terrorism*.¹²

c. The IPS provides the means for synchronizing existing systems, processes, and plans through the coordination necessary to develop homeland security plans at the strategic, operational, and tactical levels. The IPS is also designed to enhance the efficiency and effectiveness of planning by describing a combination of policies and procedures, supported by technology that provides a capability to plan and conduct integrated operations.

¹¹ *National Strategy for Homeland Security* (2007), pg. 43.

¹² *National Strategy for Homeland Security* (2007), pg. 15.

Intentionally Left Blank

CHAPTER 2: PLANNING DOCTRINE

“Planning is a methodical way to think through the entire life cycle of a potential crisis. Good planning repays the investment of time and effort in development and rehearsal by shortening the time required to gain control over an incident and by providing favorable conditions for rapid and effective exchange of information about a situation, its analysis, and alternative responses. Planning helps Federal, State, local, Tribal, and territorial governments reorient capabilities and resources to be more agile and ensures organizational structures, processes, and procedures effectively support the intended strategic direction ... This effort is a key to success in protecting people and property in crises.”

National Preparedness Guidelines, September 2007

1. **Purpose.** This chapter provides planning doctrine and fundamental planning principles to assist planning at the strategic, operational, and tactical levels. It contains new terms that will be matured over successive iterations to the IPS.

2. **General.** A sound planning process should be orderly, analytical, and consist of logical steps to identify a mission or requirement; develop, analyze, and compare alternative courses of action; select the best course of action (COA); and produce a plan. Planning should also be flexible and responsive to dynamic conditions (e.g., time constraints, varied planning expertise). Homeland security operations demand that Federal agencies gather, review, integrate, and act upon information rapidly in a knowledge-based, collaborative environment. Collaborative planning allows all levels of government to plan together to synchronize their efforts.

a. Federal, State, local, and Tribal homeland security planning includes a number of common characteristics, including acceptability, adequacy, completeness, brevity, consistency and standardization, feasibility, flexibility, clarity, and interoperability. Management engagement and direction are critical to planning success, as is the participation of trained planners.

b. The following comprehensive homeland security planning doctrine accounts for the national homeland security effort—an effort that must recognize and respond to the needs of literally thousands of jurisdictions working together to achieve common but sometimes competing goals and objectives. It is designed to help all members of the homeland security community fulfill their individual and collective obligations, and thereby accomplish the Nation’s homeland security goals.

c. Doctrine describes the fundamental principles and concepts that shape the Nation’s homeland security effort. It broadly tells the reader what planning is supposed to achieve, how it is structured and resourced, and how it is executed. Doctrine describes the systems, processes, intellectual underpinnings, and terminology that are the bedrock of homeland security planning. The doctrinal concepts and principles laid out here are consistent with planning systems already in place or being considered for adoption. Specifically, IPS doctrine supports:

- (1) *Homeland Security Presidential Directive-5 (HSPD-5)*,
- (2) *Homeland Security Presidential Directive-8 (HSPD-8)*, Annex I,
- (3) *National Response Framework (NRF)*,
- (4) *National Incident Management System (NIMS)*,
- (5) *National Preparedness Guidelines (NPG)*, and

(6) *National Strategy for Homeland Security (NSHS).*

3. Federated Planning. The Federal framework of the United States assigns, by law, unique responsibilities and authorities to each member of the homeland security community. It also imposes, by law and practice, a requirement to share responsibilities and authorities to provide for common defense and security. The planning doctrine that best accounts for the separate and shared security responsibilities of Federal, State, local, and Tribal authorities can be labeled “federated planning.”

a. Federated planning is a “multi-directional” doctrine—it flows vertically and horizontally. It recognizes that planning begins with strategic direction from senior executives at each level of government. This strategic direction is translated into strategic plans, then CONPLANS, and then OPLANS. This planning process takes place throughout the planning community, with planners at each level interacting with each other and often with planners at other levels to acquire and integrate support.

b. Government leaders at every level generate strategic goals and requirements that must be converted to executable action plans. The majority of requirements are determined and levied by local leaders.

c. Senior executives at all levels of government make strategic assessments and formulate the strategic guidance necessary to acquire, train, maintain, and employ the assets and personnel needed to protect lives and property. The scope of their strategic planning and decision making varies widely, depending on the jurisdiction’s size and location. State leaders have unique, legally mandated responsibilities to provide security within their jurisdictional boundaries. Much of their responsibility is reinforcing local officials with resources and authorities not available to them under normal circumstances. State officials strategically plan to acquire, position, and/or allocate, as appropriate, funding, State police forces, State militia, National Guard elements, communications, medical care, and other critical elements. They also identify requirements and opportunities to make emergency assistance compacts with other jurisdictions. In addition to supporting municipalities, State leaders conduct the strategic, operational, and tactical planning necessary to protect State-owned properties, installations, and other infrastructure.

d. Federal officials perform a role similar to State officials but on a larger, broader scale. Like their State and regional counterparts, they reinforce local officials, private enterprise, and nongovernmental organizations (NGO) with funding, training, equipment, authorities, and security forces. They establish the national-level structures needed to ensure that the Nation’s security elements operate in a coherent, mutually reinforcing manner. Federal authorities have primary responsibility for organizing and synchronizing the national effort. They accomplish this by guiding national investments in preparedness, facilitating standardized planning processes, and facilitating the robust training and exercise programs required to ensure national integrated preparedness.

e. Many Federal officials have “localized” responsibility for protecting Federal properties, installations, and assets under their control. In executing this responsibility, Federal authorities often require significant community support, including that provided by State, local, and Tribal officials, private entities, and other Federal agencies. In planning to secure specific sites and assets, Federal authorities mirror the actions of State, local, and Tribal leaders; they determine what must be done, identify the resources required (including authorities and

permissions), and coordinate with other levels of government and the private sector to fulfill requirements.

f. Multiple Direction Planning. Federated planning flows in multiple directions. From a local leader's perspective, planning begins locally and is processed up through State, regional, and Federal authorities as necessary.

(1) Local leaders assess their threats, hazards, and risk posture and determine what actions and capabilities are required. They provide resources when they can and petition State and Federal authorities to fill capability shortfalls as needed.

(2) State officials often establish planning assumptions and objectives that local governments in the State are required or encouraged to adopt and support. Statewide interoperable communications plans and systems are an example. At every level of government, officials set strategic goals and objectives for their jurisdictions. They also examine how their specific challenges relate to those of higher, lower, and adjacent jurisdictions. They determine how to operationalize and resource their own and other relevant strategies, as appropriate. Federated planning constitutes an approach in which each member of the homeland security community provides support and is supported by others.

g. Tailored Resourcing. A critical aspect of federated planning is *tailored resourcing*. Tailored resourcing offers leaders a high degree of confidence that they can access essential capabilities without maintaining unnecessarily large, unaffordable fleets of equipment and cadres of people. Tailoring resources balances affordability and risk.

(1) By employing horizontal and vertical integration with tailored resourcing, leaders can identify opportunities for pooling resources and maximize the potential utility of a given capability. Tailored resourcing ensures essential resources are available when, where, and as needed (i.e., time, space, and purpose). The Resource Management component of *NIMS* defines standardized mechanisms and establishes the resource management process to identify requirements for, order and acquire, mobilize, track and report, recover and demobilize, and inventory resources.

(2) Capability and resource availability fall into four categories: Organic, Assigned, Earmarked, and Potential.

(a) *Organic Capabilities*. Organic capabilities are those that are an integral part of the basic structure of an organization and thus are immediately responsive to the leadership of that organization. The organization leadership is responsible for developing, sustaining, and employing these organic capabilities.

(b) *Assigned Capabilities*. Assigned capabilities are those that supporting entities have agreed to allocate to a supported organization for agreed upon purposes in agreed upon situations. Assignment to supported organizations is automatic once predetermined and pre-agreed situation thresholds are reached. Assignment agreements are regarded as binding.

(c) *Earmarked Capabilities*. Earmarked capabilities are those that organizations *intend* to allocate to a supported organization at some future time and situation. Earmarked capabilities are allocated to support other organizations as the situation permits, but their commitment has not been prearranged. These capabilities are often formed into a pool of available resources, none of which has been allocated to a given organization.

(d) *Potential Capabilities.* Potential capabilities are those that *might* be allocated to a supported organization in specified circumstances. Potential capabilities should not be regarded as a highly reliable resource. Their accessibility is determined on a case-by-case basis.

4. Planning Fundamentals. The challenge of planning for protecting lives and property is made easier if planners consider the following common fundamentals during planning.

a. **Planning is an orderly, analytical, problem-solving process.** It follows logical steps from plan initiation to analysis of objectives, to development and comparison of ways to achieve the objectives, and to selection of the best solution. While using a prescribed planning process cannot guarantee success, inadequate plans and planning are proven contributors to failure.

b. **Planning guides preparedness activities.** It provides a common framework to guide preparedness by establishing the desired end state and the tasks required to accomplish it. This process identifies the capabilities required. Capabilities provide the means to accomplish a mission and achieve desired outcomes by performing critical tasks, under specified conditions, to target levels of performance. Exercises provide opportunities to demonstrate and evaluate performance, while periodic assessments of plans identify lessons learned and provide the means to share best products and practices.

c. **Planning helps deal with complexity.** Homeland security problems are most often complex and interrelated. The NSHS applies special emphasis to planning for catastrophic events that embody the greatest risk of mass casualties, massive property loss, and immense social disruption. Planning provides the opportunity for a jurisdiction or regional response structure to work through these very complex situations and their unique associated problems. Planning helps decision makers understand how their decisions might affect the ability of their and neighboring jurisdictions to achieve goals and objectives.

d. **Planning may address functions common to all hazards.** The causes of incidents across the spectrum of homeland security can vary greatly, but the effects do not. This means planners can address incident functions common to all hazards. For example, floods, wildfires, and hazardous materials releases may lead a jurisdiction to issue an evacuation order. Even though each hazard's characteristics (e.g., speed of onset, size of the affected area) are different, many general tasks for conducting an evacuation are the same. Differences in the speed of onset may influence when an evacuation order is given, but the process of issuing an evacuation order does not change. All-hazards planning ensures that planners identify common tasks and determine who is responsible for accomplishing those tasks.

e. **Planning does not need to start from scratch.** Planners should capitalize on the experiences of others. The State is a valuable resource for the local jurisdiction, just as the Federal Government is a valuable resource for the State. Similarly, local and State plans and experiences should inform Federal planning. Many States publish their own standards and guidance for planning, conduct workshops and training courses, and assign their planners to work with local planners. By reviewing existing emergency or contingency plans, planners can:

- (1) Identify applicable authorities and statutes,
- (2) Gain insight into community risk perceptions,
- (3) Identify organizational arrangements used in the past,

- (4) Identify mutual aid agreements with other jurisdictions, and
- (5) Learn how some planning issues were resolved in the past.

f. **Planning depicts the anticipated environment for action.** Early understanding and agreement on planning assumptions and risks provides the context for interaction. Effective planning identifies clear tasks and purposes, promotes frequent interaction among stakeholders, guides preparedness activities, establishes procedures for implementation, provides measures to synchronize actions, and allocates or reallocates resources. Planners should review the existing plans for questionable assumptions, inaccuracies, inconsistencies, omissions, and vagueness. Critiques of recent operations and exercises in the jurisdiction will help planners develop a list of topics to address when updating plans.

g. **Planning must involve all relevant partners.** Just as coordinated operations depend on teamwork, good planning requires a team effort. The most realistic and complete plans are prepared by a team that includes representatives of the Federal agencies; State, local, and Tribal governments; the private sector; and NGOs that will participate in executing the plan.

h. **Planning assigns tasks, allocates resources, and establishes accountability for homeland security operations.** Decision makers must ensure planners have the resources needed to accomplish the planning requirements.

i. **Planning includes senior officials throughout the process to ensure both understanding and buy-in.** Potential planning team members have many day-to-day concerns. For a team to come together, potential members must be convinced that planning has a higher priority, and the person to convince them is the jurisdiction's chief executive. Planning helps decision makers anticipate and think critically, reducing time between decisions and actions. The more involved decision makers are in planning, the better the planning product is. This requires reminding the chief executive that planning is an iterative, dynamic process that ultimately affects his or her performance in an emergency.

j. **Planning is influenced by time, uncertainty, risk, and experience.** These factors define the starting point where planners apply appropriate concepts and methods to create solutions to particular problems. Plans cannot be overly detailed, followed to the letter, or so general that they provide insufficient direction because creating these solutions involves judgment and balancing of competing demands.

k. **Planning identifies the task and purpose of the homeland security operation and facilitates cooperation and communication.** The task identifies what must be done, and the purpose identifies why the task must be accomplished. Planning identifies important constraints (i.e., what must be done) and restraints (i.e., what must not be done) that affect freedom of action and expectations.

l. **Planning is fundamentally a risk management tool.** Uncertainty and risk are inherent in response planning and operations. Risk management during planning identifies potential hazards and vulnerabilities, and assesses the probability and severity of each with respect to mission accomplishment. Decision makers determine and communicate acceptable levels of risk.

5. Homeland Security Spectrum of Operations. Homeland security planning will address each mission area identified in the NSHS: prevention, protection, response, and recovery.¹³

a. Prevention. The term "prevention" refers to activities undertaken by the first responder community during the early stages of an incident to reduce the likelihood or consequences of threatened or actual terrorist attacks.¹⁴

(1) Prevention planning will identify actions that eliminate the possibility of a natural or manmade disaster adversely affecting the safety, security, or continuity of the Nation, its critical infrastructures, its inhabitants, and their civil rights and liberties.

(2) Prevention planning for terrorist attacks will focus on reducing the likelihood or consequence of threatened or actual terrorist attacks. These planning efforts will be aligned with the broader efforts of the *National Implementation Plan for the War on Terror (NIP-WOT)* to disrupt and prevent terrorist attacks on the homeland, deny terrorist and terrorist weapons entry to the United States, and disrupt terrorists' ability to operate within the borders of the United States. Prevention planning must ensure the complete exploitation of classified and unclassified information to increase the likelihood of successfully thwarting terrorists' plans.¹⁵

(3) Many aspects of prevention planning are sensitive and must be produced in and controlled in a classified or law enforcement sensitive environment.

b. Protection. Protecting the lives and livelihoods of the American people requires that the United States undertake measures to deter the threat of terrorism, mitigate the Nation's vulnerabilities, and minimize the consequences of an attack or disaster if it occurs. Protection safeguards citizens and their freedoms, critical infrastructure, property, and the economy from acts of terrorism, natural disasters, or other emergencies.¹⁶

(1) Protection includes actions to mitigate the overall risk. This includes, but is not limited to, Critical Infrastructure and Key Resources (CIKR) assets, systems, networks, functions, or their interconnecting links resulting from exposure, injury, destruction, incapacitation, or exploitation. It involves actions or measures taken to cover or shield from exposure, injury, or destruction. Protective actions may occur before, during, or after an incident, and are designed to prevent, minimize, or contain the impact of an incident.¹⁷

(2) Protection addresses reducing the vulnerability of the American populace to intentional dissemination of harmful biological agents, detonation of a nuclear or radiological device, the intentional or accidental release of toxic chemicals, naturally occurring infectious disease such as an influenza pandemic, and meteorological or geological events such as hurricanes or earthquakes.¹⁸

(3) Protection planning will address structures and processes that are adaptable to incorporating lessons learned and best practices and adjusting quickly within the

¹³ HSPD-8/Annex 1, National Planning, Approved 03 December 2007.

¹⁴ HSPD-8, Preparedness, Approved December 2003, Amended December 2007 by Annex 1 to HSPD-8.

¹⁵ HSPD-8, section 2(i), National Preparedness, December 17, 2003; National Implementation Plan for the War on Terror, National Counterterrorism Center, September 2008.

¹⁶ *National Strategy for Homeland Security*, Homeland Security Council, October 2007; DHS Lexicon Terms and Definitions, Approved October 23, 2007.

¹⁷ *National Infrastructure Protection Plan*, 2006.

¹⁸ *National Strategy for Homeland Security*, Homeland Security Council, October 2007, pg. 29.

time constraints of a fast-moving crisis or threat environment. This planning should manage risk and address known and potential threats and hazards.¹⁹

c. Response. Response embodies the actions taken in the immediate aftermath of an incident to save lives, meet basic human needs, and reduce the loss of property and impact on the environment. Following an incident, either naturally occurring or manmade, response operations are essential to reduce the immediate psychological, social, and economic effects of an incident. Response planning will provide rapid and disciplined incident assessment to ensure response is quickly scalable, adaptable, and flexible. It will incorporate the national response doctrine as presented in the *NRF*, which defines basic roles and responsibilities for incident response across all levels of government and the private sector.²⁰

d. Recovery. Recovery encompasses both short-term and long-term efforts for the rebuilding and revitalization of affected communities. Response and recovery operations are closely related. Recovery planning must provide for a near-seamless transition from response activities to short-term recovery operations—including restoration of interrupted utility services, reestablishment of transportation routes, and the provision of food, water, and shelter to displaced persons.²¹

(1) Recovery planning must ensure a successful transition from short-term recovery to the long-term recovery, including rebuilding and revitalization. These long-term recovery efforts differ from short-term recovery efforts by scope, complexity of efforts required, and the effect on the social fabric of the community. These efforts can take several months to several years to complete, depending on the extent of the catastrophic incident and how extensively CIKR assets require redevelopment and reconstruction.²²

(2) Long-term recovery plans must be designed to maximize results through the efficient use of finite resources. These plans must address both public and private partnerships and integrate collective recovery efforts.²³

6. Planning Administrative Considerations.

a. Multiple Levels of Classification. Homeland security planning is conducted at multiple levels of classification, such as Controlled Unclassified Information, Secret, Top Secret, and Sensitive Compartmented Information (SCI). Disseminating time-sensitive material, limiting distribution, and limiting access/knowledge to those with need to know are imperative in the case of terrorist activities. Further, classifying information at the lowest possible level can be the difference in preventing an attack and effectively responding to one after the fact.

b. Non-Standard Lexicon/Terminology. Many organizations involved in homeland security operations have adopted different lexicons. Federal planners will develop a recommended standard homeland security planning lexicon to address this problem. The IPS is a source document for this lexicon and consolidates definitions from other official documents pertaining to planning.

¹⁹ *National Infrastructure Protection Plan*, 2006.

²⁰ National Strategy for Homeland Security, Homeland Security Council, October 2007; *National Response Framework*, January 8, 2008.

²¹ National Strategy for Homeland Security, Homeland Security Council, October 2007.

²² *Ibid.*

²³ *Ibid.*

7. Planning Concepts.

a. Planning Categories. The two basic types of planning are contingency planning (also known as deliberate planning) and crisis action planning. Contingency planning is the cornerstone of homeland security planning and supports crisis action planning by anticipating potential crises and developing plans that facilitate timely selection of courses of action and execution planning during a crisis. Crisis action planning provides the means to transition from normal circumstances to heightened threats, emergency response, and recovery.

(1) General.

(a) Planning before an incident aims to prepare plans for the most dangerous potential threats that could affect the Nation; this is called *contingency planning*.

(b) Planning that takes place during an actual incident is called crisis action planning (CAP).

(c) Both aim to produce plans that will achieve a specific national objective for a given incident; that is, they are “execution” focused.

(d) Both use the same principles to develop a plan, although the speed at which planners conduct planning will typically increase and the approval process for planning products will be compressed in crisis action planning.

(e) Parallel planning describes those situations in which planning occurs concurrently across all planning levels for a specific scenario or threat. The higher planning level must still lead off the parallel planning effort to inform the next level’s planning. The key distinction characterizing parallel planning is that the lower planning level does not have to wait for the higher planning level’s approved plan to begin planning. This parallel effort is essential to speed up the process and allows participating organizations the maximum time to conduct their own planning. Parallel planning relies on accurate and timely notification from the higher planning level and a full sharing of information between planning levels as it becomes available.

(2) Contingency Planning. Contingency planning creates plans in anticipation of future incidents based on the most current information. A contingency is an incident that would involve national resources to prevent, protect from, respond to, or recover from terrorist attacks or natural disasters.

(a) Contingency planning facilitates the transition to crisis action planning; during crisis action planning, any contingency plan may become a crisis action plan. Contingency plans are prepared by senior agency leaders in response to requirements established by the Secretary and/or the President.

(b) Contingency planning is conducted before an incident. A contingency plan provides guidance for conducting operations for a given threat or scenario. It is conducted under non-emergency conditions, evaluated through training and exercises, and refined over time.

(c) Contingency plans are not immediately executed after they are approved. They are continually refined over time and provide planners a well-developed starting point that can be rapidly modified with little or no notice to support crisis action planning requirements.

(3) Crisis Action Planning. Crisis action planning occurs in response to a credible threat or in response to an incident. It occurs in a time-compressed environment with the objective of developing an imminently executable plan. Planners operating in a crisis action planning environment normally attempt to modify an existing contingency plan related to the incident threat or scenario. If a plan is unavailable, planners will develop a plan using crisis action planning.

(a) Because crisis planning is a continuation and derivative of contingency planning, the processes used for both should be as similar as possible. To the maximum extent possible, contingency planning should be the template for crisis action planning.

(b) Crisis action planning:

1 Is based on the circumstances that exist at the time the crisis begins,

2 Is based on current dynamic conditions rather than assumptions,

3 Is based on the time available and the scale of the crisis or incident,

4 Is conducted using parallel planning, with subordinate or supporting plans developed concurrently,

5 Converts (if possible) existing plans into crisis action plans,

6 Develops new plans when no useful contingency plan exists,

7 Conducts training and exercises using similar processes for preparing planners, and

8 Requires situational awareness of the incident site(s).

b. Homeland Security Planning Levels. There are three levels of homeland security planning—strategic, operational, and tactical.

(1) Strategic. At this level, decision makers determine strategic homeland security objectives across the homeland security spectrum (i.e., prevent, protect, respond, and recover). From these objectives, they develop overall, high-level guidance for planners. Using this guidance, planners develop strategic plans designed to apply resources to accomplish these objectives. These are the widest-scoped, least-detailed plans in the planning hierarchy. At this level, the goal is a unified approach across Federal agencies executing their statutory responsibilities.

(2) Operational. Strategic plans provide guidance for operational planning. Operational objectives support strategic objectives, sequence events, initiate action, and apply resources to begin and sustain activities. Operational planning is also conducted and sustained across the homeland security spectrum (i.e., prevent, protect, respond, and recover). Plans written at this level include CONPLANs and agency OPLANs. These plans are more narrowly scoped and more detailed than strategic plans. At this level, the goal is a unified approach across Federal agencies, but with more detail, when developing a CONPLAN. The goal is a unified approach across a Federal agency when developing an OPLAN.

(3) Tactical. Tactical planning is more focused and detailed than operational planning. Activities are focused on the arrangement of resources in relation to each other and to the threat or natural disaster. Tactical plans are developed to support the objectives of operations OPLANs. At this level, the goal is a unified approach across a Federal agency's components or sub-components.

c. Planning Approaches. There are three different approaches to planning, each focusing on different requirements, authorities, levels of operation, and specific organizational missions within the homeland security spectrum of operations.

(1) Capability-Based. This planning approach focuses on available personnel and resources that can be applied to address significant incidents. Requirements and capabilities are derived from the NPSs, strategic planning, risk assessments, concepts of operations, and threat information. This capabilities-based planning approach and the *NPG* foster vertical and horizontal integration of Federal, State, local, and Tribal plans allowing State, local, and Tribal capability assessments to inform Federal requirements and capabilities planning.

(2) Functional. A functional planning approach identifies a list of common tasks that an organization must perform during an incident, an emergency, a specific event or activity, or a directed requirement. These tasks are created at all operational levels and formatted in accordance with the standards of the parent organization. They may be developed in response to HSPD/National Security Preparedness Directive (NSPD) requirements, at the initiative of an organization's senior leadership, or in response to either national policy or a guidance document requirement.

(3) Scenario-Based. The Federal Government has developed 15 all-hazards planning scenarios (the NPSs) to facilitate homeland security planning. These planning tools represent the range of potential terrorist attacks and natural disasters and the related impacts that face the United States. A scenario-based plan is developed from an NPS; the 15 current NPSs have been grouped into 8 sets. Scenarios will be developed, updated, or amended as necessary at least every 2 years. This process will be informed by a risk-based analysis intended to focus planning efforts on the most likely or most dangerous threats to the homeland. Annex I to *HSPD-8* specifically addresses this planning approach.

8. Planning Organizations. Homeland security's complex and demanding nature requires a permanent planning organization with dedicated and trained planners.

a. The permanent planning organization's purpose is to conduct the continuous planning that addresses the homeland security requirements to prepare the United States for potential terrorist attacks, natural disasters, and other emergencies. The planners in this organization must have the skills and judgments normally gained through an extensive education, training, and assignment background. The planning organization will be routinely augmented by functional subject matter experts (SMEs) and liaison personnel from organizations that have a role in the homeland security operations being planned. Permanent planning organizations will often require additional duty planners who provide unique subject matter expertise for particular planning efforts. The leadership of the permanent planning organization must ensure these planners are trained and integrated into the planning effort seamlessly, and are insulated, as much as possible, from task assignments outside of planning.

b. Temporary planning organizations are formed for limited times to achieve limited planning objectives. They may be repeatedly formed and disbanded, or organized as exceptional circumstances require. However, these organizations should contain members whose full-time role is planning and can facilitate the organization's planning effort.

9. Planning Support Systems. Planning support systems are a class of decision-support systems that planners employ to help ensure they consider all viable options, weigh their potential value correctly, make and present recommendations, and make sound decisions. Planning support systems are a complement to, not a substitute for, individual and team skills and judgment. These support systems should be interoperable to ensure transparency of planning efforts across jurisdictions. Planning support systems include:

a. Communication Systems. Supporting communications systems must handle data, video, and voice, and process classified and unclassified information.

b. Planning Tools. Planning tools fall into two categories—automated and manual.

(1) Automated Planning Tools. Local systems should be, to the maximum extent possible, compatible with networked systems. Standardized firewalls, access protocols, and common software should be maximized. At the least, local systems must be used based on a common understanding and differences accommodated well in advance of need.

(2) Manual Planning Tools. Manual planning tools should be available to, and understood by, as much of the planning community as possible. Niche systems that are understood by only a small number of planners generally lead to misunderstanding and confusion in the rest of the community, which, in turn, leads directly to disjointed action.

Intentionally Left Blank

CHAPTER 3: PLANNING ROLES AND RESPONSIBILITIES

1. Purpose. This chapter identifies and assigns the planning roles and responsibilities for Federal agencies with a role in homeland security. The President may opt to provide adjustments in the assigned planning leads as necessary.
2. Secretary of Homeland Security. The Secretary is responsible for the following planning requirements.
 - a. Strategic Guidance Statement (SGS). The Secretary shall develop an SGS for each NPS set, in coordination with the heads of Federal agencies with a role in homeland security. Additional planning requirements shall be developed as the Secretary, in coordination with Federal agencies with a role in homeland security, deems appropriate. The Secretary shall appoint a development team for each SGS. The SGS shall be effective upon the Secretary's approval.
 - b. Strategic Plan. The Secretary shall develop a corresponding strategic plan for each approved SGS, in coordination with the heads of Federal agencies with a role in homeland security and the Director of the National Counterterrorism Center (NCTC)²⁴ for terrorism-related NPS. The Secretary shall appoint a development team for each strategic plan. A strategic plan must be completed no later than 90 days after the associated SGS is approved and shall be effective upon the Secretary's approval.
 - c. Concept Plan (CONPLAN). The Secretary shall develop a CONPLAN for each approved strategic plan, in coordination with the heads of Federal agencies with a role in homeland security and in consultation with appropriate State, local, and Tribal governments. A CONPLAN must be completed no later than 180 days after the associated strategic plan is approved and shall be effective upon the Secretary's approval.
 - d. Operations Plan (OPLAN).
 - (1) The Secretary shall review OPLANs in the interest of identifying gaps and seams, enhancing unity of effort, and linking plans to exercises. The intent of this feedback process is solely to identify potential operational shortfalls that might jeopardize the ability to achieve agreed upon strategic objectives. Any identified potential shortfalls shall be resolved in as direct a manner possible, leaving difficult-to-resolve issues to the appropriate interagency policy coordination process.
 - (2) The Secretary shall develop and update, as required, the detailed process for sharing and review of Federal agency OPLANs, including special considerations and exceptions, as appropriate, in coordination with Federal agencies with a role in homeland security.
 - e. IPS Update. The Secretary shall review and update the IPS 1 year following its issuance and biennially thereafter, in coordination with Federal agencies with a role in homeland security, State governments, the private sector, and NGOs, as appropriate. The Secretary shall, through the Assistant to the President for Homeland Security and Counterterrorism, submit the revised IPS to the President for his approval.

²⁴ Consistent with section 119 of the National Security Act of 1947, as amended (50 U.S.C. 404o).

3. Director of National Intelligence (DNI) and the Director of the National Counterterrorism Center (NCTC).

a. Strategic Plan. After the approval of a terrorism-related SGS, the Director of NCTC (consistent with section 119 of the National Security Act of 1947, as amended (50 U.S.C. 404o)) shall support the development of corresponding counterterrorism strategic plans, in coordination with the heads of Federal agencies with a role in homeland security and the Secretary of Homeland Security. NCTC, as a component of the Office of the DNI (section 102a of the National Security Act of 1947, as amended (50 U.S.C. 403-1)), shall report to the DNI on intelligence operations. On the planning and progress of joint counterterrorism operations NCTC shall report to the President, pursuant to Section 119(c) of the National Security Act of 1947, as amended (50 U.S.C. 404o (c)).

b. It is a primary mission of NCTC to conduct planning for counterterrorism activities, integrating all instruments of national power, including diplomatic, financial, military, intelligence, homeland security, and law enforcement activities within and among agencies. NCTC also assigns roles and responsibilities as part of its planning duties to lead departments or agencies, as appropriate, for counterterrorism activities that are consistent with applicable law and that support counterterrorism plans, but shall not direct the execution of any resulting operations.²⁵

c. The DNI, through the Director of NCTC, shall conduct planning for counterterrorism efforts of the U.S. Government and for the effective integration of counterterrorism intelligence and operations across agency boundaries, both inside and outside the United States.²⁶

d. The DNI, through the Director of NCTC, shall monitor the implementation of plans, and shall obtain information from each element of the Intelligence Community, and from each other department, agency, or element of the U.S. Government relevant for monitoring the progress of such entity in implementing such plans.²⁷

4. Federal Agency Heads with a Role in Homeland Security. Agencies with existing planning processes shall ensure their OPLANs are compatible with the IPS.²⁸ Agencies with no existing planning processes shall adopt the IPS.

a. OPLAN. The agency head shall develop an OPLAN to execute the roles and responsibilities assigned to the agency in each CONPLAN. These OPLANs shall be developed by an agency's internal planners and shall be approved by the head of each agency or designated representative. An OPLAN must be completed no later than 120 days after the associated CONPLAN is approved.

b. Tactical Plan. At the discretion of each agency head, an agency may develop a tactical plan to provide detailed information regarding how that agency will execute the responsibilities described in an OPLAN.

c. Plan Sharing. The agency head shall share completed OPLANs and, at the discretion of the agency head, tactical plans or information across the IPS planning community.

²⁵ Intelligence Reform and Terrorism Prevention Act of 2004, Section 1021.

²⁶ Ibid

²⁷ Ibid.

²⁸ The IPS replaces the NPES.

The agency head shall inform the Secretary when the need to protect highly sensitive or classified information prevents the sharing of an OPLAN in the form and manner developed by the Secretary. If an agency head is unable to share an OPLAN, the agency shall make other efforts, which may include providing a briefing on the OPLAN, to assist the Secretary in accomplishing the goals of identifying gaps and seams, enhancing unity of effort, and linking plans to exercises.

d. Estimated Costs. Beginning in Fiscal Year 2010, as part of regular budget submissions to the Director of the Office of Management and Budget (OMB), each Federal agency shall incorporate into its overall mission priorities and guidance constraints the estimated costs (i.e., proposed funding), if any, of:

- (1) Its role in Federal strategic, operational, and tactical planning; and
- (2) Executing its responsibilities under any approved OPLAN.

5. General Responsibilities.

a. All Federal agencies have some level of responsibility to support the IPS, including:

- (1) Identifying their existing authorities, responsibilities, and capabilities that address their unique role(s) for the prevention, protection, response, and recovery mission areas;
- (2) Actively participating with interagency leads in developing plans at the strategic, operational, and tactical planning levels, as appropriate;
- (3) Reviewing those items in (1) in the context of their necessary participation to determine how best to apply these capabilities in support of the comprehensive planning effort; and
- (4) Engaging in exercise, assessment, and evaluation programs to continuously improve and update the plans that each stakeholder is supporting.

6. Planning Communities of Interest (COI). The following list identifies planning COIs for homeland security operations. It is not all inclusive; additional members will be added as they are identified.

a. Key Federal Interagency:

- (1) Department of Agriculture (USDA)
- (2) Department of Commerce (DOC)
- (3) Department of Defense (DOD)
- (4) Department of Education (ED)
- (5) Department of Energy (DOE)
- (6) Department of Health and Human Services (HHS)
- (7) Department of Homeland Security (DHS)
 - (a) Federal Emergency Management Agency (FEMA)
 - (b) Infrastructure Protection Division (Executive Agent for the

National Infrastructure Protection Plan (NIPP))

- (c) Office of Operations Coordination
 - (d) U.S. Coast Guard (USCG)
 - (8) Department of Housing and Urban Development (HUD)
 - (9) Department of the Interior (DOI)
 - (10) Department of Justice (DOJ)
 - (a) Federal Bureau of Investigation (FBI)
 - (11) Department of Labor (DOL)
 - (12) Department of State (DOS)
 - (13) Department of Transportation (DOT)
 - (14) Department of the Treasury (TREAS)
 - (15) Department of Veterans Affairs (VA)
 - (16) Environmental Protection Agency (EPA)
 - (17) Federal Communications Commission (FCC)
 - (18) General Services Administration (GSA)
 - (19) National Aeronautics and Space Administration (NASA)
 - (20) National Transportation Safety Board (NTSB)
 - (21) Nuclear Regulatory Commission (NRC)
 - (22) Office of the Director of National Intelligence (ODNI)
 - (a) Intelligence Community (IC)
 - (23) Office of Personnel Management (OPM)
 - (24) Small Business Administration (SBA)
 - (25) Social Security Administration (SSA)
 - (26) Tennessee Valley Authority (TVA)
 - (27) U.S. Agency for International Development (USAID)
 - (28) U.S. Postal Service (USPS)
- b. Other:
- (1) State, local, and Tribal governments
 - (2) Non-Governmental and Volunteer Organizations
 - (a) American Red Cross (ARC)
 - (b) Corporation for National and Community Service
 - (c) National Organization on Disability
 - (d) National Voluntary Organizations Active in Disaster (NVOAD)
 - (3) Private Sector

(4) Other

Intentionally Left Blank

CHAPTER 4: VERTICAL AND HORIZONTAL PLANNING INTEGRATION

1. Purpose. This chapter summarizes the planning considerations that shape the integration of plans within and among all levels of government. It also outlines the links between Federal and State prevention, protection, response, and recovery operations for planning purposes. Finally, this chapter discusses the role of national-level exercise and training programs in ensuring integration at all levels of government.

2. Background

a. The *NIP-WOT*, *NIPP*, and *NRF* were developed to help expedite Federal planning and support addressing terrorism and other catastrophic incidents across the spectrum of homeland security operations.

b. The Robert T. Stafford Disaster Relief and Emergency Assistance Act, Public Law 93-288, as amended, authorizes the Federal Government to respond to disasters and emergencies to provide State and local governments with assistance to save lives and protect public health, safety, and property. In general, the *NRF* is implemented when the State's resources are not sufficient to cope with a disaster and the State's governor has requested Federal assistance. The *NRF* uses existing plans, planning relationships, and standing agreements to share resources as the foundation for conducting flexible, adaptive, and robust emergency operations.

c. The terrorist attacks of September 11, 2001, Hurricanes Katrina and Rita, and other major incidents illustrate the need for all levels of government, the private sector, and NGOs to prevent, protect against, respond to, and recover from a wide spectrum of possible events and scenarios that would exceed the capabilities of any single entity.

d. To address the need for a unified and coordinated national approach to planning and to domestic incident management, the President signed several HSPDs. The ultimate goal of these directives is to develop a common, nationwide approach to prevention, protection, response, recovery planning. The following HSPDs are of particular importance to planners:

(1) *HSPD-5, Management of Domestic Incidents*, identifies steps to enhance the ability of the United States to manage domestic incidents by establishing a single, comprehensive national incident management system.

(a) HSPD-5 identifies the Secretary as the principal Federal official for domestic incident management. Pursuant to the Homeland Security Act of 2002, the Secretary is responsible for coordinating Federal preparedness activities and operations within the United States to respond to, and recover from terrorist attacks, major disasters, and other emergencies. The Secretary shall coordinate the Federal Government's resources used in response to or recovery from terrorist attacks, major disasters, or other emergencies if and when any one of the following four conditions applies:

1 A Federal agency, acting under its own authority, has requested the assistance of the Secretary;

2 The resources of State and local authorities are overwhelmed, and Federal assistance has been requested by the appropriate State and local authorities;

3 More than one Federal agency has become substantially involved in responding to the incident; or

4 The Secretary has been directed to assume responsibility for managing the domestic incident by the President.

(b) The Secretary will also:

1 Coordinate with State and local governments to ensure adequate planning, equipment, training, and exercise activities;

2 Provide assistance to State and local governments to develop all-hazards plans and capabilities, including those of greatest importance to the security of the United States, and will ensure that State, local, and Federal plans are compatible; and

3 Coordinate with the private and nongovernmental sectors to ensure adequate planning, equipment, training, and exercise activities and to promote partnerships to address incident management capabilities.

(c) HSPD-5 also identifies the Attorney General as the coordinator of law enforcement activities to detect, prevent, preempt, and disrupt terrorist attacks against the United States.

(2) *HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection*, establishes a national policy for Federal agencies to identify and prioritize United States CIKR and to protect them from terrorist attacks. It gives the Secretary responsibility for coordinating the overall national effort to enhance the protection of the CIKR. The Secretary serves as the principal Federal official to lead, integrate, and coordinate implementation of efforts among Federal agencies; State, local, Tribal governments; and the private sector to protect CIKR.

(3) *HSPD-8, National Preparedness*, describes the way Federal agencies will prepare for an incident. It requires DHS to coordinate with other Federal agencies and with State, local, and Tribal governments to develop a National Preparedness Goal.

(4) *HSPD-8, Annex I, National Planning*, describes a common Federal planning process that supports development of a family of related planning documents. The IPS concept provides the Federal Government with a consistent direction and delineation of authorities, responsibilities and requirements, common terms of reference, and plans based on shared assumptions.

(5) *HSPD-20, National Continuity Policy*, establishes the national policy on the continuity of Federal Government structures and operations. It describes eight National Essential Functions and provides guidance on continuity of government and operations for State, local, and Tribal governments and private sector organizations to ensure rapid and effective response to and recovery from national emergencies.

(6) *The National Response Framework (NRF)*. The *NRF* is a guide to how the nation conducts all-hazards incident response. It uses flexible, scalable, and adaptable

coordinating structures to align key roles and responsibilities across the Nation. It captures specific authorities and best practices for managing incidents that range from the serious but purely local, to large-scale terrorist attacks or catastrophic natural disasters. The *NRF* was written to expedite Federal support to State and local governments' planning for response to and recovery from terrorism incidents, large-scale disasters, and catastrophic events. In general, the *NRF* is implemented when the State's resources are not sufficient to cope with a disaster, and the State's governor has requested Federal assistance. The *NRF* uses existing plans, planning relationships, and standing agreements to share resources as the foundation for conducting flexible, adaptive, and robust emergency operations.

3. The Relationship Between Federal and State, Local, and Tribal Planning. Federal, State, local, and Tribal planning describe each respective government's approach to operations. Because these levels of government all provide support to operations conducted at the local level, there are similar and overlapping functions in their plans.

a. Planning must be coordinated vertically among all levels of government to ensure a singular operational focus. As key concepts for a national planning structure, integration and synchronization serve different but equally important purposes in linking Federal plans and State, local, and Tribal plans. The goal is to ensure the effectiveness of combined Federal and State, local, and Tribal operations through integration and synchronization.

b. From the Federal Government perspective, integrated planning helps define how its agencies and departments add the right resources at the right time to support State and local operations. From the States' perspective, it provides answers to questions about working with other organizations and obtaining resources. Figure 4.1 shows the relationships among Federal, State, local, and Tribal planning efforts.

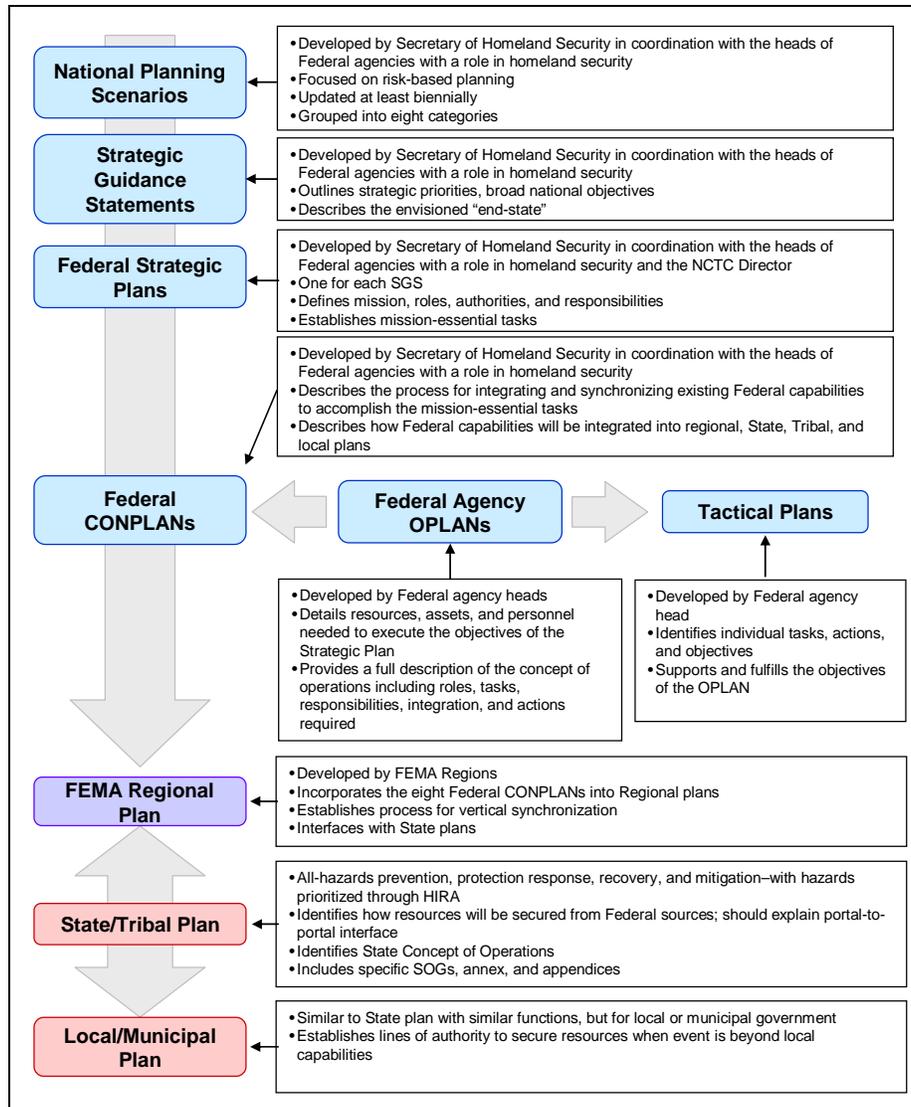


Figure 4.1 Federal and State Planning Relationships

c. Horizontal Integration. Horizontal integration is the blending of a government's effort across all agencies and departments to ensure a coordinated approach to planning for major emergencies, disasters, and catastrophes no matter their origin. The Federal Government's approach is described below; *CPG 101* describes the State and local approach.

(1) Effective integration requires each Federal agency with a role in homeland security to create a planning capability and to support interagency planning efforts. A resident planning capability will allow these agencies to integrate their planning effort with the overall interagency effort.

(2) Horizontal integration also requires interagency collaboration at the strategic, operational, and tactical levels.

(3) Horizontal integration requires a senior-level forum for conflict resolution that addresses issues Federal agencies are unable to resolve as part of the normal planning

process. At the Federal level, horizontal integration is accomplished through the *HSPD-1* process.²⁹

d. Vertical Integration. Vertical integration is the linking of planning and operations both up and down the various levels of government (Federal ↔ State ↔ Tribal/Local). The goal of vertical integration is to provide consistency of process despite different planning requirements. From the Federal perspective, only those departments and agencies whose statutory authority allows them to interact with State, local, and Tribal authorities participate in vertical integration. In some cases, one agency (e.g., FEMA) conducts the integration effort for many other Federal government entities.

(1) The vertical integration process balances the Federal Government's requirements to execute national homeland security strategies while supporting the operational requirements of State, local, and Tribal governments. This is accomplished by:

(a) Establishing a consistent planning approach across all levels of government; and

(b) Identifying the interface points in the planning process for each adjoining level of government.

(2) Federal planning must be based on the requirements of State, local, and Tribal partners so that the Federal Government can provide the necessary support. The IPS provides a common process for State, local, Tribal, NGOs, and private sector to provide essential input to Federal planners.

(3) Additionally, it is possible that traditional roles are reversed, and State, local, and Tribal officials are acting in support of the Federal Government.

e. Supporting Planning Elements. At any particular level of government, the key to successful planning is to plan as a team. A concept similar to this teaming approach exists for integrating plans across governmental levels. To accomplish the plan integration described above, the following elements need to be in place.

(1) Planning Process. A set of mutually agreed upon planning practices, cycles, and procedures supported by current and emerging technologies that provides professional planners with a capability to develop and maintain plans and conduct combined homeland security operations;

(2) Planning Network. A formal means to coordinate plans and jointly identify operations goals, roles, relationships, resources, and structures that best accomplish the activities necessary for successful operations; and

(3) Planning Community. A trained group of planners involved in prevention, protection, response, and recovery operations. Planning communities may also include NGOs and private sector elements as appropriate.

f. FEMA Regional Planning. FEMA-developed regional plans address actions and activities taken by FEMA regional offices in coordination with Federal agencies and in consultation with States to support integrated and synchronized Federal, State, local, and Tribal operations.

²⁹ *Homeland Security Presidential Directive-1*, October 29, 2001, Organization and Operation of the Homeland Security Council.

g. The FEMA Region plays a critical role in enabling state-to-state cooperation, coordinating disparate capabilities across its region, and serving as the translator between national-level planning requirements and State planning requirements. FEMA Regions determine capability gaps, resource shortfalls, and State expectations for Federal assistance through the process of the gap analysis method that best fits the need.

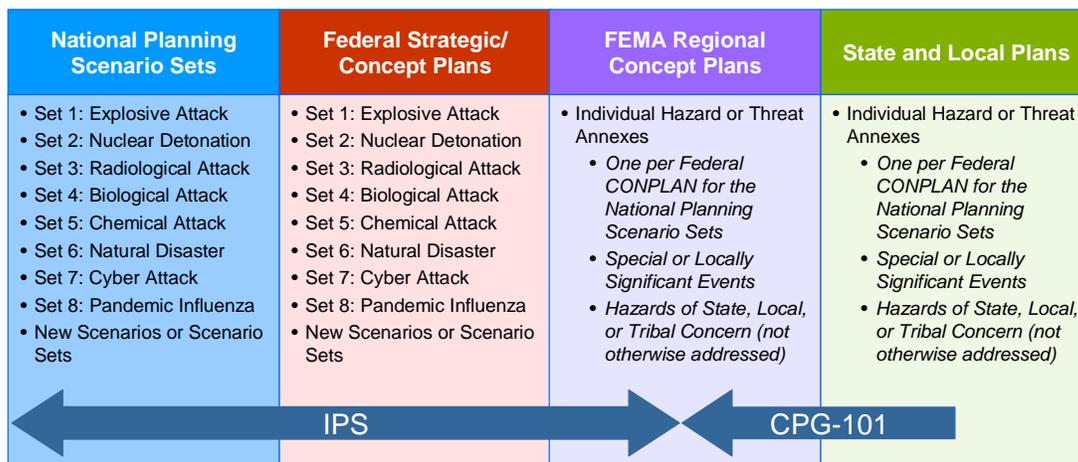


Figure 4.2 Linkages between Federal, and State and Local Planning

h. Regional planning may include development of plans, synchronization matrices, or annexes to:

- (1) Assist Federal agencies and their State counterparts in describing and documenting their relationship, concepts of operations, operational priorities, operational concerns, and/or needs;
- (2) Provide information to the States on the various response mechanisms, capabilities, and resources available to them through the Federal Government;
- (3) Include organizational tasking and implementing instructions for accomplishing the actions agreed upon in the Region/State Memoranda of Understanding (MOUs) where applicable;
- (4) Identify and propose remedies to address conflicts or omissions among multiple Federal and State plans that may be simultaneously executed across the region in response to one or more incidents;
- (5) Ensure the scope and concept of operations of these plans are sufficient to accomplish the full range of Federal and State homeland security tasks; and
- (6) Clarify authorities, roles and responsibilities, and task assignments where necessary.

i. State Plans. State plans address multiple operational functions across all mission areas in addition to providing resources to satisfy unmet local needs. These functions focus on actions—such as the special event security, direction and control, warning, public notification, and evacuation—that the State must take.

4. Exercises. Regularly performing simulated disaster exercises at all levels of government has proven beneficial in enhancing the capabilities and operational readiness of participating organizations. Exercises are valuable because planners and operators can use them to evaluate the efficiency and effectiveness (i.e., strengths and weaknesses) of a plan(s) or process. Exercises that are tied into a comprehensive lessons learned program have proven essential to improving effectiveness. To the maximum extent possible, Federal agencies must remain cognizant of exercise resource requirements in order to allow full participation.

a. The National Exercise Program (NEP) serves as the principal mechanism for examining the preparation and efficiency of Federal agencies. It provides a system that aligns Federal and State, local, and Tribal exercise programs and objectives with U.S. Government-wide priorities to prevent and respond to domestic terrorist attacks, major disasters, and other emergencies. NEP also provides a method to examine emerging policy issues and to determine procedures to implement or modify them.

b. NEP works to align all Federal, State, local, and Tribal exercises into a comprehensive and cost-effective program. By using NEP to assess their ability to prevent, protect, respond to, and recover from the effects of hazards and threats, all agencies at all levels of government are able to ensure better preparation for and response to any incident.

5. Training. The fundamental role of training is to equip the homeland security workforce with the skills and knowledge to perform their roles and ensure a qualified workforce. The overarching goal is to promote a more effective and integrated workforce that can deliver the right skill sets to the right place at the right time. Achieving this requires leveraging training resources to ensure the timely delivery of relevant education and developing and supporting initiatives that increase the collective ability of all levels of government to address major disasters and catastrophic events.

a. Training constitutes a key element that prepares and allows personnel to meet the goals and objectives of the IPS. Planning participants at all levels should be trained in the IPS process to achieve the desired end state of a standardized, coordinated, and synchronized family of plans. Similarly, users of plans at all levels must receive training on the plans that are generated, as well as have a basic understanding of the process used to create those plans. It is Federal policy that planners at all levels of government have opportunities for education, training, and practical experience in order to develop a professional planning community.

b. Planners and the users of plans must have the necessary knowledge to mitigate a range of threats. Existing emergency responder training programs support all levels of government by serving as a central resource for the creation, management, and dissemination of high-quality preparedness training and related products. Through cooperative and inter/intra-agency agreements, an effective training program maintains multiple partnerships with institutions of higher education, NGOs, and other groups to support training activities across a variety of program areas (e.g., agro-terrorism, cyber-terrorism, intelligence, transportation, port security). The partnerships supported by current efforts include the National Domestic Preparedness Consortium, the Rural Domestic Preparedness Consortium, and approximately 45 other training providers.

c. The *National Strategy for the Development of National Security Professionals* sets forth a framework that provides security professionals access to integrated education, training, and professional experience opportunities to enhance their mission-related knowledge,

skills, and experience and thereby improves their capability to safeguard the security of the Nation. Opportunities are provided across organizations, levels of government, and incident management disciplines, as appropriate. In accordance with this policy, agency heads with national security functions should identify and enhance existing national security professional development programs and infrastructure, and establish new programs, as necessary, to fulfill their respective missions to educate, train, and employ security professionals.

d. The *National Strategy for the Development of National Security Professionals* further assigns responsibility to the Secretary to develop a program to provide Federal, State, local, and Tribal government officials with education in disaster preparedness, response, and recovery plans and authorities, and training in crisis decision-making skills. Consistent with this policy, the Secretary will define, organize, and offer IPS-related training throughout the various levels. It is the intention of the DHS Secretary to:

- (1) Use established systems to incorporate IPS- and *CPG-101*-related training;
- (2) Augment existing training to standardize planning in accordance with IPS and *CPG-101*;
- (3) Tailor training for the appropriate level of planning (i.e., strategic, operational, and tactical), level of government (i.e., Federal, State, local, and Tribal), type of organization (i.e., government, NGO, and private sector), and/or role of the persons attending training within the IPS and *CPG-101*;
- (4) Integrate IPS- and *CPG-101*-related training with established training programs;
- (5) Through appropriate interagency collaboration, establish certification standards and professional levels for planners.

CHAPTER 5: FEDERAL PLAN DEVELOPMENT PROCESS

1. Purpose. This chapter outlines the process for developing Federal SGS, strategic, concept, operations, and some tactical plans. The Federal plan development process is compliant with *NIMS*; the *NIMS* planning process will still be used for developing Incident Action Plans.

2. Definitions. The following subparagraphs describe key planning documents defined by Annex I to *HSPD-8*. For scenario-based planning, Annex A provides the appropriate format for Federal SGS, Strategic Plans, and CONPLANS and the recommended format for agency OPLANS.

a. Strategic Guidance Statements. An SGS outlines broad strategic priorities, broad national strategic objectives, and basic assumptions. It describes the envisioned end state and establishes the general means necessary to accomplish that end. An SGS is developed for each of the NPS sets. Each SGS provides guidance to selected Federal agencies that will support the development of each strategic plan. A Secretary of Homeland Security-approved SGS formally initiates the Federal planning process. An SGS does not provide specific planning details; details will be addressed in the Strategic and CONPLANS. An SGS addresses prevention, protection, response, and recovery operations and formally initiates the Federal planning process.

b. Strategic Plan. Strategic plans define the Federal mission, identify authorities, delineate roles and responsibilities, establish mission-essential tasks, determine required and priority capabilities, and develop performance and effectiveness measures to meet the SGS intent.

c. CONPLAN. A CONPLAN describes the concept of operations for integrating and synchronizing existing Federal capabilities to accomplish the mission-essential tasks, and describes how Federal capabilities will be integrated into and support regional, State, local, and Tribal plans. They also provide the operational level guidance to support developing Federal agency OPLANS.

d. OPLAN. OPLANS identify detailed resource, personnel, and asset allocations in order to execute the objectives of the strategic plan and execute strategic operational priorities. An OPLAN contains a full description of the concept of operations, including specific roles and responsibilities, tasks, integration, and actions required, with support function annexes, as appropriate.

e. Tactical Plans. Tactical plans identify and develop individual tasks, actions, and objectives tailored to specific situations and fact patterns at an operational level. Tactical planning supports and fulfills the OPLAN objectives. Tactical plans may use IPS or the *NIMS* planning process.

3. National Planning Priorities. The Federal Government's homeland security planning priorities are directly affected by changes in national policy and guidance as well as national-level strategic assessments (e.g., Quadrennial Homeland Security Review). Additionally, updates in intelligence estimates and threat assessments may demand changes in our priorities. Currently, the Federal Government maintains a prioritized list of scenarios for developing SGSs and corresponding strategic plans, CONPLANS, and OPLANS.

a. NPSs include steady-state security postures, homeland security threat scenarios, and incident prequels for the terrorist scenarios, and are used for national planning by and among

all levels and jurisdictions of government, and in coordination with private, non-profit, and volunteer organizations.

b. These scenarios are intended to assist planners in prioritizing the application of resources and capabilities toward a specific end and should not limit planning for additional threats and concerns.

c. The scenarios will be revised, updated, or amended biennially or more frequently if necessary. Planning will use the most current version of these sets.

4. Federal SGS Development. SGS development uses a different process than that used for strategic and concept plans. Paragraph 5 below describes the process for developing Federal plans. Federal planners shall consult with NCTC regarding the scope of plans involving terrorist attack scenarios. This consultation should determine prevention activities to be addressed in the strategic plan to ensure consistency with the *NIP-WOT*.

a. SGS Preparation. Once the designated planning team receives direction from the appropriate authority to start developing the SGS, it accomplishes the following:

(1) Determine National Level Planners and SMEs. The planning team determines the membership of the planning and SME COI.

(2) Identify Strategic Priorities. The planning team identifies the strategic priorities from the relevant strategic documents (e.g., National Homeland Security Strategy, Presidential Directives, national strategies). This list is not all inclusive; the planning team must use as many sources as feasible.

(3) Identify National Strategic Objectives. The planning team identifies the strategic objectives for prevention, protection, response, and recovery operations. In addition, objectives common to all these mission areas are identified.

(4) Develop Basic Assumptions. The planning team develops assumptions that frame planning for the Federal mission areas of prevention, protection, response, and recover.

(5) Describe Federal End-State. The planning team describes the end-state for Federal prevention, protection, response, and recovery operations.

(6) Identify the General Means to Achieve End-State. The planning team identifies organizations, resources, and major activities to support Federal prevention, protection, response, and recovery operations for the selected scenario.

(7) Develop Planning Guidance. The planning team identifies planning roles and responsibilities for the planning COI, any modifications to the existing planning process, instructions on when the plan is due, any planning limitations that will affect planning, and policy guidance.

(8) Federal Planning Team Review.

(a) As part of SGS development, the planning team lead shall distribute the draft SGS to interagency planning team members for informal review and comment.

(b) The SGS, including any attachments, must be marked with the appropriate classification. Classified attachments may be transmitted and stored separately if the SGS is unclassified. The SGS shall contain a notice identifying the classified portion and how it can be obtained.

(c) The planning team shall adjudicate comments received during this review in coordination with counterparts with a role in the planning scenario. Comments that remain an issue shall be highlighted for the next review.

(d) The planning team will provide the draft SGS to the appropriate policy coordination body to distribute for initial review.

b. SGS Review. A Federal SGS is subject to two formal Federal interagency reviews before being approved by the Secretary.

(1) Initial Review. Initial SGS review is conducted by Federal agency designated representatives below the Assistant Secretary level.

(2) Initial Review Adjudication. Federal planners representing the Secretary, and the Director of NCTC for counterterrorism plans, shall adjudicate comments received and submit the final SGS review package for distribution by the appropriate policy coordination body.

(3) Final Review. Final SGS review is conducted by Federal agency representatives at the Assistant Secretary level.

(4) Final Review Adjudication. The Secretary shall adjudicate comments received during this review in coordination with counterparts from Federal agencies with a role in the planning scenario, including the Director of NCTC for counterterrorism plans.

c. SGS Approval and Dissemination.

(1) After concurrence by the appropriate policy coordination body, Federal planners representing the Secretary, and the Director of NCTC for counterterrorism plans, shall submit the SGS for the Secretary's approval.

(2) After approval by the Secretary, the SGS shall be disseminated by the Secretary to the planning COIs. Dissemination will be by the most expeditious manner within the bounds of operational security.

(3) An approved SGS triggers the start of the strategic plan development, which uses the process described in paragraph 5 below.

5. Federal Strategic Plan and CONPLAN Development. This process is designed to facilitate Federal planning in a coherent and logical manner. Each phase has a series of steps to provide a comprehensive analytical approach to the development, coordination, and approval of each Federal strategic plan and CONPLAN. This process can be used for planning in anticipation of future incidents (i.e., contingency) or during an actual threat or incident (i.e., crisis action). The primary differences between these situations are the time available for producing the plans and information available to conduct planning.

a. Phase 1: Understand the Situation. Federal planners receive guidance to begin planning from higher authority. The phrase "Federal planners" encompasses those personnel with Federal agencies that have been appointed and trained to plan for their respective agencies.

The phrase “higher authority” will depend on the organization to which a Federal planner is assigned. For example, a planner within a Federal agency will receive guidance from the President of the United States. A planner within a Federal agency’s component (e.g., FBI, Transportation Security Administration, Centers for Disease Control and Prevention) would receive guidance from the Secretary of the respective Federal agency. The mechanism that directs Federal planners to begin planning for each type of plan is identified below.

(1) Initiate Preparations for Planning.

(a) *Form a Collaborative Planning Team.* The person responsible for planning homeland security operations should consider establishing a dedicated and permanent planning team or teams depending on the actual or anticipated tasking from higher authorities. This planning team will collaborate with other planning teams within the planning COI for a given planning effort. An experienced planner should be designated as the team chief.

1 This planning team should have an understanding of homeland security strategy and operations across prevention, protection, response, and recovery mission areas. In addition, the team should be intimately familiar with the planning process. Requirements for team size and expertise will vary depending on the planning level.

2 A sound organizing process has a core membership drawn from SMEs from all organizations that may participate in the operation. This core team should be able to draw on other experts within their respective organizations.

(b) *Develop Planning Staff Estimates.* A staff estimate consists of significant facts, events, conclusions (based on current or anticipated situations), recommendations on how available resources can be best used, and what additional resources are required. Failure to make estimates can lead to errors and omissions when developing, analyzing, and comparing courses of action.

1 These estimates will address specific functional areas such as intelligence on terrorist threats or status of homeland security resources. Specific planning team members should be tasked to maintain specific estimates.

2 Staff estimates should be developed well in advance of a specific planning requirement and continually updated. Existing estimates provide a starting point for planning. Subject matter areas for estimates will include the following, but may address other areas depending on the specific operation and planning level:

a A *leader estimate* addresses the mission received, the time available for planning and executing; the environment in which the operation will occur (this encompasses jurisdictional issues as well as physical environment), likely courses of action the leader may want planners to consider, and other subjects as the leader deems necessary. The term “leader” refers to the person who is responsible for executing the operation being planned. The leader is typically the Federal agency head within the context of Federal agency operations. The Secretary of Homeland Security meets this definition exercising his role under *HSPD-5*.

b An *intelligence/information estimate* addresses intelligence assessments on terrorist threats, information on natural disasters, the likely effects of attacks and natural disasters, and required capabilities to collect intelligence/information.

c A *resource estimate* addresses availability of personnel and assets for the operation.

d A *communication estimate* addresses the ability of the organization responsible for the operation to plan and execute successfully.

(2) Conduct Research. In this step, the leader responsible for homeland security operations (henceforth, the leader) assesses the tasking from higher authority and makes planning preparations.

(a) Conducting research begins with the receipt or anticipation of a new mission and ends with notifying Federal Government planning COIs that planning has started. A new mission can come from guidance issued by the higher authorities or can be derived from an ongoing operation. This guidance will vary according to planning level—at the strategic level, guidance will come from the President of the United States; at the operational level, guidance will come from a Department Secretary; at the tactical level, guidance will come from the component leader in a specific Federal agency.

(b) A mission identifies the task and purpose of an operation. A mission statement should be clear and unambiguous; confusion regarding a mission will typically end in failure of the operation or excessive costs. Planners must request additional guidance if the mission received from higher authority is ambiguous or confusing.

(c) The leader will then notify the appropriate Federal planning COIs. It is essential that the leader contact the leaders of those organizations that will play a critical role in the intended operation. To ensure mission success, the leader must garner support from his/her counterparts to ensure planning occurs in a collaborative and integrated manner.

(d) Preparations for planning are best described in a standard operating procedure. This procedure should describe when planning meetings will be held and specify who should attend. These procedures should be made available to all participants expected to be involved in planning.

b. Phase 2: Determine Goals and Objectives.

(1) Information Analysis. Information analysis is the most critical step because it drives the rest of the entire decision-making process. It defines the incident problem and initiates the process of determining feasible solutions—the COAs. It allows the leader and his/her planning team to develop a clear understanding of the current situation related to the threat and the environment, envision a desired end-state, and then visualize the sequence of activity that will achieve the end-state. The keys to successful analysis are preparation, professional competence, and the identification of the operation's purpose and all its essential tasks. A thorough analysis focuses the efforts of the leader and the planning staff, thereby saving time.

(a) *Identify Critical Facts and Assumptions*. During this step, the planners identify critical facts and assumptions.

1 Facts are statements of known data concerning the incident, threat, available resources/capabilities, and material readiness. Facts are what is known and can be substantiated.

2 Assumptions consist of information accepted by planners as true in the absence of facts. Assumptions are not predictions; an event assumed may not come about, but planning for the event ensures resources are available.

a An assumption is appropriate if it passes the tests of “validity” and “necessity.” An assumption is not valid if there is little possibility that the assumption is likely to be true. “Necessity” means the assumption is essential to planning.

b Decision makers replace assumptions with facts when they execute a plan. Planners should use assumptions sparingly and put great effort into doing research and acquiring facts.

(b) *Update Staff Estimates.* Staff estimates continue to be updated throughout this step to assist the leader in decision making. Information analysis, facts and assumptions, and the situation analysis provide the staff estimate’s structure. Planners responsible for these estimates should ensure they remain as current as practicable.

(c) *Develop Threat/Hazard Scenario.* A threat/hazard scenario describes what the planned operation will counter. Planners will use the *NPS* as a starting point for scenario-based planning. A threat/hazard within the context of homeland security operations spans the homeland security mission areas of prevention, protection, response, and recovery. For example, a team planning to prevent terrorist attacks would express the threat as the method a terrorist group would use to conduct an attack. In contrast, a team planning to respond to the terrorist attack would express the threat/hazard as the attack’s effects (i.e., potential casualties, the extent of radioactive contamination, damage to critical infrastructure, etc.).

(d) *Develop Objectives.* The leader, with the assistance of the planning team, will develop objectives that articulate what the organization must do to succeed with respect to the threat, the environment, and the desired end-state. The objectives link the mission and the concept of the operations by stating the key tasks that, along with the mission, are the basis for subordinates to exercise initiative when unanticipated opportunities arise or when the original concept of the operations no longer applies. Planners will use the information developed under this subparagraph to prepare a draft of the leader’s intent statement for the appropriate planning level.

1 The leader develops objectives using the objectives from his/her superior and may modify these objectives during or after the analysis briefing. These objectives describe a broader purpose that looks beyond the purpose of the immediate operation to the broader operational context of the mission.

2 The leader’s objectives do not include the “method” by which the organization will get from its current state to the end-state; the concept of operations is the method. The objectives do not address “acceptable risk;” risk is stated in the leader’s guidance and is addressed in all COAs. If purpose is addressed in the objectives, it does not restate the mission statement’s purpose.

(e) *Develop Tasks.* Tasks are not tied to a specific COA; rather they identify what is fundamental to the agency’s success.

1 Planners will identify specified tasks from the guidance sent by higher authority. The planners will then determine any implied tasks in each of those specified tasks. Finally, the planners will determine which tasks are essential to mission

accomplishment; these are the essential tasks. Normally, all specified tasks are essential, while a few implied tasks will be considered key.

2 Essential tasks are those that must be performed by the agency, or conditions that must be met, to achieve the stated purpose of the operation. Subordinates use essential tasks to ensure their efforts continue to support the senior leader's goals when the circumstances change, when significant opportunities present themselves, or when the COA no longer applies. The operation's tempo, duration, and effect on the threat are examples of essential tasks.

(f) *Develop Mission Statement.* The planners will then develop a mission statement and desired end-state for approval by the leader using the essential tasks and objectives from the previous steps. The mission statement must address, clearly and unambiguously, who will conduct the operation, what will be accomplished by the operation, and why the operation is being conducted. If known, the mission will also address when and where the operation will be conducted.

(g) *Identify Available Resources.* Planners will also determine what resources and conditions are required for mission success. Planners will then ascertain any resource shortfalls when they compare resources needed for the operation with the resources actually available. Shortfalls critical to mission success must be identified to higher authority for resolution prior to the operation, if practicable. Planners should also develop work-arounds for any identified shortfalls.

(h) *Brief Senior Leader(s).* Planners will brief the completed information analysis to the leader of the organization responsible for the operation. The leader should invite leaders from planning COIs that will be key participants of the operation. If the leader accepts the results of information analysis, he/she will direct the planning team to begin COA development. The leader has the option to provide detailed guidance to the planning team on specific COAs to investigate or may give broad guidelines on potential COAs. If the leader rejects the results of the analysis, he/she will provide guidance on which part of mission analysis to reinvestigate.

(i) *Notify Planning COIs.* The organization responsible for planning will notify planning COIs when the analysis is accepted. This notification will include the analysis brief and supporting information that will allow members of the COI to begin their own planning effort.

(2) COA Development. After receiving the leader's guidance, the planning staff develops COAs that will accomplish the objectives for an operation. A COA is any sequence of activities that an organization may follow to accomplish a mission. COA development provides options on how the mission might be accomplished. See Annex E to determine the risk for each COA developed.

(a) COAs and Planning Levels. COAs exist at each planning level (i.e., strategic, operational, and tactical). The most distinctive feature among these planning levels is the organizational level involved. Examples for the Federal Government include:

1 A strategic-level COA discusses how the Federal agencies organize and coordinate efforts to address a specific incident. It does not describe tasks for

components of those Federal agencies nor does it provide details on specific tactical activities. A strategic-level COA must avoid micromanaging the operational and tactical levels.

2 An operational COA provides more details on how the Federal agencies and, specifically, how their components organize and coordinate efforts to address a specific incident. It does not describe specific details of tactical units. An operational-level COA must avoid micromanaging the tactical level.

3 A tactical-level COA discusses actions by tactical units within Federal agency components (i.e., search and rescue, security, law enforcement, etc.).

(b) Each COA considered must meet the following criteria:

1 Suitability. The COA must accomplish the mission and comply with the leader's guidance.

2 Feasibility. The COA can accomplish the mission within the established time, space, and resources limitations.

3 Acceptability. The advantage gained by executing the COA must justify the cost in resources. This assessment is largely subjective and based on the leader's experience and the information available.

4 Distinguishability. Each COA must differ significantly from any others.

5 Completeness. The COA must incorporate objectives, effects, and tasks to be performed; major resources required; concepts for deploying, employing, and sustaining required resources; time estimates for achieving objectives; and the end-state and mission success criteria.

(c) Brainstorming is the preferred technique for generating COAs because it provides the widest range of options. Brainstorming requires planners to remain unbiased and open-minded in evaluating proposed COAs. Planners can quickly identify COAs obviously not feasible in their particular areas of expertise. They can also quickly decide whether they can modify a COA to accomplish the requirement or need to eliminate it immediately. If a planner identifies information that might affect another's analysis, he/she shares it immediately to eliminate wasted time and effort.

(d) Planners and leaders must avoid choosing or favoring one COA over another. The decision-making process is a tool that will help select the best COA for a given situation, but only if planners and leaders use it appropriately.

c. Phase 3: Plan Development. Federal planners develop the initial draft of the plan based on the guidance received. SMEs participate in the development of the plan with the designated Federal planners. The product at the conclusion of this phase is the initial draft of the plan.

(1) COA Analysis. COA analysis identifies which COA accomplishes the mission with minimum resources in the shortest amount of time. COA analysis is a disciplined process, with rules and steps designed to attempt to visualize the flow of an operation. It relies heavily on doctrinal foundation, judgment, and experience. COAs are not compared against each other during COA analysis.

(a) COA analysis positions the organization for future operations and provides flexibility to meet unforeseen events during execution. It also provides the maximum latitude for initiative by subordinate organizations.

(b) COA analysis enables the leader and planning team to continue the risk management process. It assists the planning team in developing a synchronization matrix that organizes the different COAs into a model that provides a side-by-side comparison.

(2) COA Comparison.

(a) The COA comparison starts with the planning team analyzing and evaluating the advantages and disadvantages of each COA. The team outlines each COA using the evaluation criteria developed earlier, highlighting advantages and disadvantages. Comparing the strengths and weaknesses of the COAs identifies their advantages and disadvantages with respect to each other.

(b) The planning team compares feasible COAs to identify the one that has the highest probability of success against the threat COAs. The team may focus on the most likely and the most dangerous threat COAs in a time-constrained situation. The selected COA should:

- 1 Pose the minimum risk to personnel, assets, and mission accomplishment;
- 2 Best position the organization for future operations;
- 3 Provide the best flexibility to meet “unknowns” during execution; and
- 4 Provide maximum latitude for initiative by participants.

(c) The actual comparison of COAs is critical. The team may use any technique that facilitates reaching the best recommendation and that poises the leader to make the best decision. The most common technique is the decision matrix, which uses evaluation criteria to assess the effectiveness and efficiency of each COA.

(d) Each COA is rated based on weighted criteria to present a quantified basis for leader decision.

1 The planning team must develop criteria that address the operation being planned and represent a sound measure of a given COA. Examples include economic impact, complexity (i.e., multiple jurisdictional issues), the time it takes to achieve the end-state, required resources, and risk.

2 A weight (i.e., number) is assigned to each criterion based on relative importance among the criteria: the greater the weight, the more important the criterion.

3 Each COA is given a numerical value for each criterion based on the relative advantage or disadvantage the COA represents against the criterion.

4 That COA’s value for each criterion is multiplied by the criterion’s weight.

5 The COA's overall score is determined by adding these values together.

(3) COA Approval. The leader will approve the COA recommended by the planning team or direct the team to start over.

(a) The planning team will prepare a briefing that includes the results of COA comparison and a recommended COA for the leader to approve.

(b) Upon reviewing the information presented, the leader may decide to:

1 Accept the COA as recommended by the planners. Planners will then begin preparing the draft plan;

2 Select another COA presented by the planners. Likewise, planners will prepare the plan based on selected COA;

3 Direct the creation of an additional COA that combines attributes of two or more of the courses of action presented. (Planners will then repeat COA development, analysis, and comparison, as appropriate, and brief the new COA to the leader); or

4 Reject the COAs presented and direct the planners to start planning anew.

(c) The approved COA becomes the plan's concept of operations and provides additional clarity regarding the operation's purpose. A concept of operations is a broad statement of the leader's assumptions or goals with regard to a homeland security operation. The concept is designed to give an overall picture of the operation.

(d) The planning team chief will then notify the planning COIs of the decision and provide information on the selected COA to those COIs. The preferred notification method is via electronic means either by plain e-mail, a special form, or via a dedicated information sharing system, such as the Homeland Security Information Network (HSIN). It is essential that all key organizations expected to participate in the operation being planned be notified of the decision in an expeditious manner. Planning team members from these organizations should be allowed to contact their organizations as an informal method. Sound planning puts a premium on information sharing.

d. Phase 4: Plan Preparation and Review.

(1) Plan Preparation. The planners will prepare the plan using the appropriate format.

(a) The plan, including associated annexes and any attachments, must be marked with the appropriate classification. Classified annexes or attachments may be transmitted and stored separately if the overall plan is unclassified. The plan will contain a notice identifying the classified portion and how it may be obtained.

(b) Federal Planning Team Review. Federal strategic plans and Federal CONPLANs will follow the same review process.

1 The Federal planning team lead shall distribute the draft plan to interagency planning team members for initial review and comment.

2 The planning team shall adjudicate comments received during this review in coordination with counterparts with a role in the planning scenario. Comments that remain an issue shall be highlighted for the next review.

3 The planning team shall provide the draft plan to the appropriate policy coordination body to distribute for initial review.

(2) Strategic Plan/CONPLAN Review. Each Federal strategic plan/CONPLAN completes two formal Federal interagency reviews before being approved by the Secretary.

(a) *Initial Review.* Federal strategic plan/CONPLAN initial review is conducted by Federal agency designated representatives below the Assistant Secretary level.

(b) *Initial Review Adjudication.* Federal planners representing the Secretary, and the Director of NCTC for counterterrorism plans, shall adjudicate comments received and submit the final Federal strategic plan/CONPLAN review package for distribution by the appropriate policy coordination body.

(c) *Final Review Distribution.* Federal final strategic plan/CONPLAN review is conducted by Federal agency designated representatives at the Assistant Secretary level.

(d) *Final Review Adjudication.* The Secretary shall adjudicate comments received during this review in coordination with counterparts from Federal agencies with a role in the planning scenario, including the Director of NCTC for counterterrorism plans.

(3) Federal Strategic Plan Approval and Dissemination. Federal planners shall submit the plan for senior leadership approval. The product at the conclusion of Phase 4 is an approved plan that will be ready for further refinement or execution.

(a) Because the Strategic Plan delineates roles and responsibilities, establishes mission-essential tasks, and determines required and priority capabilities, approval of the Strategic Plan is contingent upon concurrence by the heads of the agencies with a role in homeland security.

(b) After concurrence by the appropriate policy coordination body, Federal planners representing the Secretary and the Director of NCTC for counterterrorism plans shall submit the Strategic Plan for the Secretary's approval.

(c) After approval by the Secretary, the Strategic Plan shall be disseminated by the Secretary to the planning COIs. Dissemination shall be by the most expeditious manner within the bounds of operational security.

(d) An approved Strategic Plan triggers the start of CONPLAN development, which uses the process described in paragraph 5.

(4) Federal CONPLAN Approval and Dissemination.

(a) Federal planners representing the Secretary and senior agency representatives, and the corresponding NCTC representatives for counterterrorism plans, shall submit the CONPLAN for the Secretary's approval.

(b) After approval by the Secretary, the CONPLAN shall be disseminated by the Secretary to the planning COIs. Dissemination shall be by the most expeditious manner within the bounds of operational security.

(c) An approved CONPLAN triggers the start of OPLAN development, which uses the plan development process described above.

(5) Interagency Conflict Resolution. As plans are submitted for review and approval, any conflicts should be resolved at the lowest possible level within the Federal Government. If a conflict cannot be resolved within the existing interagency planning organization, the issue will be elevated for resolution at the appropriate-level Federal Government policy-making body (through the policy process established by *HSPD-1*).

e. Phase 5: Plan Refinement Through Training, Exercising, and Execution.

(1) Federal Plan Refinement. While plans may be approved and distributed as final products, the planning effort continues because each plan is based on perishable information and retains the context of the time in which it was prepared. As the risks, capabilities, policies, or connected plans change, these plans must be updated through a continuous development and revision process. Factors that may create the need for more frequent review include:

- (a) New intelligence;
- (b) New guidance from senior leadership; and/or
- (c) Lessons learned from actual events and/or exercises.

(2) Plan review and refinement essentially repeats plan development phases 2 to 5 above. However, the planners will tailor the review to those aspects of the planning effort that have changed (e.g., higher-level guidance, assumptions, and resources available). In the worst case, the entire planning effort may have to be started again from the beginning, but this should not be the case if reviews occur on a regular basis.

(3) The review process for any plan should begin within 12 months of the plan approval or change, or as incidents and plan use identify the need for an earlier change. Just as the plan should be developed by a team of stakeholders, the review and updates should also occur through a similar team effort.

(4) Refinements may be made to plans using input from lessons learned from planned exercises or actual operations. This information is collected during the assessment and evaluation phase and fed directly into the plan review process. It may also influence the development of guidance and policy.

(5) Lessons learned should be communicated to other agencies and stakeholders so that similar plans can benefit from the information.

f. Training and Exercise. Once plans are developed and coordinated with stakeholders, adequate training of those that will use the plan and careful exercising of the plans is imperative for the plan's successful use and subsequent refinement. Key practices include:

- (1) Training should occur as soon as possible after plan approval;
- (2) Training should include all stakeholders;

- (3) Plans should be widely available and known to all users and those that the plan intends to support; and
- (4) Plans should be exercised in conjunction with other agencies and stakeholders to broaden the knowledge and interoperability of the plans.

g. Federal Plan Execution. During execution of the plans, careful attention to the development of lessons learned is key for refining and improving the plan.

(1) Existing plans shall be reviewed and refined by the planning team to meet the details of the situation at hand using crisis action planning (see Chapter 2). The time available will not allow for a weeks-long development, review, and approval process. The process will have to conform to how an agency is organized to handle an actual event.

(2) Lessons learned must be captured during execution in order to make improvements to the planning process.

Intentionally Left Blank

ANNEX A: FEDERAL STRATEGIC GUIDANCE STATEMENT FORMAT

{TITLE} FEDERAL STRATEGIC GUIDANCE STATEMENT FOR *[Identify the National Planning Scenario addressed.]*

- 1. Purpose.** *[Describe the purpose of the strategic guidance: identify the types of plans that will be developed and the intent of planning.]*
- 2. Strategic Priorities.** *[Identify the strategic priorities from the relevant strategic documents (e.g., National Homeland Security Strategy, National Security Strategy, Presidential Directives, and national strategies). This list is not all inclusive; the planning team must use as many sources as practicable.]*
- 3. National Strategic Objectives.** *[Identify the strategic objectives for prevention, protection, response, and recovery operations. Common objectives across each mission area should also be addressed.]*
- 4. Basic Assumptions.** *[List assumptions that frame planning for the Federal mission areas of prevention, protection, response, and recovery.]*
- 5. Federal End-State.** *[Describe the end-state for Federal prevention, protection, response, and recovery operations.]*
- 6. Means to Achieve End-State.** *[Identify policy and plans to support Federal prevention, protection, response, and recovery operations for the selected scenario. Identify specialized resources, training, and exercises to support the selected scenario.]*
- 7. Planning Guidance.** *[Identify planning roles and responsibilities for the planning community of interest, any modifications to the existing planning process, instructions on when the plan is due, any planning limitations that will affect planning, and policy guidance.]*

Enclosures

[First enclosure identifies the list of designated Federal Departments and Agencies requested to provide subject matter experts for the planning effort.]

[Second enclosure contains any classified information about the planning effort. This enclosure will be maintained under separate cover, published separately, and maintained according to the highest classification.]

Intentionally Left Blank

ANNEX B: FEDERAL STRATEGIC PLAN FORMAT

In accordance with *Homeland Security Presidential Directive 8 (HSPD-8)* Annex 1, strategic plans define the mission, identify authorities, delineate roles and responsibilities, establish mission-essential tasks, determine required and priority capabilities, and develop performance and effectiveness measures to complement guidance from the Strategic Guidance Statement (SGS). Together, the SGS and Strategic Plan provide operational-level planners with the necessary strategic guidance to craft operational-level concept plans (CONPLANS).

[Address of Organization Preparing the Plan]

[Date-time group of signature]

[Organization's Plan Reference Number]

{STRATEGIC PLAN TITLE} *[A plan's title should be short and concise but still describe the plan's purpose.]*

1. PURPOSE. *[Briefly describe the plan's purpose, scope, and any special information required.]*

2. MISSION STATEMENT. *[State the senior leader's mission statement in a short sentence or paragraph that describes the key objective(s) and purpose—a clear statement of the action to be taken and the purpose for doing so. The mission statement contains the elements of who, what, when, where, and why, but seldom specifies how. It forms the basis for planning and is included in the planning guidance, senior leader and staff estimates, the concept of operations, and the completed plan. The mission statement is a key product from mission research and analysis.]*

3. SITUATION. *[Provide background information, identify any impact on existing authorities, briefly describe the threat and the potential effects, and identify critical considerations and critical assumptions. The situation should provide senior leaders and planners with an understanding of what will happen within the context of a given incident and allow them to orient to the expected conditions. This "situation" must be understood by leaders and planners to properly develop courses of action (COAs) that will address the potential incident. The research and analysis step in the planning process is the primary source of information for this paragraph.]*

a. **Background.** *[Provide background information that supports understanding of the plan. This may include who has responsibility to issue the plan, the instruments of national power that will be used, the role of non-governmental organizations and the private sector, any policies altered or modified by the plan, key terms unfamiliar to the planning community, and any other information thought pertinent. In general, background information should be repetitive.]*

b. **Policy Decisions/Guidance.** *[Provide key policy decisions and/or directives from the National Security Council/Homeland Security Council bearing on the crafting of the plan. Often, such policy guidance departs from routinely assigned agency roles and responsibilities.]*

c. **Threat.** *[Describe the threat posed by the type of incident and/or planning scenario the plan addresses. For prevention plans, information should focus on how a terrorist group would carry out an attack. For protection, response, and recovery plans, information should focus on the consequences of the actual occurrence of an incident, especially regarding potential impacts on critical infrastructure and key resources. Provide enough information for understanding of*

the consequences of an incident; reference source documents rather than repeating the information in its entirety.]

d. Critical Assumptions. *[List critical assumptions used to develop the strategic plan. Assumptions are suppositions about the current or future situation that are accepted as true in the absence of facts to facilitate planning.]*

e. Strategic Objectives. *[List strategic objectives from the approved SGS.]*

4. IDENTIFICATION OF AUTHORITIES.

a. Authorities. *[Identify key authorities required to develop, coordinate, and execute the plan.]*

b. Critical Considerations. *[Identify critical considerations. These include, but are not limited to, classification, spectrum of operations, legal considerations, and international/trans-national coordination requirements.]*

c. Strategic Limitations. *[Identify any actions the Federal Government is prohibited from taking or is unable to take, and those actions dictated that it must accomplish. In addition, identify those actions that the Federal Government may take under special authorities.]*

5. ROLES AND RESPONSIBILITIES.

a. Federal Common Roles and Responsibilities. *[Identify roles and responsibilities assigned to all participating departments and agencies.]*

b. Federal Specific Roles and Responsibilities. *[Identify roles and responsibilities assigned to key Federal entities that will take part in executing the plan.]*

c. State, Local, and Tribal Coordination Actions. *[Identify expected State, local, and Tribal government actions that will necessitate the coordinated support of the Federal Government.]*

d. Non-Governmental Organization (NGO) Coordination Actions. *[Identify expected NGO actions that will require coordination with the Federal Government.]*

e. Private Sector Coordination Actions. *[Identify expected private sector actions that will require coordination the Federal Government.]*

6. MISSION-ESSENTIAL TASKS.

a. Federal Common Mission-Essential Tasks. *[Identify mission-essential tasks assigned to all participating departments and agencies. Include identification of key Federal decisions, coordinating instructions, and critical information requirements.]*

b. Federal Specific Mission-Essential Tasks. *[Identify mission-essential tasks assigned to key Federal entities that will take part in executing the plan.]*

c. State, Local, and Tribal Coordination Tasks. *[Identify expected State, local, and Tribal government mission-essential tasks that will necessitate the coordinated support of the Federal government.]*

d. NGO Coordination Tasks. *[Identify expected NGO mission-essential tasks that will require coordination with the Federal Government.]*

e. **Private Sector Coordination Tasks.** *[Identify expected private sector mission-essential tasks that will require coordination the Federal Government.]*

7. REQUIRED AND PRIORITY CAPABILITIES. *[Identify Federal capabilities required to accomplish the strategic plan. These capabilities are listed in order of priority.]*

8. SUSTAINMENT STRATEGY. *[This section should provide broad guidance for sustainment of the homeland security effort **at the strategic level**, with information and instructions broken down by phases. Identify strategic resource management oversight requirements for sustainment priorities and resources, site development, and interagency responsibilities; national resupply nodes; transportation policies, guidance, and procedures; resource and transportation assumptions; and planning requirements and subordinate objectives. Discuss the administrative management of participating personnel, reconstituting personnel, leadership replacement and rotation policies, and required individual augmentation to headquarters and other operational requirements.]*

9. PERFORMANCE AND EFFECTIVENESS MEASURES. *[List identified performance and effectiveness measures for accomplishing the mission-essential tasks. Each performance task will have a metric that is used to determine whether the objective is achieved.]*

10. OVERSIGHT, COORDINATING INSTRUCTIONS, AND COMMUNICATIONS.

a. **Oversight.** *[Identify the organization or individual that will exercise oversight of the operation.]*

b. **Coordinating Instructions.**

(1) **General.** *[Provide common instructions applicable to two or more departments and/or agencies that are necessary for proper coordination of the operation. Coordinating instructions establish, in particular, the conditions for execution. Examples include the time or condition when a plan or an order becomes effective, risk reduction control measures, use of force and force protection guidelines, and environmental considerations. Terms pertaining to the timing of execution and deployments should be explained, as should other operational terms that appear in the plan but are not defined in department or agency publications. Identify departments and agencies, including interagency centers, that have coordination responsibilities during the operation.]*

(2) **Critical Information Requirements (CIR).** *[List the CIRs needed by the senior leader to support making critical decisions within the context of expected operations. The list should be limited to 10 or fewer to enhance comprehension. Key sources for CIRs include mission analysis and COA analysis.]*

c. **Communications.** *[Identify what entity will establish communications with applicable communities of interest (COIs). Identify specific communications systems (e.g., Homeland Security Information Network) that will be used.]*

ATTACHMENTS:

1—Responsibilities Matrix. *[The responsibilities matrix identifies critical information, such as the threat, decision points, and other key responsibilities (e.g., medical and public health, public*

safety and security, mass care, logistics), and shows how these change over the expected time frame.]

2—Classified. *[Selected plans may have one or more classified attachments to address sensitive requirements related to the plan. These may include, but are not limited to, operations, intelligence, reference materials, and selected authorities. These attachments will be published separately and distributed to appropriate audiences.]*

3—Other. *[Additional attachments may be added to a strategic plan to provide additional clarity or facilitate coordination among COIs. Examples would include glossary, special assessments, modeling/analytical products, decision support aids/checklists, etc.]*

ANNEX C: FEDERAL CONCEPT PLAN FORMAT

Concept plans (CONPLANS) describe the concept of operations for integrating and synchronizing existing Federal capabilities to accomplish the mission-essential tasks identified in the Strategic Plan, and describe how Federal capabilities will be integrated into and support regional, State, local, and Tribal plans. The Integrated Planning System (IPS) Federal CONPLAN template below is not meant to be a replacement format for an agency's existing CONPLAN but a mechanism to provide a common framework for a Federal CONPLAN addressing a common threat. A concept plan comprises a title, plan identification information, five paragraphs and associated sub-paragraphs, and attachments as described below.

[Address of Organization Preparing the Plan]
[Date-time group of signature]
[Organization's Plan Reference Number]

{PLAN TITLE} *[A plan's title should be short and concise but still describe the plan's purpose.]*

1. SITUATION. *[Describe the plan's purpose, provide background information, identify any impact on existing authorities, briefly describe the threat and the potential effects, and identify critical considerations and critical assumptions. The situation should provide senior leaders and planners with an understanding of what will happen within the context of a given incident and allow them to orient to the expected conditions. This "situation" must be understood by leaders and planners to properly develop courses of action (COAs) that will address the potential incident. Mission analysis is the primary source of information for this paragraph.]*

a. Purpose. *[Briefly describe the plan's purpose, scope, and any special information required.]*

b. Background. *[Provide any background information that supports understanding of how the CONPLAN will implement the Strategic Plan. This may include who has responsibility to issue the plan, the instruments of national power that will be used, the role of non-governmental organizations (NGOs) and the private sector, any policies altered or modified by the plan, and any other information thought pertinent. In general, information should not be repetitive.]*

c. Authorities. *[Identify any impacts on existing authorities exercised under Federal laws, policies, or strategies by the senior leader.]*

d. Threat. *[Describe the threat posed by the type of incident the plan is intended to address. For prevention plans, information should focus on how a terrorist group would carry out an attack. For protection, response, and recovery plans, information should focus on the consequences of the actual occurrence of an incident, especially regarding potential impacts on critical infrastructure and key resources. Provide enough information for understanding of the consequences of an incident; reference source documents rather than repeating the information in its entirety.]*

e. Critical Considerations. *[Identify critical considerations. These include, but are not limited to, classification, spectrum of operations, and legal considerations.]*

f. Critical Assumptions. *[List critical assumptions used to develop the concept of operations. Assumptions are suppositions about the current or future situation accepted as true in the absence of facts to facilitate planning.]*

g. Mission-Essential Tasks. *[Provide the list of mission-essential tasks identified in the Strategic Plan.]*

2. MISSION. *[State the senior leader’s mission statement. This should be a short sentence or paragraph that describes the essential task(s) and purpose—a clear statement of the action to be taken and the purpose for doing so. The mission statement contains the elements of who, what, when, where, and why, but seldom specifies how. It forms the basis for planning and is included in the planning guidance, senior leader and staff estimates, the concept of operations, and the completed plan. The mission statement is a key product from mission analysis.]*

3. EXECUTION. *[Describe the senior leader’s concept of operations, key Federal roles and responsibilities for participating departments and agencies, and coordination requirements for State and local governments, NGOs, and the private sector. Identify key Federal decisions, Federal actions required and prohibited, and Critical Information Requirements (CIR).]*

a. Senior Leader’s Intent. *[The intent is a clear and concise expression of the purpose of the operation, method, and the desired end-state. It provides focus for the planning staff and helps department and agency leaders take actions to achieve the end-state without further direction, even when operations do not unfold as planned. A good intent allows subordinates to decide how to act when facing unforeseen opportunities and threats, and in situations where the concept of operations no longer applies. This statement deals primarily with the conditions that lead to mission accomplishment, so the senior leader may highlight selected objectives and desired and undesired effects.]*

b. Concept of Operations. *[The concept of operations at the operational level clearly and concisely expresses what the senior leader intends to accomplish and how it will be done using available resources. It describes how the actions of department and agency components and supporting organizations will be integrated, synchronized, and phased to accomplish the mission, including potential branches and sequels.]*

(1) **General**

(2) **Alert/Activation**

(3) **Deployment**

(4) **Employment**

(5) **Demobilization**

c. Key Federal Roles and Responsibilities

(1) **Common Roles and Responsibilities.** *[Identify roles and responsibilities that are assigned to all participating departments and agencies.]*

(2) **Specific Roles and Responsibilities.** *[Identify roles and responsibilities that are assigned to key Federal departments and agencies that will take part in executing the plan.]*

d. State, Local, and Tribal Coordination Requirements. *[Identify expected State, local, and Tribal government actions that will necessitate the coordinated support of the Federal Government.]*

e. NGO Coordination Requirements. *[Identify expected NGO actions that will require coordination with the Federal Government.]*

f. Private Sector Coordination Requirements. *[Identify expected private sector actions that will require coordination the Federal Government.]*

g. Key Federal Decisions. *[Identify any key decisions required for the expected operation, determine who will make the required decision, and establish the timeline for when the decision must be made.]*

h. Actions Required of and Prohibited to the Federal Government. *[Describe any actions the Federal Government must take and those it cannot take. In addition, identify those actions that the Federal Government may take under special authorities.]*

i. Critical Information Requirements (CIR). *[List the CIRs needed by the senior leader to support making critical decisions within the context of expected operations. The list should be limited to 10 or fewer to enhance comprehension. Key sources for CIRs include mission analysis and COA analysis.]*

4. ADMINISTRATION, RESOURCES AND FUNDING

a. Administration.

(1) *Responsibility for management oversight of all administrative and logistical requirements supporting operations.*

(2) *Senior Financial Advisor responsibilities.*

(3) *Coordination of State mutual aid agreement(s).*

(4) *Financial oversight.*

(5) *Personnel administrative management responsibilities.*

(a) *Authorities for and policy on personnel augmentation.*

(b) *Personnel training.*

(c) *Travel and Travel Reimbursement.*

b. Resources. *[Identify sustainment priorities and resources, site development, and interagency responsibilities; the priority and movement of major resources for each phase of the operation; national and regional resupply nodes; transportation policies, guidance, and procedures; resource and transportation assumptions; and planning requirements and subordinate tasks. Identify detailed planning requirements and subordinate taskings. Assign tasks for establishing and operating personnel facilities, managing accurate and timely personnel accountability and strength reporting, and making provisions for staffing. Discuss the administrative management of participating personnel, reconstituting personnel, leadership replacement and rotation policies, and required individual augmentation to headquarters and other operational requirements.]*

(1) **Concept of Logistics Support.** *[State the policies, guidance, and procedures to support all options for anticipated operations.]*

(a) **Logistics Management.** *[Summarize the system being used for logistics management. Usually refers to Annex D for more detailed system descriptions.]*

(b) **Pre-Positioned Resources.**

c. **Funding.** *[Describe/identify how Federal funding for operations will occur.]*

5. OVERSIGHT, COORDINATING INSTRUCTIONS, AND COMMUNICATIONS

a. **Oversight.** *[Identify the organization or individual that will exercise oversight of the operation.]*

b. **Coordinating Instructions.** *[List the common instructions applicable to two or more departments and/or agencies that are necessary for proper coordination of the operation. Coordinating instructions establish, in particular, the conditions for execution. Examples include the time or condition when a plan or an order becomes effective, priority intelligence requirements, essential elements of friendly information, risk reduction control measures, use of force and force protection guidelines, environmental considerations. Terms pertaining to the timing of execution and deployments should be explained; as should other operational terms that appear in the plan but are not defined in department or agency publications. Identify departments and agencies, including interagency centers, that have coordination responsibilities during the operation.]*

c. **Communications.** *[Identify what entity will establish communications with applicable communities of interest. Identify specific communications systems (e.g., Homeland Security Information Network) that will be used during the operation. Usually refers to Annex K for more detailed system descriptions.]*

Attachments

1—Synchronization Matrix. *[A synchronization matrix displays the selected COA developed during Plan development. Specifically, the synchronization matrix identifies critical information such as the threat, decision points, and other key categories (e.g., medical and public health, public safety and security, mass care, logistics). The matrix shows how these elements change over the course of the homeland security operation (i.e., by the phase of the operation).]*

2—Operational Executive Decision Checklist. *[Executive Decision Checklists are senior leader decision support aids. They summarize key actions, decisions, milestones, and key reference information identified in a specific plan. Executive Decision Checklists are simply the key highlights from a plan to facilitate informed decision making at all levels. Checklist formats are determined by the authors of the plan.]*

Annexes (Sample Listing)

A. Task Organization

B. Intelligence

C. Operations

D. Logistics

F. Public Affairs

K. Coordination, Communications, and Computer Systems

X. Execution Checklist

Z. Distribution

Note: These annexes should be included in every CONPLAN required under IPS. Additional annexes may be used as appropriate.

Intentionally Left Blank

ANNEX D: FEDERAL OPERATIONS PLAN FORMAT

Operations plans (OPLANs) identify detailed resource, personnel, and asset allocations in order to execute the objectives of the strategic plan and execute strategic operational priorities. An OPLAN contains a full description of the concept of operations, including specific roles and responsibilities, tasks, integration, and actions required, with support function annexes, as appropriate. The Integrated Planning System (IPS) Federal OPLAN template below is not meant to be a replacement format for an agency's existing OPLAN but a mechanism to provide a common framework for a Federal OPLAN addressing a common threat. An operations plan comprises a title, plan identification information, five paragraphs and associated sub-paragraphs, and attachments as described below.

[Address of Organization Preparing the Plan]

[Date-time group of signature]

[Organization's Plan Reference Number]

{PLAN TITLE} *[A plan's title should be short and concise but still describe the plan's purpose.]*

1. SITUATION. *[Describe the plan's purpose, provide background information, identify any impact to existing authorities, briefly describe the threat and the potential effects, and identify critical considerations and critical assumptions. The situation should provide senior leaders and planners with an understanding of what will happen within the context of a given incident and allow them to orient to the expected conditions. This "situation" must be understood by leaders and planners to properly develop courses of action (COAs) that will address the potential incident. Mission analysis is the primary source of information for this paragraph.]*

a. Purpose. *[Briefly describe the plan's purpose, scope, and any special information required.]*

b. Background. *[Provide any background information that supports understanding how the OPLAN will implement the concept plan (CONPLAN). This may include who has responsibility to issue the plan, the instruments of national power that will be used, the role of non-governmental organizations (NGOs) and the private sector, any policies altered or modified by the plan, and any other information thought pertinent. In general, information should not be repetitive.]*

c. Authorities. *[Identify any impacts on existing authorities exercised under Federal laws, policies, or strategies by the senior leader.]*

d. Threat. *[Describe the threat posed by the type of incident the plan is intended to address. For prevention plans, information should focus on how a terrorist group would carry out an attack. For protection, response, and recovery plans, information should focus on the consequences of the actual occurrence of an incident, especially regarding potential impacts on critical infrastructure and key resources. Provide enough information for understanding of the consequences.]*

e. Critical Considerations. *[Identify critical consideration. These include but are not limited to, classification, spectrum of operations, and legal considerations.]*

f. Critical Assumptions. *[List critical assumptions used to develop the concept of operations. Assumptions are suppositions about the current or future situation accepted as true in the absence of facts to facilitate planning.]*

g. Mission-Essential Tasks. *[Provide the list of mission-essential tasks from the Strategic Plan and CONPLAN.]*

2. MISSION. *[State the senior leader's mission statement. This should be a short sentence or paragraph that describes the essential task(s) and purpose—a clear statement of the action to be taken and the purpose for doing so. The mission statement contains the elements of who, what, when, where, and why, but seldom specifies how. It forms the basis for planning and is included in the planning guidance, senior leader and staff estimates, the concept of operations, and the completed plan. The mission statement is a key product from mission analysis.]*

3. EXECUTION. *[Describe the senior leader's concept of operations, define key Federal roles and responsibilities for participating departments and agencies, and coordination requirements for State and local governments, NGOs, and the private sector. Identify key Federal decisions, Federal actions required and prohibited, and Critical Information Requirements (CIR).]*

a. Senior Leader's Intent. *[The intent is a clear and concise expression of the purpose of the operation, method and the end-state. It provides focus for the planning staff and helps department and agency leaders take actions to achieve the end-state without further direction, even when operations do not unfold as planned. The intent should also include where the senior leader will accept risk during the operation. A good intent allows subordinates to decide how to act when facing unforeseen opportunities and threats, and in situations where the concept of operations no longer applies. This statement deals primarily with the conditions that lead to mission accomplishment, so the senior leader may highlight selected objectives and desired and undesired effects.]*

b. Concept of Operations. *[The concept of operations at the operational level clearly and concisely expresses what the senior leader intends to accomplish and how it will be done using available resources. It describes how the actions of department and agency components and supporting organizations will be integrated, synchronized, and phased to accomplish the mission, including potential branches and sequels.]*

(1) **General**

(2) **Alert/Activation**

(3) **Deployment**

(4) **Employment**

(5) **Demobilization**

c. Key Federal Roles and Responsibilities

(1) **Common Roles and Responsibilities.** *[Identify roles and responsibilities that are assigned to all participating departments and agencies.]*

(2) **Specific Roles and Responsibilities.** *[Identify roles and responsibilities that are assigned to key Federal departments and agencies that will take part in executing the plan.]*

d. State, Local, and Tribal Coordination Requirements. *[Identify expected State, local, and Tribal government actions that will necessitate the coordinated support of the Federal Government.]*

e. NGO Coordination Requirements. *[Identify expected NGO actions that will require coordination with the Federal Government.]*

f. Private Sector Coordination Requirements. *[Identify expected private sector actions that will require coordination the Federal Government.]*

g. Key Federal Decisions. *[Identify any key decisions required for the expected operation, who will make the decision, and when the decision must be made.]*

h. Actions Required of and Prohibited to the Federal Government. *[Describe any actions the Federal Government must take and those it cannot take. In addition, identify those actions that the Federal Government may take under special authorities.]*

i. Critical Information Requirements (CIR). *[List the CIRs needed by the senior leader to support making critical decisions within the context of expected operations. The list should be limited to 10 or fewer to enhance comprehension. Key sources for CIRs include mission analysis and COA analysis.]*

4. ADMINISTRATION, RESOURCES AND FUNDING

a. Administration.

(1) *Responsibility for management oversight of all administrative and logistical requirements supporting operations.*

(2) *Senior Financial Advisor responsibilities.*

(3) *Coordination of State mutual aid agreement(s).*

(4) *Financial oversight.*

(5) *Personnel administrative management responsibilities.*

(a) *Authorities for and policy on personnel augmentation.*

(b) *Personnel training.*

(c) *Travel and Travel Reimbursement.*

b. Resources. *[Identify sustainment priorities and resources, site development, and interagency responsibilities; the priority and movement of major resources for each phase of the operation; national and regional resupply nodes; transportation policies, guidance, and procedures; resource and transportation assumptions; and planning requirements and subordinate tasks. Identify detailed planning requirements and subordinate taskings. Assign tasks for establishing and operating personnel facilities, managing accurate and timely personnel accountability and strength reporting, and making provisions for staffing. Discuss the administrative management of participating personnel, reconstituting personnel, leadership replacement and rotation policies, and required individual augmentation to headquarters and other operational requirements]*

(1) **Concept of Logistics Support.** *[State the policies, guidance, and procedures to support all options for anticipated operations.]*

(a) **Logistics Management.** *[Summarize the system being used for logistics management. Usually refers to Annex D for more detailed system descriptions.]*

(b) **Pre-Positioned Resources.**

c. **Funding.** *[Describe/identify how Federal funding for operations will occur.]*

5. OVERSIGHT, COORDINATING INSTRUCTIONS, AND COMMUNICATIONS

a. **Oversight.** *[Identify the organization or individual that will exercise oversight of the operation.]*

b. **Coordinating Instructions.** *[List the common instructions applicable to the entire department/agency or two or more components within a department that are necessary for proper coordination of the operation. Coordinating instructions establish, in particular, the conditions for execution. Examples include the time or condition when a plan or an order becomes effective, priority intelligence requirements, essential elements of friendly information, risk reduction control measures, use of force and force protection guidelines, environmental considerations. Terms pertaining to the timing of execution and deployments should be explained; as should other operational terms that appear in the plan but are not defined in department or agency publications. Identify departments and agencies, including interagency centers, that have coordination responsibilities during the operation.]*

c. **Communications.** *[Identify what entity will establish communications with applicable communities of interest. Identify specific communications systems (e.g., Homeland Security Information Network) that will be used during the operation. Usually refers to Annex K for more detailed system descriptions.]*

Attachments

1—Synchronization Matrix. *[A synchronization matrix displays the selected COA developed during Plan Development. Specifically, the synchronization matrix identifies critical information such as the threat, decision points, and other key categories (e.g., medical and public health, public safety and security, mass care, logistics). The matrix shows how these elements change over the course of the homeland security operation (i.e., by the phase of the operation).]*

2—Operational Executive Decision Checklist. *[Executive Decision Checklists are senior leader decision support aids. They summarize key actions, decisions, milestones, and key reference information identified in a specific plan. Executive Decision Checklists are simply the key highlights from a plan to facilitate informed decision making at all levels. Checklist formats are determined by the authors of the plan.]*

Annexes (Sample Listing)

A. Task Organization

B. Intelligence

C. Operations

D. Logistics

F. Public Affairs

K. Coordination, Communications, and Computer Systems

X. Execution Checklist

Z. Distribution

Intentionally Left Blank

ANNEX E: RISK MANAGEMENT OVERVIEW AND THE INTEGRATED PLANNING SYSTEM

1. Introduction.

a. The Integrated Planning System (IPS) describes a risk-informed approach to national planning in which plans are oriented toward managing the potential for major adverse outcomes from current and future homeland security risks. The IPS strives to identify and coordinate an optimized mix of prevention, protection, response, and recovery measures as part of the planning effort to best manage the risks under anticipated constraints on the types and numbers of assets and resources available.

b. To accomplish this, planners will use 1) assessments of a range of homeland security risks to create a prioritization for plans, and 2) a framework of risk management that can be applied throughout all levels of planning. Systematic risk assessment and management provides specific insight for planners into how natural and manmade hazards threaten, and how adversaries might seek to exploit, key vulnerabilities for each type of high-risk scenario; and how to best act to prevent, protect against, respond to, and recover from incidents.

2. Definitions. Definitions presented here are working definitions. As such, they are subject to future modification as the lexicon for risk-informed homeland security planning matures.

a. Risk—An estimate of expected losses over time; homeland security risk for a particular scenario is a function of the expected threat, vulnerability, and consequence;

b. Risk Management—A process by which risks are assessed, analyzed, accepted, mitigated, reduced, or controlled to an appropriate level of risk at an appropriate cost;

c. Risk Assessment—A structured process for identifying the expected loss for a system, organization, object, or asset through the evaluation of threats, vulnerabilities, and consequences;

d. Scenario—A sequence of possible events leading to an adverse outcome, manmade or natural; for planning applications, scenarios begin with a defined threat that may exploit vulnerabilities in prevention and protection strategies to produce an incident that can have major consequences unless mitigated by effective response and recovery strategies.

3. Application of Risk in the IPS—Risk and Planning Scenarios. Planners employ risk analysis to support, organize, and prioritize planning activities using planning scenarios.

a. Develop Planning Scenarios. The *National Planning Scenarios (NPSs)* are developed, updated, or amended as necessary by the Secretary of Homeland Security, in coordination with the heads of Federal agencies with a role in homeland security and are informed by an analysis intended to focus planning efforts on the greatest risks to the Nation.

b. Refining Planning Scenarios. In the initial execution of the IPS, the eight scenario sets referenced in Chapter 5 will be used for Federal planning. In the future, however, planning scenarios (including the NPSs) will be updated and potentially expanded to be representative of newly prioritized homeland security risk and mission needs, based on the most likely or most dangerous threats to the homeland. Ideally, planning scenarios would be informed by the results of a national risk assessment. This update process will involve an assessment of

the homeland security risk to the Nation and its regions, and the definition of the specific threats, vulnerabilities, and consequences associated with each scenario.

c. A fully developed planning scenario is essential for effective planning. The development of the planning scenarios should involve detailing all key parameters, such as the scenario's timeline, possible attack/hazard vectors, variations in weapon/hazard types and destructive capacity, type of terror actor, and exposure—including type, number, distribution of targets, and consequence types (e.g., deaths, economic impacts). The parameters of interest to the planner will vary depending on the nature of the individual planning scenario.

4. Risk Assessments and Management in the Development of Plans. This section outlines a high-level approach for using a risk management cycle to support strategic, operational, and tactical planning efforts within the IPS construct. This approach is consistent with the overall planning process laid out in the IPS.

a. The recommended risk management cycle to support planning is made up of five analytical and management steps (see Figure E.1):

- (1) Setting strategic goals and objectives, and determining constraints;
- (2) Assessing the risks;
- (3) Evaluating alternatives for addressing these risks;
- (4) Selecting the appropriate alternatives; and
- (5) Implementing the alternatives and monitoring the progress made and the results achieved.

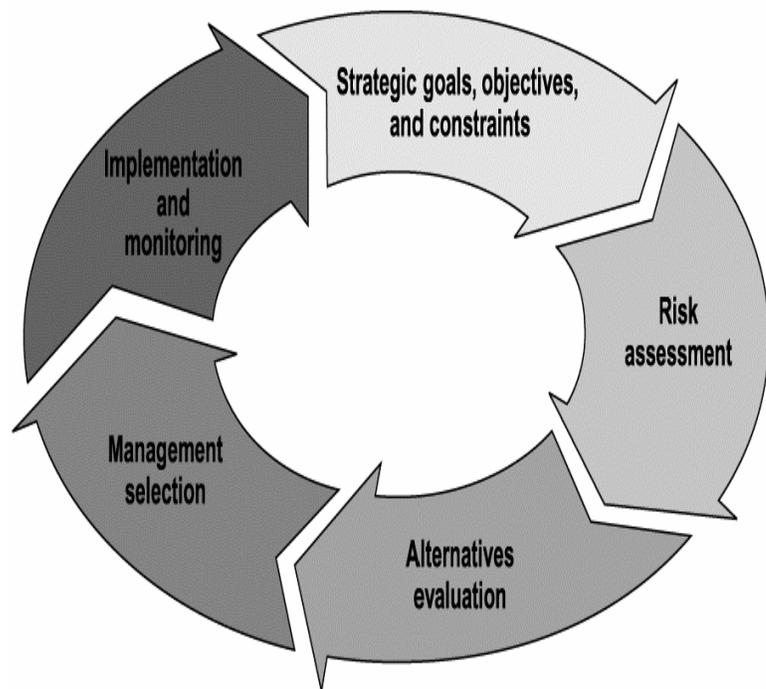


Figure E.1 Risk Management Cycle

b. Setting Strategic Goals, Objectives, and Constraints. Strategic goals, objectives, and constraints in plans are developed based on existing strategies, policies, and doctrine as well as available capabilities and resources. The objectives and tasks within each plan are the direct reflection of the guidance given to planners by those with the responsibility for leading the development and execution of plans. All aspects of plans should derive from the goals, objectives, and constraints associated with the plan.

c. Assessing the Risks.

(1) Risk assessments provide an understanding to planners and decision makers by answering the following three questions (see Figure E.2):

- scenario.
- (a) *What can go wrong?* This is typically captured in a planning scenario.
 - (b) *How likely is it?* This is typically captured in threat and vulnerability analyses.
 - (c) *How severe are the impacts?* This is typically captured in consequence analysis.

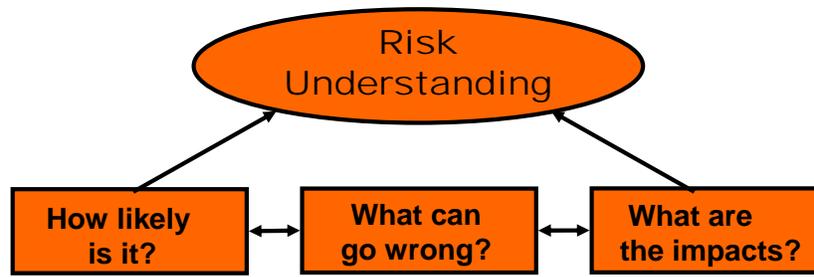


Figure E.2 Fundamentals of a Risk Assessment

(2) To assess the risk, planners need to determine and describe the information required. For each information item, the planning team needs to specify the information type, precision, and certainty required, and the analysis resources available. Once the information has been gathered, the planning team can assess the threat, vulnerability, and consequences related to the planning scenario, where:

- (a) *Threat* is the likelihood of a type of attack that might be attempted or that a particular hazard will occur;
- (b) *Vulnerability* is the likelihood that an attacker would succeed with a particular attack type or that the scenario will result in the expected level of consequence;
- (c) *Consequence* is the potential impact of a particular attack or the negative impact of the scenario;

(3) Conducting a risk assessment to support planning can cover a wide range of approaches from very simple screening approaches to quite sophisticated quantitative/qualitative modeling approaches. For every scenario, detailed quantitative modeling may not be necessary; simple estimations may be suitable. The key in applying these techniques is always to fit the level of sophistication employed to the level of information needed by decision makers; this information is typically derived from a combination of 1) historical experience, 2) analytical methods, and 3) knowledge and intuition.

(4) Depending on the nature of the scenario, planners can use different sources to assess the scenario's risk. For instance, the team may be able to leverage historical accident reporting databases to assess the risk associated with some manmade scenarios or detailed stochastic models may be available to assess the risk of natural disaster scenarios. For scenarios for which historical data or detailed modeling are scarce, as in the case of some critical but unprecedented terrorism scenarios, available intelligence, vulnerability assessments, and

consequence modeling, as well as subject matter expertise, can be leveraged to produce the risk assessment.

(5) For each scenario, planners should identify the existing safeguards that are in place to reduce either the likelihood (e.g., security countermeasures) or consequence (e.g., redundant capabilities) of the incident. In developing courses of action (COAs), this information will be useful to ensure that the plan will reduce the risk of an incident.

d. Alternatives Evaluation.

(1) Develop Alternative COAs. In developing plans, planners should attempt to determine how the risks for each scenario can be managed most effectively. Each COA within a plan should be completely developed and documented by recording a number of critical factors, including how the elements of the COA will interact with the scenario to reduce risk, as well as estimated costs, schedules, and implementation risks.

(2) Assess the Risk Impact of the Proposed COAs. Planners should reassess the risk of each scenario based on the implementation of each alternative COA based on the expected effectiveness of the countermeasures within the COA. This step provides the risk reduction value of each of the alternative strategies. Again, the sophistication of the risk impact assessment should be guided by the information required by decision makers. While quantitative estimates of risk reduction might be optimal, qualitative assessment at the strategy element level might be sufficient to inform the planning process.

e. Management Selection.

(1) Once the alternative COAs have been fully developed and evaluated, the planning process moves to the approval phase, in which decision makers choose the collection of alternatives for implementation. Selecting among COAs takes into account risk management to increase the chance that a developed plan will be successfully executed. In developing COAs, planners identify potential risks that could arise and threaten successful execution, as well as ways to mitigate those risks.

(2) In this case, “risk” is more than just homeland security risk. It also includes risk of failed execution of a portion of the plan (or the entire plan), as well as organizational and political risk associated with the plan. By necessity, all plans acknowledge or imply a certain level of residual risk that needs to be managed. It is up to the senior decision maker, as part of the approval process, to determine whether a plan takes on too much risk or whether the risk is not appropriately managed. Planning assumptions generally help define risk management considerations that need to be taken into account. As plans are created, however, these assumptions must be tested and evaluated to ensure that they do not exceed an appropriate level of risk.

f. Implementation and Monitoring. The IPS is based on the notion that planning is a dynamic process and that the overall planning system is flexible and responsive to changes in priorities and/or new needs. One of the mechanisms for accomplishing that goal is regular monitoring and update of developed plans based on lessons learned, new capabilities, or a change in risk. For example, when the risk level is judged to have changed based on new information or analysis, lessons learned from exercises or real-life events, or new trends, completed plans should be updated as necessary based on new guidance and/or newly identified gaps.

ANNEX F: RELATED AUTHORITIES

1. Statutes.

a. *The Constitution of the United States of America.* The Constitution provides the fundamental justification for homeland security through the guarantee of domestic tranquility and provision for the common defense of the Nation.

b. *Homeland Security Act of 2002 (Public Law 107-296).* This Act established the Department of Homeland Security (DHS) to coordinate all Federal homeland security activities to protect the Nation against threats to the homeland. To better facilitate the overarching homeland security mission, DHS was established by merging numerous agencies into a single department.

c. *Post-Katrina Emergency Management Reform Act (PKEMRA) (Public Law 109-295).* This statute makes extensive revisions to emergency response provisions while keeping the Federal Emergency Management Agency (FEMA) within DHS. It sets forth provisions regarding FEMA's mission, which include (1) leading the Nation's efforts to prepare for, respond to, recover from, and mitigate the risks of, any natural and manmade disaster, including catastrophic incidents; (2) implementing a risk-based, all-hazards plus strategy for preparedness; and (3) promoting and planning for the protection, security, resiliency, and post-disaster restoration of critical infrastructure and key resources, including cyber and communications assets.

d. *Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458).* This Act established the Office of the Director of National Intelligence. The Director of National Intelligence serves as head of the intelligence community; acts as the principal adviser to the President, National Security Council, and Homeland Security Council for intelligence matters related to the national security; and, consistent with section 1018 of the National Security Intelligence Reform Act of 2004, oversees and directs the implementation of the National Intelligence Program. This Act also established the National Counterterrorism Center to serve as the primary organization in the U.S. Government for analyzing and integrating all intelligence possessed or acquired by the U.S. Government pertaining to terrorism and counterterrorism, excepting intelligence pertaining exclusively to domestic terrorists and domestic counterterrorism.

e. *Title 18 of U.S. Code, Section 2332b(f).* This statutory provision assigns to the Attorney General primary investigative responsibility for all Federal crimes of terrorism.

2. Presidential Directives.

a. *Homeland Security Presidential Directive (HSPD)-1, Organization and Operation of the Homeland Security Council* (October 29, 2001).

b. *HSPD-2, Combating Terrorism Through Immigration Policies* (October 29, 2001).

c. *HSPD-3, The Homeland Security Advisory System* (March 11, 2002).

d. *HSPD-5, Management of Domestic Incidents* (February 28, 2003).

e. *HSPD-6, Integration and Use of Screening Information* (September 16, 2003).

- f. HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection* (December 17, 2003).
- g. HSPD-8, *National Preparedness* (December 17, 2003).
- h. HSPD-9, *Defense of United States Agriculture and Food* (January 30, 2004).
- i. National Security Presidential Directive (NSPD)-26, *Intelligence Priorities* (February 24, 2003) [Classified].
- j. NSPD-33/HSPD-10, *Bio-defense for the 21st Century* (April 28, 2004).
- k. HSPD-11, *Comprehensive Terrorist-Related Screening Procedures* (August 27, 2004).
- l. HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors* (August 27, 2004).
- m. NSPD-41/HSPD-13, *Maritime Security Policy* (December 21, 2004).
- n. NSPD-43/HSPD-14, *Domestic Nuclear Detection* (April 15, 2005).
- o. NSPD-46/HSPD-15, *United States Policy and Strategy in the War on Terror* (March 6, 2006). [Classified].
- p. NSPD-47/HSPD-16, *Aviation Security Policy* (June 20, 2006).
- q. NSPD-48/HSPD-17, *Nuclear Materials Information* (August 28, 2006). [Classified].
- r. HSPD-18, *Medical Countermeasures against Weapons of Mass Destruction* (January 31, 2007).
- s. HSPD-19, *Combating Terrorist Use of Explosives in the United States* (February 12, 2007).
- t. NSPD-51/HSPD-20, *National Continuity Policy* (May 9, 2007).
- u. HSPD-21, *Public Health and Medical Preparedness* (October 18, 2007).
- v. HSPD-22, *Domestic Chemical Defense* (December 21, 2007) [Classified].
- w. NSPD-54/HSPD-23, *Cybersecurity Policy* (January 8, 2008) [Classified].
- x. NSPD-59/HSPD-24, *Biometrics for Identification and Screening to Enhance National Security* (June 5, 2008).
- y. Executive Order 13231, *Critical Infrastructure Protection in the Information Age* (October 16, 2001). This order established the President's Critical Infrastructure Protection Board and authorized a protection program to secure information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems.

3. National Strategies

- a. The National Intelligence Strategy (NIS) (October 2005). The NIS includes mission objectives and enterprise objectives. Mission objectives relate to the Nation's efforts to predict, penetrate, and preempt threats to national security, and to assist all who make and

implement U.S. national security policy, fight wars, protect the Nation, and enforce laws in the implementation of national policy goals. Enterprise objectives relate to capacity to maintain competitive advantage over states and forces that threaten the security of the Nation.

b. *The National Security Strategy (NSS)* (March 2006). The NSS establishes broad strategic guidance for advancing U.S. interests in the global environment through the instruments of national power.

c. *The National Strategy for Aviation Security (NSAS)* (March 2007). This Strategy aligns Federal Government aviation security programs and initiatives into a comprehensive and cohesive national effort involving appropriate Federal, State, local, and Tribal governments and the private sector to provide active layered aviation security for, and support defense in-depth of, the United States.

d. *The National Strategy for Homeland Security (NSHS)* (October 2007). The NSHS defines homeland security as a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur. Consistent with the *National Strategy for Combating Terrorism* (September 2006), the purpose of the NSHS is to guide and unify the Nation's homeland security efforts. It provides a common framework within which the entire Nation should focus its efforts on the following four goals: prevent and disrupt terrorist attacks; protect the American people, the Nation's critical infrastructure, and key resources; respond to and recover from incidents that do occur; and continue to strengthen the foundation to ensure long-term success. The NSHS outlines the Homeland Security Management System, and within that context, planning.

e. *The National Strategy to Combat Weapons of Mass Destruction* (December 2002). This document states that nuclear, biological, and chemical weapons in the possession of hostile states and terrorists represent one of the greatest security challenges facing the United States and that the Nation must pursue a comprehensive strategy to counter this threat in all of its dimensions. Three principal pillars are counter-proliferation to combat its use, nonproliferation to combat proliferation, and consequence management to respond to its use.

f. *The National Strategy for Combating Terrorism* (September 2006). This document expands on the NSS by expounding on the need to destroy terrorist organizations, win the war of ideas, and strengthen America's security at home and abroad. While the NSS focuses on preventing terrorist attacks within the United States, this strategy is more proactive and focuses on identifying and defusing threats before they reach United States borders. The direct and continuous action against terrorist groups will disrupt, and over time, degrade and ultimately destroy their capability to attack the United States.

g. *The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets* (February 2003). This document defines the road ahead for a core mission area identified in the President's NSHS. It identifies a clear set of national goals and objectives to achieve the United States' critical infrastructure protection goals. The strategy identifies 13 critical infrastructure sectors. Key asset protection represents a broad array of unique facilities, sites, and structures whose disruption or destruction could have significant consequences across multiple dimensions. Examples include, but are not limited to, nuclear power plants, national monuments, and commercial centers where large numbers of people congregate.

h. *The National Strategy for Securing Cyberspace* (February 2003). This document, an implementing component of the NSHS, engages and empowers Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact – an effort that will require a coordinated and focused effort from the entire society, including Federal, State, and local governments. This strategy outlines a framework for organizations as well as for individual Americans to improve the collective cyber security. It identifies three strategic objectives prevent cyber attacks against American critical infrastructure, reduce national vulnerability to cyber attacks, and minimize damage and recovery time from cyber attacks that do occur.

i. *The National Strategy for Maritime Security* (September 2005). This document provides three broad principles as overarching guidance for maritime security:

- (1) Preserving the freedom of the seas;
- (2) Facilitating and defending commerce to ensure this uninterrupted flow of shipping; and
- (3) Facilitating the movement of desirable goods and people across United States borders, while screening out dangerous people and material.

j. *The National Military Strategy (NMS)* (February 2008). The NMS, derived from the NSS, focuses on how the Armed Forces of the United States will be employed to accomplish national strategic objectives.

4. Other National Documents

a. *National Response Framework (NRF)* (January 2008), issued by the Department of Homeland Security. The NRF is a guide to how the Nation conducts all-hazards response. It is built on scalable, flexible, and adaptable coordinating structures to align key roles and responsibilities across the Nation, linking all levels of government, non-governmental organizations (NGO), and the private sector. It is intended to capture specific authorities and best practices for managing incidents that range from the serious but purely local, to large-scale terrorist attacks or catastrophic natural disasters.

b. *National Incident Management System (NIMS)* (March 2004), issued by the Department of Homeland Security. The NIMS represents a core set of doctrine, concepts, principles, terminology, and organizational processes to enable effective, efficient, and collaborative incident management at all levels.

c. *National Infrastructure Protection Plan (NIPP)* (2006), issued by the Department of Homeland Security. The NIPP provides a coordinated approach to establish national priorities, goals, and requirements for CIKR protection so that Federal funding and resources are applied in the most effective manner to reduce vulnerability, deter threats, and minimize the consequences of attacks and other incidents. It establishes the overarching concepts relevant to all CIKR sectors identified in HSPD-7, and addresses the physical, cyber, and human considerations required for effective implementation of comprehensive programs. The plan specifies the key initiatives, milestones, and metrics required to achieve the Nation's CIKR protection mission. It sets forth a comprehensive risk management framework and clearly defined roles and responsibilities for the Department of Homeland Security; Federal Sector-Specific Agencies; and other Federal, State, local, Tribal, and private sector security partners.

d. National Preparedness Guidelines (September 2007), issued by the Department of Homeland Security. The *Guidelines* include a vision, capabilities, and priorities for national preparedness. To support a consistent nationwide approach to implementation, the *Guidelines* establish three capabilities-based preparedness tools and a National Preparedness System. Purposes of the *Guidelines* include:

- (1) Organize and synchronize national (including Federal, State, local, and Tribal) efforts to strengthen national preparedness;
- (2) Guide national investments in national preparedness;
- (3) Incorporate lessons learned from past events into national preparedness priorities;
- (4) Facilitate a capability-based and risk-based investment planning process; and
- (5) Establish readiness metrics to measure progress and a system for assessing the Nation's overall preparedness capability to respond to major events, especially those involving acts of terrorism.

e. National Implementation Plan for the War on Terror (NIP-WOT) (September 2008). The NIP-WOT is designed to integrate U.S. Government counterterrorism activities and to provide a common strategic direction. It implements NSPD-46/HSPD-15 (*U.S. Strategy and Policy in the War on Terror* (March 2006)).

f. The Strategy for Homeland Defense and Civil Support, issued by the Department of Defense (DOD), June 2005. This *Strategy* focuses on achieving DOD's paramount goal: securing the United States from direct attack. It states that DOD's response capabilities will be planned, practiced, and carefully integrated into the national response. Guiding homeland defense planning is the concept of an active, layered defense, predicated on seizing the initiative from adversaries. A major objective of DOD's enabling activity is to improve national and international capabilities for homeland defense and homeland security, with DOD's core capability of effective interagency planning and interoperability.

Intentionally Left Blank

ANNEX G: SELECTED GLOSSARY OF IPS TERMS

All-Hazards	Term that encompasses domestic terrorist attacks, major disasters, and other emergencies. ³⁰
Branch Plan	A modification to an existing plan that usually adjusts the required resources or concept of operations. However, the end-state normally remains the same. For example, an existing plan calls for delivering medical supplies by rail transport but the situation prevents using rail. Delivering the supplies by air transport or a combination of air and road transport represent a “branch” plan. See “sequel plan.”
Capability-based Planning	Planning approach that focuses on available personnel and their resources that can be applied to address various significant incidents.
Catastrophic Incident	Any natural disaster, act of terrorism, or other manmade disaster that results in extraordinary levels of casualties or damage or disruption severely affecting the population (including mass evacuations), infrastructure, environment, economy, national morale, or government functions in an area. ³¹
Communities of Interest (COI)	Groups of organizations or organizational components that have a common interest or overlapping responsibilities.
Concept of Operations (CONOPS)	A statement that clearly and concisely expresses what the senior leader intends to accomplish and how it will be done using available resources. The concept is designed to give an overall picture of the homeland security operation. A CONOPS’ scope will change based on the planning level; a strategic CONOPS has a broader scope in space and time while a tactical CONOPS has a narrower scope in space and time.
Concept Plan (CONPLAN)	A plan that briefly describes the concept of operations for integrating and synchronizing existing Federal capabilities to accomplish the mission-essential tasks, and describes how Federal capabilities will be integrated into and support regional, State, local, and Tribal plans. ³² It is a product of the operational planning level.
Contingency Planning	Planning that occurs before the incident or in the pre-incident phase. A contingency plan provides guidance for conducting operations.

³⁰ *National Response Framework.*

³¹ Public Law 109-295, Post Katrina Emergency Management Act (PKEMRA) of 2006.

³² HSPD-8/Annex I, National Planning, Approved 03 December 2007.

Course of Action (COA)	Means available to the decision maker by which the objectives may be attained. A course of action is a broadly stated, potential solution to an assigned mission. A systems analysis usually considers several possible courses of action, which are then referred to as alternatives or as the decision maker's options.
Crisis Action Planning	A planning approach that outlines incident priorities, objectives, and initial actions, and drives the development of supporting plans. Initial activities may include search and rescue, evacuations, communication of key information to the public, restoration of essential critical infrastructure, and provision of community law enforcement, fire, and emergency medical services among others. ³³
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.
Dynamic Planning	The process used by the National Counter Terrorism Center (NCTC) Directorate of Strategic Operational Planning (DSOP) to react to emerging threats and/or incidents.
Federal	Of or pertaining to the Federal Government of the United States of America. ²⁴
Functional Planning	Planning approach that identifies the common tasks that the community must perform during emergencies.
Hazard	A source of potential danger or harm, often the root cause of an unwanted outcome. ³⁴
Homeland Security Management System (HSMS)	A continuous cycle of four phased activities, including guidance, planning, execution, and assessment and evaluation. ³⁵
Incident	An occurrence or event, natural or manmade, that requires a response to protect life or property. Incidents can, for example, include major disasters, emergencies, terrorist attacks, terrorist threats, civil unrest, wildland and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, tsunamis, war-related disasters, public health and medical emergencies, and other occurrences requiring an emergency response. ³⁶

³³ *National Strategy for Homeland Security*, Homeland Security Council, Approved October 2007.

³⁴ *National Incident Management System (NIMS)*, March 2004

³⁵ *National Strategy for Homeland Security*, Homeland Security Council, Approved October 2007.

³⁶ *National Incident Management System*, Approved 01 March 2004

Lessons Learned	A collection and analysis of data from a variety of current and historical sources, including operations and training events, that produces lessons for leaders and practitioners, staffs, and homeland security community at large.
National	Of a nationwide character, including Federal, State, local, and Tribal aspects of governance and policy.
National Domestic Preparedness Consortium (NDPC)	Organization composed of five organizations: the DHS Center for Domestic Preparedness, the U.S. Department of Energy’s Nevada Test Site, Louisiana State University, the New Mexico Institute of Mining and Technology, and Texas A&M University. The NDPC leverages the collaborative relationship among its members, its affiliations with academic, State, and Federal institutions, and its expertise in academic disciplines, curriculum development, and instructional techniques to develop and deliver specialized training programs that address the most urgent needs of the emergency response community.
National Exercise Program (NEP)	A national, interagency-wide program that serves as the principal mechanism for examining the preparation and efficiency of Federal departments and agencies. It provides a system that aligns Federal, State, local, and Tribal exercise programs and objectives with U.S. Government-wide priorities to prevent and respond to domestic terrorist attacks, major disasters, and other emergencies. NEP also provides a method to examine emerging policy issues and to determine procedures to implement or modify them.
National Incident Management System (NIMS)	A system mandated by HSPD-5 that provides a consistent nationwide approach for Federal, State, local, and Tribal governments; the private sector; and NGOs to work effectively and efficiently together to prepare for, respond to, and recover from incidents, regardless of cause, size, or complexity. To provide for interoperability and compatibility among Federal, State, Tribal, and local capabilities, NIMS includes a core set of concepts, principles, and terminology. HSPD-5 identifies these as the Incident Command System (ICS); multi-agency coordination systems; training; identification and management of resources (including systems for classifying types of resources); qualification and certification; and the collection, tracking, and reporting of incident information and incident resources. ³⁷
National Planning Scenario (NPS)	An event or threat scenario appropriate for national planning by and among all levels and jurisdictions or government, and in coordination with private, non-profit, and volunteer organizations. ³⁸

³⁷ *National Incident Management System*, Approved 01 March 2004.

³⁸ HSPD-8/Annex I, National Planning, December 3, 2007.

National Preparedness Guidelines (NPG)	Guidance for Federal departments and agencies; State, Tribal, and local officials; the private sector; NGOs; and the public in determining how to most effectively and efficiently strengthen preparedness for terrorist attacks, major disasters, and other emergencies. This document lays out 15 NPSs that form the basis of the newly coordinated national exercise schedule and priorities, and it identifies 37 core capabilities that are needed to support incident management across the Nation. These <i>Guidelines</i> identify core community and State capabilities that will be supported by the DHS homeland security grant programs.
National Response Doctrine	Defines basic roles, responsibilities, and operational concepts for response across all levels of government and with NGOs and the private sector. The doctrine contains the following five key principles: 1) Engaged partnership; 2) Tiered response; 3) Scalable, flexible, and adaptable operational capabilities; 4) Unity of effort through unified command and 5) Readiness to act. ³⁹
Objective	A clearly defined, decisive, and attainable goal toward which a homeland security operation is directed.
Operation	A homeland security action or the carrying out of a strategic, operational, or tactical homeland security mission.
Operations Plan (OPLAN)	A plan that identifies detailed resource, personnel, and asset allocations in order to execute the objectives of the strategic plan and turn strategic priorities into operational execution. An operations plan contains a full description of the concept of operations, including specific roles and responsibilities, tasks, integration, and actions required, with support function annexes as appropriate. ⁴⁰ It represents a product of the operational planning level.
Parallel Planning	Those rare situations when planning occurs concurrently across all Federal planning levels for a specific scenario or threat. The higher planning level must still lead off the parallel planning effort to inform the next level's planning. The key distinction with parallel planning is that the lower planning level does not have to wait for the higher planning level's approved plan in order to begin planning. This is essential to speed up the process and allows participating organizations the maximum time to conduct their own planning. Parallel planning relies on accurate and timely notification from the higher planning level and a full sharing of information between planning levels as it becomes available.

³⁹ *National Response Framework*, January 8, 2008.

⁴⁰ HSPD-8/Annex I, *National Planning*, December 3, 2007.

Planning Policy	A standardized approach to national planning to integrate and effect policy and operation objectives to prevent, protect against, respond to, and recover from all hazards, and comprises: (a) a standardized Federal planning process; (b) national planning doctrine; (c) resourced operational and tactical planning capabilities at each Federal department and agency with a role in homeland security; (d) strategic guidance, strategic plans, concepts of operations, and operations plans and as appropriate, tactical plans; and (e) a system for integrating plans among all levels of government. ⁴¹
Prevention	Term that refers to activities undertaken by the first responder community during the early stages of an incident to reduce the likelihood or consequences of threatened or actual terrorist attacks. ⁴²
Protection	Involves actions or measures taken to cover or shield from exposure, injury, or destruction. Protection safeguards citizens and their freedoms, critical infrastructure, property, and the economy from acts of terrorism, natural disasters, or other emergencies. ⁴³
Recovery	Short-term and long-term efforts for the rebuilding and revitalization of affected communities and region. ⁴⁴
Response	Embodies the actions taken in the immediate aftermath of an incident to save lives, meet basic human needs, and reduce the loss of property. ⁴⁵
Risk	A measure of expected losses over time; homeland security risk for a particular scenario is a product of the expected threat, vulnerability and consequence based on a particular scenario.
Risk Assessment	A structured process for identifying the expected loss for a system, organization, object, or asset through the evaluation of threats, vulnerabilities and consequences.
Risk Management	The human activity that integrates recognition of risk, risk assessment, developing strategies to manage it, and mitigation of risk using managerial resources. The strategies include transferring the risk to another party, avoiding the risk, reducing the negative effect of the risk, and accepting some or all of the consequences of a particular risk.

⁴¹ HSPD-8/Annex I, National Planning, December 3, 2007.

⁴² HSPD-8, Preparedness, Approved December 2003, Amended December 2007 by Annex I to HSPD-8.

⁴³ DHS Lexicon Terms and Definitions, Approved 23 October 2007.

⁴⁴ *National Strategy for Homeland Security*, Homeland Security Council, October 2007.

⁴⁵ *Ibid.*

Scenario-Based Planning	Planning approach that uses scenarios as a focal point for developing the actions necessary to prevent, protect against, respond to, and recover from the specific scenario. <i>HSPD-8</i> , Annex I, requires the production of scenario based plans by using the NPSs.
Senior Leader	For the purposes of the IPS, the Federal official tasked to oversee homeland security operations under the plan being prepared. For example, the Secretary of Homeland Security would be the senior leader for strategic plans based on the NPSs.
Sequel Plan	A follow-on plan to an existing plan. A sequel has a different end-state from the previous plan. For example, a prevention plan's end-state is to prevent a terrorist attack. If terrorist organization successfully attacks, a response plan will be executed; this response plan is a sequel plan to the prevention plan. See "branch plan".
Situational Awareness	The mental representation and understanding of objects, events, people, system states, interactions, environmental conditions, and other situation-specific factors affecting human performance in complex and dynamic tasks.
Staff Estimate	An estimate that consists of significant facts, events, and conclusions for various functional areas (e.g., information, intelligence, resources, and operations) based on current or anticipated situations.
State Militia/State Defense Forces	A defense force organized and maintained by a State, the Commonwealth of Puerto Rico, the District of Columbia, Guam, or the Virgin Islands may, as provided by its laws. A defense force established under 32 U.S.C. Section 109 may be used within the jurisdiction concerned, as its chief executive (or commanding general in the case of the District of Columbia) considers necessary, but it may not be called, ordered, or drafted into the armed forces.
Strategic Guidance Statement	A document that outlines strategic priorities, broad national strategic objectives, and basic assumptions; describes the envisioned end state; and establishes the general means necessary to accomplish that end. ⁴⁶
Strategic Plan	A plan that defines the mission, identifies authorities, delineates roles and responsibilities, establishes mission-essential tasks, determines required and priority capabilities, and develops performance and effectiveness measures. ⁴⁷ It is the product of the strategic planning level.
Task	Specific actions that are implemented to achieve the identified objectives.

⁴⁶ HSPD-8/Annex I, National Planning, Approved 03 December 2007.

⁴⁷ HSPD-8/Annex I, National Planning, Approved 03 December 2007.

Tactical Plan	The detailed development and identification of individual tasks, actions, and objectives tailored to specific situations and fact patterns at an operational level. Tactical planning is meant to support and achieve the objectives of the operations plan. ⁴⁸ It represents the product of the tactical planning level.
Threat	In general, threat refers to terrorist organizations that may attack the United States. It also encompasses the potential effects from a successful terrorist attack.
Tribe or Tribal	Referring to any Indian tribe, band, nation, or other organized group or community, including any Alaskan Native Village as defined in or established pursuant to the Alaskan Native Claims Settlement Act (85 Stat. 688) [43 U.S.C.A. and 1601 et seq.], that is recognized as eligible for the special programs and services provided by the United States to Indians because of their status as Indians.
Unified Command	An element of multi-jurisdictional or multi-agency incident management activities that provides structure to enable agencies with different legal, geographical, and functional responsibilities to coordinate, plan, and interact effectively. ⁴⁹
Voluntary Training Enhancement Program (VTEP)	Accelerates first responder training by decentralizing approved training. VTEP builds Federal, State, local, and Tribal training capacity by leveraging the expertise of existing training programs.

⁴⁸ HSPD-8/Annex I, National Planning, Approved 03 December 2007.

⁴⁹ National Response Framework, Approved 08 January 2008.

Intentionally Left Blank

ANNEX H: SELECTED ABBREVIATIONS AND ACRONYMS

ARC	American Red Cross
CAP	Crisis Action Planning
CI	Critical Infrastructure
CIR	Critical Information Requirement
COA	Course of Action
COI	Communities of Interest
CONOPS	Concept of Operations
CONPLAN	Concept Plan
CPG	Comprehensive Preparedness Guide
DHS	Department of Homeland Security
DOC	Department of Commerce
DOD	Department of Defense
DOE	Department of Energy
DOI	Department of the Interior
DOJ	Department of Justice
DOL	Department of Labor
DOS	Department of State
DOT	Department of Transportation
DNI	Director of National Intelligence
DSOP	Directorate of Strategic Operational Planning
ED	Department of Education
EPA	Environmental Protection Agency
FBI	Federal Bureau of Investigation

FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
GSA	General Services Administration
HHS	Department of Health and Human Services
HSC	Homeland Security Council
HSIN	Homeland Security Information Network
HSMS	Homeland Security Management System
HSPD	Homeland Security Presidential Directive
HUD	Department of Housing and Urban Development
IC	Intelligence Community
ICS	Incident Command System
IPS	Integrated Planning System
KR	Key Resources
MOU	Memorandum of Understanding
NASA	National Aeronautics and Space Administration
NCTC	National Counterterrorism Center
NDPC	National Domestic Preparedness Consortium
NEP	National Exercise Program
NGO	Nongovernmental Organizations
NHSP	National Homeland Security Plan
NIMS	National Incident Management System
NIP-WOT	National Implementation Plan for the War on Terror
NIPP	National Infrastructure Protection Plan
NIS	National Intelligence Strategy
NPES	National Planning and Execution System

NPG	National Preparedness Guidelines
NPS	National Planning Scenario
NRC	Nuclear Regulatory Commission
NRF	National Response Framework
NSAS	National Strategy for Aviation Security
NSC	National Security Council
NSHS	National Strategy for Homeland Security
NSPD	National Security Presidential Directive
NSS	National Security Strategy
NTSB	National Transportation Safety Board
NVOAD	National Voluntary Organizations Active in Disaster
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
OPLAN	Operations Plan
OPM	Office of Personnel Management
P.L.	Public Law
PKEMRA	Post-Katrina Emergency Reform Act
SBA	Small Business Administration
SCI	Sensitive Compartmented Information
SGS	Strategic Guidance Statement
SME	Subject Matter Expert
SSA	Social Security Administration
TREAS	Department of the Treasury
TVA	Tennessee Valley Authority
USAID	U.S. Agency for International Development

U.S.C.	United States Code
USCG	U.S. Coast Guard
USDA	Department of Agriculture
USPS	U.S. Postal Service
VA	Department of Veterans Affairs
VTEP	Voluntary Training Enhancement Program

