2005-09

Homeland security and capabilities-based planning : improving national preparedness

Caudle, Sharon L.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

HOMELAND SECURITY AND CAPABILITIES-BASED PLANNING: IMPROVING NATIONAL PREPAREDNESS

by

Sharon L. Caudle

September 2005

Thesis Co-Advisors: C. J. LaCivita
Kathryn E. Newcomer

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2005	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Homeland Security and Capabilities-Based Planning: Improving National Preparedness			**5. FUNDING NUMBERS**
6. AUTHOR(S) Sharon L. Caudle			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense, the Government Accountability Office, or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

Beginning in 2004, the Department of Homeland Security (DHS) began to define and implement a national domestic all-hazards preparedness goal, intended to improve the nation's preparedness for national catastrophes, including terrorist attacks. DHS's approach was capabilities-based planning (CBP), adopted from the Department of Defense (DoD). CPB is intended to develop the means—capabilities—for organizations to set priorities responding to a wide range of potential, but uncertain challenges and circumstances, mindful of issues of cost and sustainability. This thesis is intended to help officials better understand CBP and the factors important to its successful implementation. These factors range from setting out the business case for CBP adoption to necessary organizational and cultural enablers. In conclusion, the thesis recommends enhancing the CBP approach to national preparedness planning through integrating its approach with use of a national preparedness management standard, coverage of the mission areas of the National Strategy for Homeland Security, and encouraging performance partnership and collaborative methods.

14. SUBJECT TERMS Homeland security, national preparedness, capabilities-based planning			**15. NUMBER OF PAGES** 111
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited.

HOMELAND SECURITY AND CAPABILITIES-BASED PLANNING: IMPROVING NATIONAL PREPAREDNESS

Sharon L. Caudle
B.A., University of Nevada, Reno, 1971
M.P.A., The George Washington University, 1985
Ph.D., The George Washington University, 1988

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES (HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
September 2005

Author: Sharon L. Caudle

Approved by: Dr. C. J. LaCivita
Thesis Co-Advisor

Dr. Kathryn E. Newcomer
Co-Advisor

Dr. Douglas Porch
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Beginning in 2004, the Department of Homeland Security (DHS) began to define and implement a national domestic all-hazards preparedness goal, intended to improve the nation's preparedness for national catastrophes, including terrorist attacks. DHS's approach was capabilities-based planning (CBP), adopted from the Department of Defense (DoD). CPB is intended to develop the means—capabilities—for organizations to set priorities responding to a wide range of potential, but uncertain challenges and circumstances, mindful of issues of cost and sustainability. This thesis is intended to help officials better understand CBP and the factors important to its successful implementation. These factors range from setting out the business case for CBP adoption to necessary organizational and cultural enablers. In conclusion, the thesis recommends enhancing the CBP approach to national preparedness planning through integrating its approach with a national preparedness management standard, coverage of the mission areas of the National Strategy for Homeland Security, and encouraging performance partnership and collaborative methods.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

ASJETs	Australian Joint Essential Tasks
CBP	Capabilities based planning
CONOPS	Concepts of operations
CRRA	Capabilities Review and Risk Assessment
DoD	Department of Defense
DHS	Department of Homeland Security
FCB	Functional Capabilities Board
GAO	Government Accountability Office, General Accounting Office
HSPD	Homeland Security Presidential Directive
IED	Improvised explosive device
JCIDS	Joint Capabilities Integration and Development System
NIMS	National Incident Management System
NRP	National Response Plan
ODP	Office for Domestic Preparedness (DHS)
OSLGCP	Office of State and Local Government Coordination and Preparedness (DHS)
PPBS	Planning, Programming, and Budgeting System
TCL	Target Capabilities List
TCP	Technical Cooperation Program
UJTL	Universal Joint Task List
UTL	Universal Task List

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. MANAGING FOR RESULTS

Over the past several years, government's "managing for results" movement has shifted management attention from inputs, processes, and outputs to what they accomplish—outcomes or results. Wholey (2002, p. 14) defines results-oriented management as "the purposeful use of resources and information to achieve and demonstrate measurable progress toward outcome-oriented agency and program goals." Newcomer (1997) pinpoints the importance of linking measures to program mission, setting performance targets, and reporting whether the target levels of performance or expected results were achieved. Aristigueta (1999) writes that the rationale for results management is that government's effectiveness, efficiency, and accountability will improve as agencies focus management on what programs should achieve.

A few months after the September 11, 2001, terrorist attacks, David (2002, pp. 2-3) presented the challenge of managing results for homeland security. Focusing on the need to set a homeland security goal, she observed that a goal would provide a context to make decisions, set investment priorities, and measure progress. A few years later, a presidential homeland security directive required a national preparedness goal, priorities, targets, and measures. In response, the Department of Homeland Security (DHS) began implementing the presidential directive through a capabilities-based planning approach (CBP) adopted from the Department of Defense (DoD). Kelley and others (2003) and Davis (2002) describe CPB as planning under uncertainty to develop the means—capabilities—to respond to a wide range of potential challenges and circumstances while mindful of costs and sustainability.

This thesis recommends an approach to better leverage CBP for national preparedness planning by combining it with other components. The thesis first provides an overview of homeland security and preparedness expectations. Second, it presents an overview of CBP concepts and methodology. Third, it describes the DHS adoption of CBP and its current status. Fourth, it describes components for CBP implementation, drawing on experiences of DoD and other allied countries' defense communities. Fifth,

the thesis contrasts the homeland security and defense community components, transferability factors, and other implementation issues. Finally, it recommends integrating CBP with a national management system standard, comprehensive homeland security mission area coverage, and performance partnerships.

B. METHODOLOGY

The primary research method was a content analysis of 1) homeland security literature, government strategies and reports, formally chartered commissions examining homeland security and homeland defense, and observations of experts in the field describing results expectations, strategies, and measurement, 2) public sector literature on managing for results, including performance management and measurement approaches, implementation strategies, and challenges, and 3) material on defense community and homeland security adoption of capabilities-based planning. In addition, the author participated in several meetings and conferences on capabilities-based planning and is an active participant on committees involved with national emergency management and national preparedness standards. This material was used in a synthesis approach to describe and analyze homeland security mission results expectations, defense community capabilities-based planning experiences and core components, homeland security adoption of capabilities-based planning, and enhancements for homeland security capabilities-based planning.

Homeland security results management is an uncertain area at present. Well-defined approaches, including capabilities-based planning, have not been rigorously tested. As part of the methodology, the author asked homeland security and defense community experts to review findings and recommendations about the preliminary CBP adoption. The experts included officials from the Government Accountability Office's Homeland Security and Justice Team (four officials), Defense Capabilities Management Team (two), and Advanced Research Methods Team (one); the Analytical Services' Homeland Security Institute (three); the George Washington University's Homeland Security Policy Institute (two); the Congressional Research Service (one); the Department of Defense Joint Chiefs of Staff (one); the National Emergency Management Accreditation Program (one); the American National Standards Institute (three); the IBM

Business of Government program (one), BearingPoint, Inc. (two), and the Department of Homeland Security (three). In addition, selected state and local officials were asked to review the draft thesis (three).

The experts' observations were incorporated into the final thesis. The experts agreed with the characterization of the implementation factors, their importance, and the utility of integrating CBP with other tools and approaches. State and local officials requested more details on how the recommendations might be implemented.

THIS PAGE NTENTIONALLY LEFT BLANK

II. HOMELAND SECURITY AND NATIONAL PREPAREDNESS OVERVIEW

A. DEFINING HOMELAND SECURITY

The definition of homeland security is the starting point for managing homeland security results. The National Strategy for Homeland Security (Office of Homeland Security 2002, p. 2) defines homeland security in sweeping terms 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." The National Strategy defines these areas more fully, where:

- Prevention means action at home and abroad to deter, prevent, and eliminate terrorism.
- Vulnerability reduction means identifying and protecting critical infrastructure and key assets, detecting terrorist threats, and augmenting defenses, while balancing the benefits of mitigating risk against economic costs and infringements on individual liberty.
- Response and recovery means managing the consequences of attacks, and building and maintaining the financial, legal, and social systems to recover.

The more broadly-scoped "national preparedness" covers any major disaster or emergency event, including terrorist attacks, as part of all-hazards planning. For example, Homeland Security Presidential Directive 8 (HSPD-8) defines preparedness as the "existence of plans, procedures, policies, training, and equipment necessary at the federal, state, and local level to maximize the ability to prevent, respond to, and recover from major events" (The White House 2003, p. 2). The National Incident Management System (DHS 2004a, p. 4) adds personal qualification and certification standards and publication management processes and activities to the HSPD-8 definition.

The December 2003 Gilmore Commission (formally known as the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction) report stresses capacity for preparedness. It defines preparedness as "the measurable demonstrated capacity by communities, States, and private sector entities throughout the United States to respond to acute threats with well-planned, well-

coordinated, and effective efforts by all of the essential participants, including elected officials, police, fire, medical, public health, emergency managers, intelligence, community organizations, the media, and the public at large" (Gilmore Commission 2003, p. 8).

B. HOMELAND SECURITY GOALS AND STRATEGIES

Whether the more narrowly targeted homeland security mission or the broader national preparedness definition is used, there are many expectations for what homeland security or national preparedness should accomplish and how. National strategies, presidential directives, and reports from Congressionally-charted commissions provide rich sources of expectations.

The National Strategy for Homeland Security (National Strategy) is the primary document that frames results expectations. The National Strategy defines homeland security and its missions, what should be accomplished, and the most important goals, current accomplishments, and recommendations for federal and non-federal governments, the private sector, and citizen action. The core of the National Strategy is its six critical mission areas focusing on prevention, vulnerability reduction, and response and recovery expectations. The mission areas include:

- Intelligence and warning: Deter terrorist activity before it manifests itself in an attack so proper preemptive, preventative, and protective action can be taken;
- Border and transportation security: Promote the efficient and reliable flow of people, goods, and services across borders while preventing terrorists from using transportation conveyances or systems to deliver implements of destruction;
- Domestic counterterrorism: Identify, halt, and where appropriate, prosecute terrorists in the United States, including those directly involved in terrorist activity and their sources of support;
- Critical infrastructure and key asset protection: Protect the nation's critical infrastructure and key assets to levels appropriate to each target's vulnerability and criticality;
- Catastrophic threat defense: Develop new approaches, a focused strategy, and a new organization to address chemical, biological, radiological, and nuclear terrorist attacks; and

- Emergency preparedness and response: Develop a comprehensive national system to bring together and coordinate all necessary response assets quickly and effectively.

The National Strategy also sets out four foundations of the six mission areas to involve all levels of government and sectors of society. The foundations are law, science and technology, information sharing and systems, and international cooperation. The National Strategy is joined by other national strategies, described by the Government Accountability Office (GAO) (2004a, table 2, pp. 5-6), covering other security aspects or expanding implementation details for specific topics. These strategies include, for example, the National Security Strategy of the United States of America, the National Strategy for Combating Terrorism, and the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. Each strategy has specific objectives. To illustrate, the critical infrastructures and key assets strategy has objectives to 1) identify and assure the protection of the most critical assets, 2) ensure protection of infrastructures and assets facing specific, imminent threats, and 3) pursue collaborative measures and initiatives to ensure the protection of other potential targets.

DHS's first strategic plan (Department of Homeland Security 2004b, p. 9) also identifies a series of strategic goals for securing the homeland from terrorist attacks, similar to the National Strategy. In addition to organizational excellence, these included:

- Awareness: Identify and understand threats, assess vulnerabilities, determine potential impacts, and disseminate timely information to our homeland security partners and the American public;
- Prevention: Detect, deter, and mitigate threats to our homeland;
- Protection: Safeguard our people and their freedoms, critical infrastructure, property, and the economy of our nation from acts of terrorism, natural disasters, or other emergencies;
- Response: Lead, manage, and coordinate the national response to acts of terrorism, natural disasters, or other emergencies.
- Recovery: Lead national, state, local, and private sector efforts to restore services and rebuild communities after acts of terrorism, natural disasters, or other emergencies.
- Service: Serve the public effectively by facilitating lawful trade, travel, and immigration.

In addition to the high-level direction provided by these national strategies, homeland security presidential directives outline homeland security expectations, many much the same as the strategies. These include, for example, immigration policies to combat terrorism, provide domestic incident management, and protect critical infrastructure. The national strategies and presidential directives are further joined by the recommendations of Congressionally-chartered commissions. In addition to the Gilmore Commission, other well-known commissions include the Bremer Commission (formally known as the National Commission on Terrorism), the Hart-Rudman Commission (formally known as the U.S. Commission on National Security/21st Century), and the 9/11 Commission (formally known as the National Commission on Terrorist Attacks Upon the United States). Table 1 highlights the major recommendation areas of these commissions, with illustrative examples, drawing on a Government Accountability Office (GAO) report (2004b).

Table 1. Examples of Commission Recommendations

Recommendation Areas	Examples
Border and Transportation Security	Integrate US border security into larger network of transportation system screening points Complete biometric entry-exit screening system
Domestic Counterterrorism	Track and confront terrorist financing and travel Make homeland security a primary mission of the National Guard
Critical Infrastructure and Key Asset Protection	Set-risk based priorities Designate DHS as the lead and USDA as the technical advisor on food safety and agriculture and emergency preparedness
International Antiterrorism	Identify and prioritize terrorist sanctuaries Make long-term commitment to Pakistan and Afghanistan Confront US-Saudi relationship problems Negotiate more comprehensive treaties and agreements for combating terrorism with Canada and Mexico
Roots of Terrorism	Provide moral leadership and action; define and defend ideals abroad Encourage economic development, open societies Develop comprehensive coalition strategy against Islamist terrorism
State and Local Assistance	Reform homeland security grant-making and funding sustainability; base assistance on risk assessment Develop comprehensive process for training and exercise standards Revise Homeland Advisory System; adopt Incident Command System
Private Sector Engagement	Promote the adoption of a recommended standard for private preparedness
Weapons of Mass Destruction	Prevent proliferation of WMD Use authority to designate foreign governments as not fully cooperating Establish DoD unified command structure for catastrophic terrorist capabilities
Intelligence and Information Sharing	Establish National Counterterrorism Center, built on TTIC and be a center for joint operational planning and joint intelligence Replace DCI with a National Intelligence Director Aggressively recruit human intelligence sources on terrorism Develop and disseminate continuing comprehensive strategic threat assessments

Recommendation Areas	Examples
	Designate authorities to grant clearances recognized by all federal agencies; develop a new regime of clearances and classification of intelligence for dissemination to states, localities, private sectors Establish a specialized and integrated national security workforce Establish comprehensive procedures for sharing information with relevant state and local officials

C. SETTING EXPECTATIONS

One might argue that implementing all the goals and objectives from the many sources mentioned above would ensure comprehensive homeland security. However, the argument can be made that the many expectations are tantamount to "laundry lists" that may do little to significantly improve homeland security. Instead, there should be a formal process to systematically set what homeland security or national preparedness programs should achieve, even though such a process will be challenging.

Even before the September 11 attacks, Falkenrath (2001) identified issues in defining reasonable and measurable preparedness goals, sustaining preparedness capabilities over time as resource commitments changed, and leveraging a preparedness program to fulfill multiple government priorities. He, like David (2002), recognized that the lack of measurable objectives would prevent the rational allocation of resources and meaningful measurement of progress.

After the September 11 attacks, Kettl (2002) also wondered what homeland security performance systems might work. He identified possible approaches based on outcomes (the presence or absence of a terrorist attack), basic thresholds of preparedness (such as response plans, mutual aid compacts, and equipment availability), and a statistical index of preparedness based on variables (such as the availability of basic equipment and supplies, training and exercises, and external assessments). An independent task force sponsored by the Council on Foreign Relations (2003, p. 8) identified national standards of preparedness as essential capabilities. The task force advocated a minimal level of preparedness and equipment. It urged performance standards to tie funding initiatives to systematic preparation. It also wanted the degree and quality of nationwide preparedness to be measured.

Others emphasize preparedness expectations should further be tied to risk. For example, in its final report, the Gilmore Commission (2003, p. 2) wrote the nation's response to terrorists threats should be measured by how risk is managed, not by seeking total security. More recently, the 9/11 Commission (9/11 Commission 2004) recommended basing homeland security assistance on assessing risks and vulnerabilities, including population and critical infrastructure within each state. The Commission envisioned a panel of security experts to develop written benchmarks for evaluating community needs, with federal homeland security funds allocated according to those benchmarks.

What all agree on is that capabilities must be prioritized, funded, sustained, and assessed to set and update homeland security goals and strategies. Moreover, the capabilities should be defined as a central component of a risk-based planning approach. The next chapter describes the capabilities-based planning approach and its specific features that address these requirements.

III. CAPABILITIES-BASED PLANNING OVERVIEW

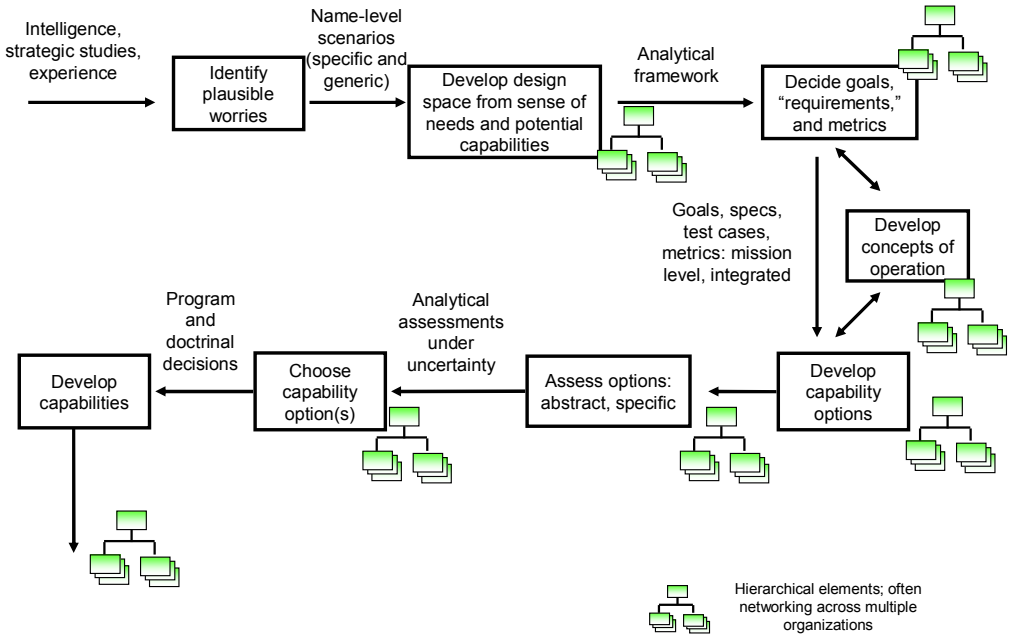
A. CBP ELEMENTS AND PROCESS

Capabilities-based planning is one approach that meets, at least on the surface, the need to manage risk, set specific preparedness goals and priorities, make investment choices, and evaluate preparedness results. The crafters of the CBP approach stress the abilities to accomplish clearly-defined missions in an atmosphere of uncertainty as a fundamental condition and efficient portfolio management as a necessary component. Capabilities are intended to define future operational needs. Davis (2002, p. 4) includes three key elements in his description of CBP for the defense community:

- A conceptual framework for planning under uncertainty by emphasizing capability flexibility, robustness, and adaptiveness,
- An analytical framework with three components: understanding capability needs; assessing capability options at the level of mission or operation; and choosing capability levels and among capability options Choices are done through a portfolio framework that considers other factors such as force management, different types of risk, and economic limitations, and
- A solution framework that emphasizes building blocks.

Davis' (2002, p. 12) CBP model is shown in Figure 1.

Figure 1. Davis CBP Process Model



Davis' model starts with intelligence, strategic studies, and experiences that result in what he calls "plausible worries" (p. 15). The "plausible worries" are the wide range of potential future threats that produce specific and generic scenarios for action. These scenarios can be specific events or longer-term scenarios and should deal with the current term, mid-term, and longer-term timeframes. Scenario inputs can include the political-military context, an adversary's objectives and strategies, forces, force effectiveness, environment, and strategic assumptions, such as how fast maneuvering forces can move.

The scenarios produce, Davis explains, a sense of needs and related capabilities, which enter an analytical framework to define specific capabilities. His analytical framework 1) defines an operational challenge (mission objectives, measures of strategic and operational success), 2) considers a set of options (forces, weapons, command and control, logistics, doctrine, plans, skills, readiness) for meeting the operational challenge, 3) analyzes mission-system capabilities across a wide range of highly uncertain

circumstances (scenario space), and 4) generates an assessment of options that distinguish among situations, characterize risk, and evaluate flexibility, adaptiveness, and robustness. The end-point is making choices among options for mission requirements and the ways to achieve them, including considering tradeoffs in capabilities and addressing issues such as the impact on others, such as allies. Understanding potential requirements, developing proposed capabilities, and evaluating capability options are done at multiple levels both within and across organizational components. Thus, Davis has included hierarchy symbols in his model graphic to reflect the multiple levels of analysis and decision-making.

For results management, the end product might be measures for success contained in what Davis calls "envelopes of capability" (p. 18). These envelopes define specific operational needs. For example, one envelope of capability he cites is the number of cities that can be simultaneously supported with rescue and decontamination teams. In his framework, goals, requirements, and measures are conceived much more in terms of these capability envelopes than particular scenarios.

In later work, Davis (2003) says that the scientific way to look at uncertainty is to acknowledge that wars and military competitions are complex adaptive systems. Small events can have large effects and the system itself is not a constant. The planning approach starts with the core environment, or "no-surprises" future. Then two types of uncertainties are identified. One type are uncertainties that are taken seriously and monitored. They will be resolved at some point as events occur and addressed by in-depth contingency plans. Another type are plausible events that are considered mostly unlikely, but if they occur, can be disruptive.

Davis says planners should develop a broad strategy that would prevent surprises. The approach should include a series of sub-strategies employed on a contingent basis to deal with deviations from what was anticipated in the future. It also should include a set of actions for more ad hoc adaptations to contingencies. The strategy should be designed to positively shape the environment and influence the future. Davis goes on to say that strategic planning to address uncertainty is about judging how best to allocate

investments—a portfolio management approach. He describes a scorecard approach as part of a desirable planning structure.

His framework considers the potential benefits of a new capability and deciding how much mission capability is needed. In addition, capability building blocks must be suitably identified, tailored, and assembled at different levels of organizations and through networks. He states that the defense building blocks for capabilities will be in many forms, such as battalions and brigades; operations to accomplish missions, such as halt an invading army; operational concepts to accomplish operations, such as how to specifically suppress air defenses to help halt an invading army; and resources in the form of platforms such as aircraft, physical systems, such as radars, and enabling infrastructure, such as the global information grid.

B. INCLUSION OF RESULTS MANAGEMENT SYSTEM PRINCIPLES AND ELEMENTS

Davis' CBP approach captures elements found in well-known results management approaches and thus is a viable framework for setting homeland security capabilities. These approaches include 1) traditional strategic planning to set goals, objectives, strategies, and measures, 2) a program logic model, 3) scenario-based planning, and 4) risk management. These approaches and their elements are briefly summarized in Table 2.

Table 2. Results Management Approaches

Approach	Description	Core Elements
Traditional	Formal goal-setting, measurement, and assessment system	Mission driven expectations Strategic and short-term goals and objectives "Vital few" outcome and process measures Assessment
Program Logic Model	Theory of program performance displayed as conversion of inputs to outputs leading to outcomes and desired impacts	Logical, explicit argument of program intervention and impact production Identification of links for production Targeted monitoring of conversion from inputs to outputs to outcomes
Scenario-Based Planning	Identify and plan for possible short and long-term futures and outcomes	Conceptualizing possible futures and outcomes Strategies to address most probable or common across the scenarios
Risk Management	Analysis and decision making to achieve an affordable, acceptable level of risk	Risk and capability assessment Risk profile Risk-based decision-making Evaluation of results

The traditional results management approach contains elements of formal goal-setting, measurement, and assessment as part of a strategic planning effort. Typically, a traditional strategic planning approach consists of several parts (Hatry 1999 and Bryson 1995). One part is defining the mission from legislation, stakeholder performance expectations, or other mission statement or mandate sources. A second part is clarifying strategic and shorter-term goals and objectives from everything possible an organization or program might try to achieve. Long-term programmatic, policy, and management goals set the stage for expected performance levels between two points in time, creating a "vital few" performance goals and specific objectives. Third is developing supporting outcome and process measures. For each vital goal and related objectives, an organization defines what has to happen and possible measures to evaluate progress and compares them to existing process and outcome measures. A final set of measures is selected and incorporated into a measurement system from the activity to the enterprise level. The last part is putting the measures to work—measures are communicated to an organization, baselines and benchmarks defined, strategies (programs, resources, policies, actions) put in place, and progress tracked and reinforced. Goals, strategies, and assessment across organizational boundaries may be included, but not often as a main feature. In addition, the traditional approach typically includes performance-based budgeting, where investment decisions are aligned with expected performance (GAO 1997).

A second approach is a program logic model, also known as a chain of evidence or program theory of action. A program logic model defines program performance or results in terms of a reasonable, sequential "conversion" process: initial inputs are converted to produce outputs that lead to outcomes and final impacts. It provides guidance on what should be monitored to achieve expected immediate, intermediate, and ultimate effects, and makes clear connections from inputs to those effects (see, for example, Hatry 1999; McLaughlin and Jordan 1998, 2004; Millar, Simeone, and Carnevale 2001; Swiss 1995). The individual elements and their connections identify

points of success and failure for program achievements. Performance measurement occurs across the logic model to include capacity, conversion, and effectiveness or impact measures.

A third approach is scenario-based planning. Long-term (stretching over many years) scenario planning was originally designed to deal with how a firm's managers could craft a successful course into the future in the face of significant uncertainty (see, for example, Schwartz and Ogilvy, 1998, p. 2). Scenario planning asks what the future might hold and considers many different possible futures of developments and related outcomes. Not knowing which scenario or variation of a scenario might develop, managers craft strategies to address all scenarios. Longer-term scenario development can help officials anticipate variables and their relationships. For example, the U.S. Coast Guard (McClellan, 2004) uses scenario planning to describe five alternative futures in 2025, such as "Forever War," which features continued terrorist attacks, long-term occupation of Arab countries, and a growing rivalry with China. Specific event, short-term scenarios also are used in planning, such as detailed threat scenarios for preparedness exercises Considering multiple scenarios also can help identify strategies common across the scenarios in a form of nonlinear planning.

A final results management approach is risk management. This is the process of assessing asset value (including people), ranking priorities, and executing decisions under uncertainty to achieve an acceptable level of risk at an affordable cost to support the organization's mission. Risk management tools often are used at a facility level, but can be applied to a large scope, such as an organization or a community. The risk management process consists of four parts—risk and capability assessment, risk profile development, risk-based decisionmaking, and evaluating results and adjusting risk management action (ASIS International, 2003 and Treasury Board of Canada, 2001).

CBP planning incorporates the main features of these four approaches. CBP sets requirements and measures through a process of scenario-analysis. It then selects options, and makes final decisions through multiple levels of analysis and decision-making. These are features of traditional planning. Like the program logic model, CBP considers a set of options to meet operational needs or outcomes. Scenario-based

planning is reflected in the use of specific events or longer-term scenarios dealing with current term, mid-term, and longer-term timeframes. Finally, CBP addresses risk management through upfront intelligence about possible disruptive events, analyzing capabilities across uncertain circumstances and risk characteristics, and then making investment choices about how to achieve mission requirements. Overall, CBP's process includes the basic elements for a results management approach that should be useful for homeland security.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. DHS CAPABILITIES-BASED PLANNING ADOPTION AND CURRENT STATUS

A. HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 8

The directive underlying DHS' CBP adoption is HSPD-8. Issued by the President in December 2003, HSPD-8 called for the DHS Secretary, in coordination with other federal officials and in consultation with state and local governments, to develop a national domestic all-hazards preparedness goal. The goal is to establish readiness priorities that are measurable. It is to balance the potential threat and magnitude of terrorist attacks, major disasters, and other emergencies with the resources required to prevent, respond to, and recover from them. It is to include readiness measures and focus on standards for preparedness assessments and strategies and a system to assess the nation's overall preparedness to respond to major events, especially terrorist acts. The due date for the national preparedness goal was set as the DHS fiscal year 2006 budget submission. Federal preparedness assistance was to be delivered based on state all-hazard preparedness strategies consistent with the national preparedness goal by September 30, 2005 (The White House 2003).

Congress subsequently mandated a national preparedness requirement and its funding application. The October 9, 2004 House-Senate conference report on the DHS fiscal year 2005 appropriations cited HSPD-8 implementation. The report called for DHS's Office of State and Local Government Coordination and Preparedness (OSLGCP) to 1) provide state and local jurisdictions with nationally-accepted first responder preparedness levels no later than January 31, 2005, 2) include in the fiscal year 2005 formula-based grant guidance guidelines for state and local jurisdictions to adopt national preparedness standards in fiscal year 2006, and 3) issue final guidance on the implementation of the national preparedness goal no later than March 31, 2005. According to OSLGCP (2004c), DHS planned to continue utilizing CBP to meet these Congressional requirements. More recently, the National Intelligence Reform Act of 2004 (P. L. 108-458) required DHS to set national performance standards and to ensure that state homeland security plans are in conformance with those standards.

B. HSPD-8 IMPLEMENTATION CONCEPT PAPER

DHS consistently has taken the position, also required by HSPD-8, that DHS would develop the national preparedness goal and related priorities, targets, measures, and standards in coordination with federal organizations and in consultation with state, local, and tribal governments. Since HSPD-8 was issued, DHS drew on experts and governmental and association representations in its rapid development of the national preparedness goal.

In April 2004, DHS's Office for Domestic Preparedness (ODP) issued a draft implementation concept paper for HSPD-8 (ODP 2004c). According to the concept paper, federal preparedness programs must be reoriented in a more unified manner to deliver needed capabilities and correlate to threats. A capability is defined as "a combination of resources (personnel, equipment, and other elements) that provide a means to achieve an outcome, under specified conditions and to national standards" (p. 7). "Unified" means efforts to allow all agencies and government levels with mission responsibility to work together by establishing a common set of objectives and strategies (p. 7). The key actor is the homeland security community, which the document specifies as all levels of government and the private sector and their resources.

The concept paper outlined unified capabilities as the foundation for preparedness programs. Planning would be done as a nationally integrated effort and capabilities developed using a consistent community-wide view of priorities and risks. The concept paper drew heavily on DoD documents and the Davis (2002) CBP approach.

The draft concept paper stated that DHS had identified four priority initiatives to reorient current preparedness programs and implement HSPD-8. These included (p. 9):

- Creation of a unified national preparedness strategy to build the capabilities required by homeland security strategies, missions, and tasks.
- Development of a capabilities-based national preparedness assessment and reporting system to conduct continuous subjective assessments of current national preparedness and to obtain a systematic view of future critical capabilities.
- Establishment of a comprehensive national training and exercise system that provides performance-based training and exercises to achieve and sustain capabilities.

- Balancing of the national portfolio of preparedness investments through tools to inform resource allocation decisions that are linked to required capabilities.

In the concept paper, implementing a unified national preparedness strategy started with building a common lexicon for capabilities citizens expected from elected officials and public agencies to address a terrorist attack, major disaster, or other emergency. This list of mission-level capabilities could draw on documents such as the National Strategy for Homeland Security and the National Incident Management System Resource Typing System.

Another key step was developing standard scenarios to plan, test alternative strategies, set requirements, and determine priorities as it is not possible to predict when and where an incident will occur. The Homeland Security Council developed planning scenarios viewed as describing national significant threats and hazards with high credibility, consequence, and probability. The scenarios included (ODP 2004c, p. 17):

- Four chemical scenarios, including both chemical warfare and toxic industrial chemicals,
- Three biological scenarios, including both contagious and non-contagious agents and pandemic influenza,
- One radiological and one nuclear scenario,
- One improvised explosive device scenario,
- Two agricultural scenarios, including food safety and animal disease,
- Two natural disaster scenarios, a catastrophic earthquake and major hurricane, and
- One cyber attack.

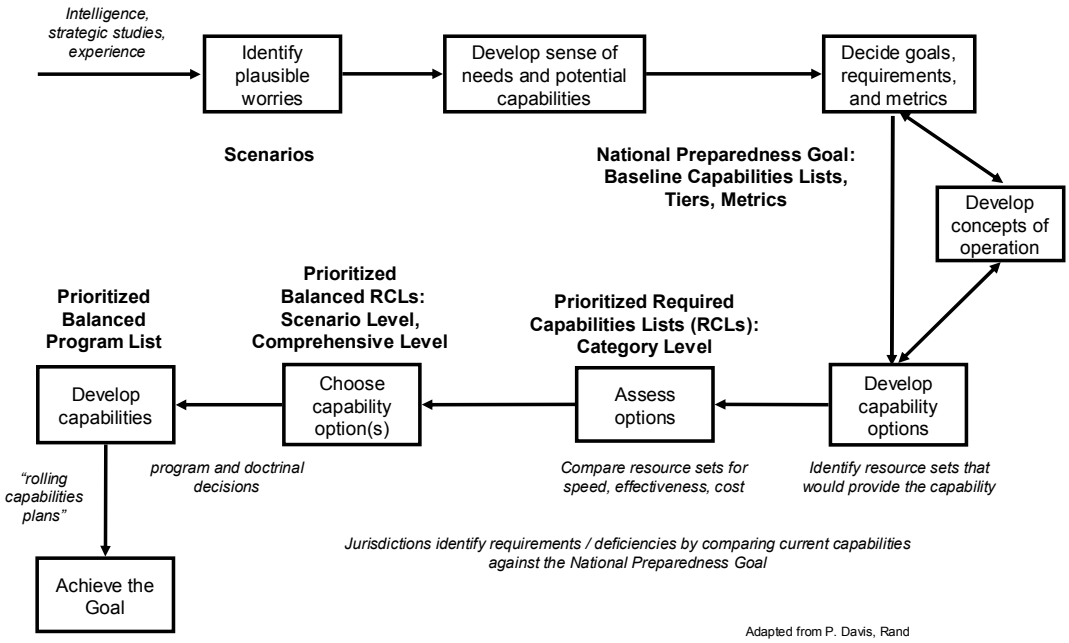
In July 2004, the Homeland Security Council (2004) issued executive summaries of the planning scenarios. The Council document stated that the 15 scenarios were the minimum number necessary to test the range of response capabilities and resources. The Council excluded other high-impact scenarios, such as industrial and transportation incidents or frequently occurring natural disasters. These were considered to have well-developed and tested response plans or the response would be a subset of response capabilities and resources included in the 15 scenarios.

The concept paper stated that the generation and maintenance of the 15 scenarios were to be integrated into the homeland security community's strategic and operational planning systems. The document detailed eight mission areas for each scenario response, such as a) prevention, deterrence, and protection and b) emergency management and response. For example, for the nuclear detonation scenario, the prevention, deterrence, and protection mission area included law enforcement attempts to prevent the device's development and detonation, protection and survey of site boundaries after the detonation, and response to any additional threats or looting or theft issues. The mission areas drew in part on ODP work on homeland security exercises and evaluations.

Finally, the concept paper said that scenario analysis would produce baseline capabilities lists. The lists would include essential capabilities in specific missions considered critical to successfully accomplishing a scenario's mission. The lists would be further tailored to expectations for different jurisdictional tiers, such as localities of different sizes. Limited measures would be used to assess achieving or exceeding the basic capabilities lists. Entities below the federal level were expected to tailor the scenarios used in defining mission-level capabilities to their specific locations and environments. However, the basic capabilities lists were considered the minimum capabilities required to carry out core competencies and essential tasks and would be used as the national preparedness standard.

The concept paper (p. 20) included a CBP process model derived from Davis (2002), shown in Figure 2, to better explain the overall approach, key deliverables, and key decision points. For example, the national preparedness goal of baseline capability lists, jurisdictional tiers, and measures would be the result of the top part of the process.

Figure 2. DHS CBP Process Model



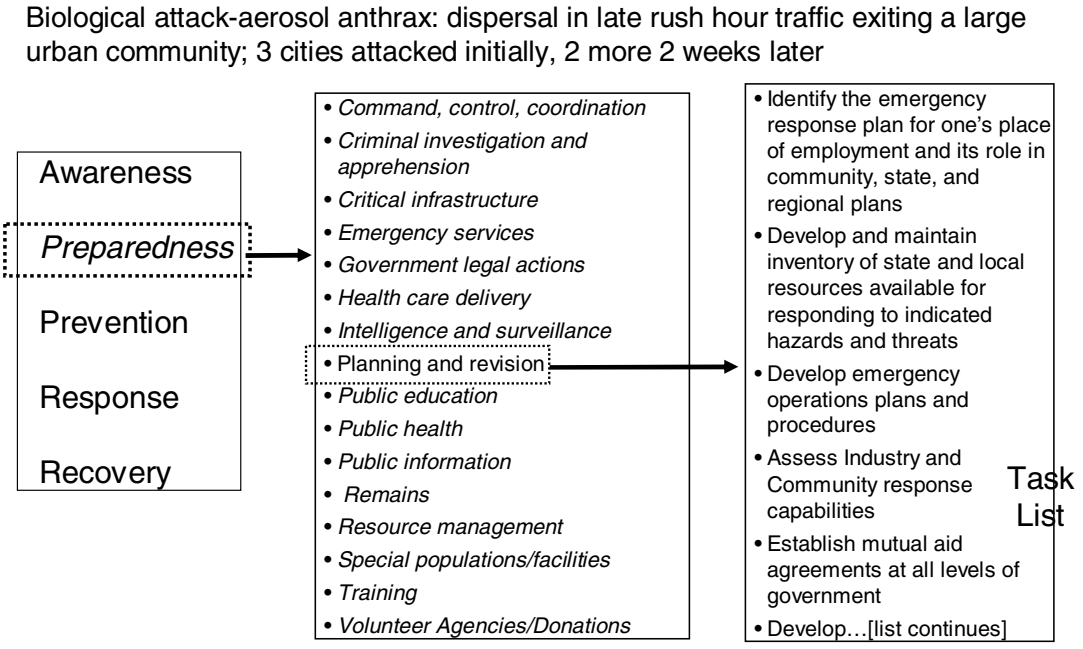
C. DEVELOPING THE INITIAL TASK LISTS

ODP sponsored a Universal Task List Workshop in June 2004 to define the homeland security tasks that should be implemented at all government levels to prevent, respond to, and recover from major terrorist attacks, natural disasters, and other emergencies. Following that workshop, ODP (2004a) released a draft list of tasks for each scenario (with the exception of the cyber attack). ODP asked for review of the tasks and whether they needed to be changed or augmented. The resulting scenario lists of tasks then would be combined into a single Universal Task List (UTL).

Tasks for each scenario were categorized in the major functional areas of 1) awareness, 2) preparedness, 3) prevention, 4) response, and 5) recovery. Under each major area, sub-areas were defined, such as command, control, coordination; planning and revision; and intelligence and surveillance with related tasks. For example, for the

anthrax scenario, shown in Figure 3, the functional area of preparedness had a sub-area of planning and revision, with a detailed task list for the sub-area.

Figure 3. Anthrax Scenario Sub-Areas



In August 2004, ODP (2004b) requested comments on a July 2004 Universal Task List draft resulting from the work in June. The UTL draft included every unique task identified from the analysis of tasks in individual scenario task lists. The UTL was an important step in the CBP process as it would be used to develop a Target Capabilities List (TCL) and related conditions and measures of performance. The manual accompanying the draft UTL stressed the value of the list in providing a common language and common reference for homeland security professionals at all government levels and in the private sector. It also echoed a theme of emphasis on emergency response and recovery, stating that the universal list "facilitates requirements analysis by providing a template and a list of possible tasks that serve as a starting point for assessing what is required to respond to an event" (p. 2). The manual stated that many documents

informed the task development process, such as the National Response Plan, the National Incident Management System, and the Emergency Management Accreditation Program Standard.

DHS's first UTL was organized by functional areas, including awareness, prevention, and response, familiar to first responder communities. However, the August 2004 draft UTL was organized in a much different manner. It used four levels of 1) national strategic tasks; 2) planning, coordination, and support tasks; 3) incident management tasks; and 4) incident prevention and response tasks. These categories reflected a level of responsibility and focus of action at an organizational level rather than function or operation:

- The document described first level national strategic tasks as those normally performed by federal departments and agencies, such as developing national strategic intelligence.
- The second level tasks generally related to the development of plans to prevent, respond to, and recover from significant events, coordination of efforts, and support for local responders, such as managing regional and state resources. According to the document, any government level could perform these tasks, but it was expected actors below the national level would be involved.
- The third level incident management tasks included resource management and support tasks, normally performed at the local level, such as coordinating urban search and rescue.
- The last level of incident prevention and response were tasks performed in prevention or response activities, including protection, mitigation, and recovery. These, according to the document, would be performed by large metropolitan areas, midsize, and small jurisdictions.

Each task was further defined by sub-tasks. For example, for the area "incident prevention and response," the task to conduct incident management has five sub-tasks, with some defined by one or two more levels of tasks. The document reiterated the selection of scenarios to define the UTL. ODP planned to update the scenarios for changes in the homeland security strategic environment (ODP 2004a; OSLGCP 2004a).

D. ISSUANCE OF THE DRAFT NATIONAL PREPAREDNESS GOAL

During the universal task list development, OSLGCP (2004a) issued a draft national preparedness goal for comment in September 2004. This included extensive directions for implementing the goal and using a capabilities-based planning framework.

The September 2004 goal (p. 6) was "Federal, State, local, and tribal entities will achieve and sustain a risk-based standard of national preparedness within 3 years (by September 30, 2008) that provides assurance of the Nation's capability to prevent, prepare for, respond to, and recover from major events, especially terrorism." Overall, the national preparedness goal, according to the document (p. 16), was to provide demonstrable national assurance that combined federal, state, local, and tribal capabilities are organized, manned, trained, equipped, well-led, and guided by sound policies, plans, and procedures.

The September 2004 national goal document described seven elements of preparedness for HSPD-8 implementation (p. 8), described in Table 3.

Table 3. Preparedness Elements

Element	Description
Guidance	Including strategies, plans, operating procedures, regulations, or policies that govern or guide national preparedness activities.
Organization	Including organizations needed to conduct a homeland security mission or task, as well as organizational characteristics.
Personnel	Encompassing qualified personnel supporting a homeland security capability, including identification of the knowledge, skills, abilities, and competencies needed to perform a homeland security task.
Training	Including training content and all methods of delivering that content to intended audiences, which enables performance and support of homeland security missions and tasks.
Equipment	Encompassing materiel, supplies, and facilities used to prepare for, directly perform, or support a homeland security mission.
Leadership	Providing management, responsibility, and accountability across the spectrum of national preparedness elements.
Linked Performance	Encompassing the ability of the other elements to successfully interact to standard to prevent, prepare for, respond to, and recover from domestic terrorist attacks, major disasters, and other emergencies.

In the same document, OSLGCP listed eight mission areas to represent all incident management operations (p. 9). The mission areas were the same as earlier draft mission areas and those used in the planning scenarios that scoped response

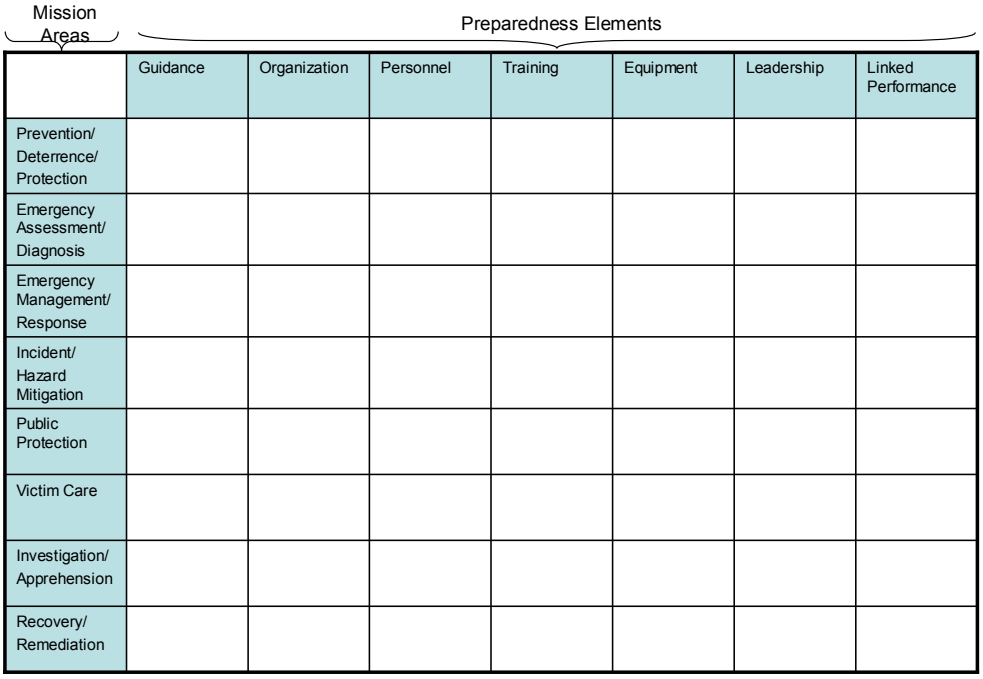
requirements. These, according to the document, represented assigned or shared homeland security missions and the categories to bundle capabilities for interconnected sets of tasks. The mission areas are shown in Table 4.

Table 4. Mission Areas

Mission Areas	Ability To
Prevention, Deterrence, Protection	Prevent, deter, or protect against terrorist attacks.
Emergency Assessment, Diagnosis	Detect an incident, determine its impact, classify the incident, conduct environmental monitoring, and make government-to-government notifications.
Emergency Management, Response	Direct, control, and coordinate a response; provide emergency public information to the population at risk and the population at large; and manage resources. This outcome includes direction and control through the Incident Command System, Emergency Operations Center, and Joint Information Center.
Incident, Hazard Mitigation	Control, collect, and contain an incident at its source and to mitigate the magnitude of its impact. Includes all response tasks conducted at the incident scene except those associated with victim care.
Public Protection	Provide initial warnings to the population at large and at risk, notify people to shelter-in-place or evacuate; provide evacuee support (e.g., transportation); protect schools and special populations; and manage traffic flow and access to the affected area.
Victim Care	Treat victims at the scene, transport patients, treat patients at a medical treatment facility, track patients, handle and track human remains, and provide tracking and security of patients' possessions and evidence.
Investigation, Apprehension	Investigate the cause and source of the attack; prevent secondary attacks; and identify, apprehend, and prosecute those responsible.
Recovery, Remediation	Ability to restore essential services, businesses and commerce, clean up the environment and render the affected area safe; compensate victims; provide long-term mental health and other services to victims and the public; and restore a sense of well-being in the community.

According to the draft September 2004 national preparedness goal document, each mission area would be assessed across these preparedness elements (e.g., guidance) for 1) a specific entity or group of entities (e.g., departments or agencies, jurisdictions, states, areas, sectors, regions) operating individually or together, 2) for a specific scenario; or 3) collectively for entities or multiple scenarios. The assessment would include a preparedness rating or scorecard for states, local jurisdictions, Indian tribes, and federal departments and agencies, in categories such as "capable," "mostly capable," and "partially capable." The document included a figure (Figure 3, p. 10) that represented the matrix to assess specific levels of preparedness for a mission area and preparedness element. The matrix is shown in Figure 4.

Figure 4. Preparedness Rating Scorecard



The document further emphasized that a capabilities-based planning framework would be used to build the capabilities required for achieving the national preparedness goal. The framework would include a Homeland Security Universal Task List (UTL) with associated conditions and task standards; a target capabilities list, organized by tier; performance measures; and national planning scenarios.

E. REVISED UTL AND PROTOTYPE CRITICAL TASKS

Based on comments on the August 2004 UTL draft, ODP revised the UTL to include every unique task identified from the analysis of tasks required to prevent and respond to the events in the scenarios. The revision still kept categories such as national strategic tasks and incident management tasks. In drafting the revised UTL, ODP partnered with the National Training Consortium (Center for Domestic Preparedness, Louisiana State University, Nevada Test Site, Texas A&M, and New Mexico Tech). The

Consortium convened focus groups with subject matter experts to identify a list of critical tasks for the Target Capabilities List (TCL) and related capabilities, conditions, and measures of performance.

According to DHS, the TCL was intended to define the capabilities to cope with diverse homeland security scenarios and to define conditions and measures of performance. Conditions were those environmental variables that affect task performance, such as weather or the number of casualties. Measures and performance criteria described a standard for how well a task must be performed and the basis for varying levels of acceptable task performance (ODP 2004b, OSLGCP 2004c). Homeland security agencies could use the performance criteria to assess their ability to perform tasks for which they were responsible (OSLGCP 2004a).

In October 2004, DHS conducted a capabilities workshop of primarily state and local officials to select critical capabilities by scenario and propose quantitative measures for each of the critical capabilities. At the meeting and in written information (OSLGCP 2004b), DHS stated that the CBP process for national preparedness would include ten detailed steps to answer preparedness questions:

1. Define the threats—what are we preparing for? The national planning scenarios define probable threats from terrorists, natural disasters, and other emergencies. While the scenarios do not include every possible threat, those having the capacity to respond to these scenarios should have the skills and flexibility to respond to any emergency.

2. Identify the tasks that need to be performed—what do we need to do to prevent or respond to the threat? The UTL defines what tasks need to be performed by federal, state, and local governments and the private sector to prevent, respond to, and recover from events defined by the scenarios as well as other strategy and planning documents. The first UTL version contains tasks to be performed primarily by public agencies. In 2005, ODP will work with stakeholders to expand the UTL for private sector, non-government organizations, and citizen groups.

3. Identify the critical tasks—what are the most important tasks? Critical tasks are those tasks that if not performed, will result in unsuccessfully preventing or responding to an event.

4. Define required capabilities—what capabilities do we need to perform the critical tasks? Capabilities are combinations of capability elements—personnel; planning;

organization and leadership; equipment; training; and exercises, evaluations, and corrective actions—providing the means to perform tasks under specified conditions and to national standards.

5. Determine level of capabilities required—What level of the capabilities do we need? Many of the tasks and capabilities are common across several or all of the scenarios, but stakeholders will need to set target capabilities' levels balancing need with an acceptable level of risk.

6. Assign responsibility for capabilities—Where should we, as a nation, place the required capabilities? This step involves an analysis of which capabilities should be developed and maintained at the local level, regionally within states, at the state level, at a multi-state regional level, or by the federal government. The analysis should include 1) the role of different levels of government for each capability and 2) the requirements for local jurisdictions of different sizes and risk levels, grouping jurisdictions into tiers to define tier capabilities.

7. Define capabilities requirements for jurisdictions/agencies—What capabilities should my jurisdiction or agency have? Tier capabilities will guide determinations of what each jurisdiction should have or have available through mutual aid. The TCL for the tiers defines the range of capabilities for which local jurisdictions may use federal grant funds. States and local jurisdictions would use federal funds only for those capabilities defined for their tier in the TCL.

8. Assess current capabilities against target capabilities—Do we have adequate capabilities? An assessment would contrast current capabilities against TCL requirements, determining gaps, deficiencies, and excess or overlaps.

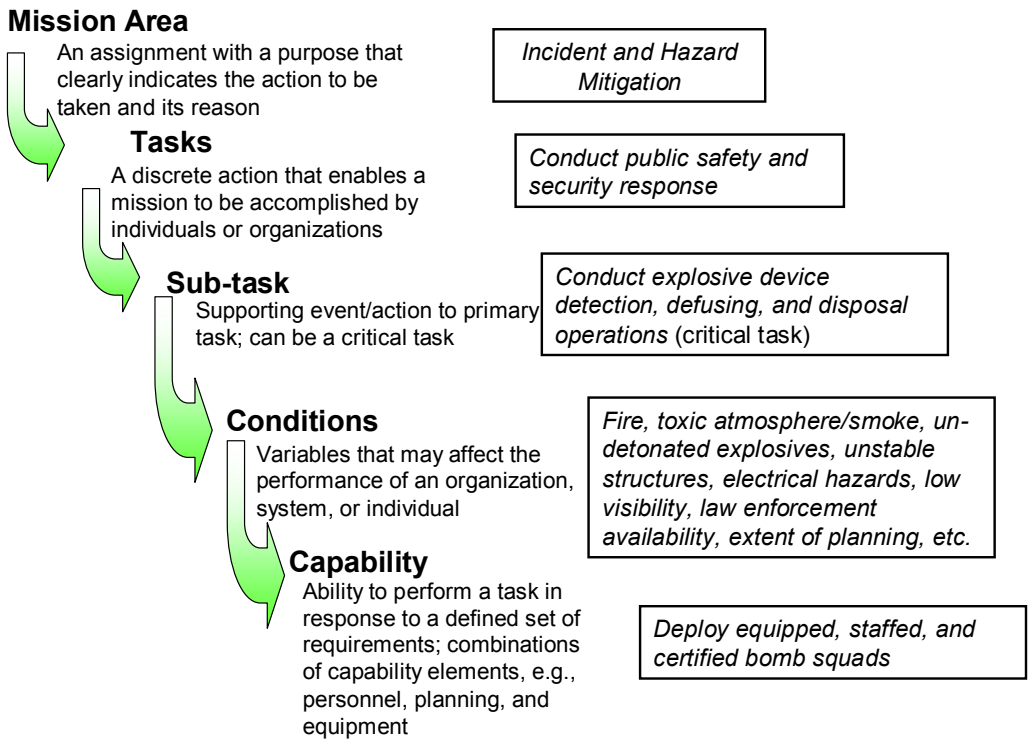
9. Allocate resources to address priority needs—How should we allocate our limited resources to make the most difference in preparedness? Cost estimates would be determined for required capabilities to address gaps and deficiencies.

10. Assess performance of tasks—How prepared are we? Performance measures for each task will provide uniform criteria to measure task performance. A preparedness scorecard will measure progress toward achieving specific preparedness objectives that support the national preparedness goal.

DHS (OSLGCP 2004b) also provided workshop participants with an improvised explosives device (IED) scenario prototype to illustrate the use of CBP. DHS estimated that approximately 1100 prevention and response tasks from the UTL would have to be performed for the IED scenario, with 71 considered critical. The critical tasks range across nine of the ten mission areas identified in the National Preparedness Goal. The prototype used tasks for the mission area of incident and hazard mitigation to explain the

CBP process. Drawing on the prototype information, Figure 5 illustrates the "waterfall" from this mission area to capabilities.

Figure 5. DHS Explosives Scenario Waterfall Example



F. STAKEHOLDER CONCERNS

The October 2004 workshop participants overwhelmingly supported a national preparedness goal and standards, but many voiced major concerns with the CBP process and DHS progress to date (Caudle 2004; NEMA 2004; ASTHO 2004). Their concerns emphasized proceeding with what one called a fatally flawed process following artificially-imposed timeframes to produce an invalid UTL. Many participants characterized the UTL and capabilities lists as producing an untenable standard of care that could be considered in civil litigation cases.

Participants presented four major arguments highlighting significant flaws in the CBP process:

- Lack of clarity about the expected outcome and rationale for the national preparedness goal's selection of CBP as its planning framework and confusion about how CBP worked, particularly to define national level capabilities and thus later federal funding criteria for state and local entities. Many believed the result would be an UTL planning framework and task list too large and too complex for realistic field use.
- Anticipating that the entire nation—all jurisdictions—would contribute to the prevention, protection, and response and recovery for a large-scale event, with a heavy focus on terrorist attack scenarios that most jurisdictions likely would never encounter. This "national response view" created an extremely detailed "one size fits all" national standard requirement for every jurisdiction. The argument was that a sustained capacity may be needed in certain jurisdictions, but not every locality and state should be prepared for a large scale event. Most jurisdictions, it was believed, could anticipate smaller-scale events, such as the use of explosive devices or natural hazards such as a flood, hurricane, or earthquake.
- Ignoring 1) lessons learned from previous disasters, 2) already existing comprehensive assessments, plans, systems, and capabilities for preparedness at the state and local level, often in response to requirements imposed by DHS and other federal agencies, such as the Department of Health and Human Services, and 3) national management standards and related certification programs for emergency preparedness, such as the Emergency Management Accreditation Program based on a national management system standard, and the requirements of the National Response Plan and the National Incident Management System.
- Failing to address what resources would be needed for timeframes before, during, and after an event. The approach also ignores realities such as trends in surge preparedness or the inability to fund a surge capacity with current shortages or hold and resource capacity in anticipation of an event that would likely never happen.

In November 2004, OSLGCP (2004c) responded to participants and reiterated the commitment to the rigorous timeline, justified the use of CBP, and emphasized the need for a coordinated national approach to enhance preparedness. The rational was that threats and hazards faced were national in scope, and thus there should be a national preparedness perspective. OSLGCP said that state and local jurisdictions were not expected to plan for and exercise all tasks in the UTL, but should only select tasks that

apply to their roles in specific homeland security missions for their level of government. However, local decision-making should be done within a national context of building and maintaining capabilities necessary for prevention, response, and recovery from large-scale and smaller all-hazards incidents.

G. MOVING TO ISSUANCE OF THE 2005 NATIONAL PREPAREDNESS GOAL

In early December 2004, Gruber (2004a, 2004b) reported that a small group of state and local officials were working to streamline the task lists and capabilities templates. He described HSPD-8 implementation as a transformation in building a true national preparedness capability. It would, he said, provide the ability to measure task performance and the adequacy and sufficiency of capabilities against key risk scenarios. In the end, it should achieve an objective assurance of national performance and a rational method to allocate limited resources. The Administration's view was that there should be a national, objective assurance of readiness and he believed that CBP was the right approach to achieve that goal.

However, he also recognized the difficulty of the implementation process. In contrast to the DoD experience, he said DHS implementation of CBP must rely on a consensual community that would adopt the approach. He recognized that a consensual approach is difficult with federalism concerns and the sovereignty of many stakeholders, such as states. He stated that DHS should have spent more time in explaining the rationale for CBP adoption instead of devoting almost all its time to designing a CBP process for homeland security.

The assurance of readiness is now presented as a cornerstone of federal homeland security grants. ODP's (2004f) fiscal year 2005 Homeland Security Grant Program guidelines state that statewide all-hazards preparedness strategies are to be consistent with HSPD-8's national preparedness goal. During 2005, states are to review and incorporate the national planning scenarios, the UTL, and the TCL in their preparedness efforts, anticipating full implementation of HSPD-8 in 2006. The guidelines also state that the TCL will include tiers for capability level differences among entities based on factors such as population density, critical infrastructure, and other risk factors.

In mid-December, DHS (OSLGCP 2004d) requested comments on a new draft list of capabilities that would be used for the TCL. The capability categories included 1) prevention/intelligence, 2) agriculture and food, 3) incident management, 4) incident response, 5) public protection, 6) criminal investigation, 7) mass care, 8) public health and medical care, 8) public information, and 9) recovery. By March 31, 2005, ODP planned on issuing a National Planning Guidance describing the national preparedness goal, the capability target levels, and how entities were to apply them in developing and updating preparedness assessments and strategies. For fiscal year 2005, grantees were to use homeland security grant funding to develop capabilities to prevent, detect, interdict, and respond to improvised explosive devices. The use of the improvised devices was considered to have a high probability of being used in a terrorist attack and was the CBP prototype. It also might be interpreted as normalizing basic preparedness expectations. In other words, capabilities for improvised explosive devices established a baseline level of preparedness across the nation.

In December 2004, DHS also issued a new version of the UTL that further defined the tasks and added more specifications, such as expanding intelligence and surveillance tasks as part of preventative efforts. This version maintained the four levels that defined the types of tasks to be performed. The draft August and December 2004 UTL categories are very similar. In April 2005, DHS issued another draft UTL version (OSLGCP 2005b). However, the April 2005 version is a considerable departure from the two earlier versions and is now organized by mission areas and not level of responsibility.

Table 5 contrasts the primary task categories for the December 2004 and April 2005 UTL versions. Each major category also has lower level tasks or objectives with one or more levels. For example, the task category "manage national preparedness activities" has eight sub-task categories, such as "provide for the protection of national infrastructure." These sub-tasks have further categories, such as "develop and implement strategy and policies for secure cyberspace," with another level, such as "promote a comprehensive national cyberspace defense awareness program."

The April 2005 UTL contains approximately 1,800 tasks, still covering the national strategic to the local incident level. Thus, the UTL is very detailed with list upon list of universal tasks. Consistent with DHS statements, the UTL does not state how a task is to be performed. DHS plans to add tasks for the private sector and the public at a later date.

Table 5. Draft UTL Comparisons

December 2004 UTL	April 2005 UTL (Summaries of Objectives)
National Strategic: Primarily federal departments and agencies.	***Common Tasks***
• Develop national strategic intelligence and surveillance • Manage national preparedness activities • Conduct national prevention operations • Provide for command and management of incidents of national significance • Provide national incident support • Manage national resources • Provide national communications and information management support • Support national technologies	• Preparedness: Build, sustain, and improve the operational capability to prevent, protect against, respond to, and recover from domestic incidents • Resource management: Coordinate and oversee tools, processes, and systems that provide incident managers with timely and appropriate resources during an incident • Communications and information management: Identify the requirements for a standardized framework for communications, information management, and information sharing support at all levels of incident management • Supporting technology: Provide supporting technology and technology systems essential to implement incident response actions
Planning, Coordination, and Support: Primarily single states or groups of states, regions within states or counties, federal regions.	***Prevent Mission***
• Conduct regional, State and local intelligence and surveillance operations • Conduct regional, State and local preparedness activities • Conduct regional, State and local preparedness operations • Command and manage incidents • Provide regional and State incident support • Manage regional, tribal and State resources • Provide regional and State communications and information management support	• Detect threats: Identify, assess, investigate and communicate terrorist activities, intentions, and capabilities in order to preempt and prevent attacks • Control access: Conduct security functions to prevent entry to the United States and/or access to targets within the United States of terrorists and the instruments of terror • Eliminate threats: Eradicate terrorist threats using all the tools in out Nation's arsenal to stop those who wish to do us harm
Incident Management Mayor, city manager, county executive, or emergency operations center.	***Protect Mission***
• Coordinate transportation operations • Operate/manage telecommunications and information technology • Manage/direct building department, public works and engineering • Coordinate firefighting operations • Coordinate incident management operations • Coordinate mass care, housing, and human services • Coordinate resource support • Coordinate public health and medical services • Coordinate urban search and rescue • Coordinate oil and hazardous materials response • Coordinate agriculture and natural resource response and recovery • Coordinate energy recovery • Coordinate public safety and security • Coordinate community recovery, mitigation, and economic stabilization	• Assess critical infrastructure and key assets: Identify critical infrastructure, key resources, and other assets, assess potential consequence if they were destroyed or disrupted, assess potential vulnerabilities, prioritizing assets, and develop information sharing mechanisms to ensure flow of information between the public and private sector stakeholders • Protect critical infrastructure and key assets: Protect critical infrastructures and key assets that face a specific, imminent threat • Mitigate risk: Take strategic actions to raise security levels appropriate to each asset's vulnerability and criticality

December 2004 UTL	April 2005 UTL (Summaries of Objectives)
• Coordinate emergency public information and external communications	
Incident Prevention and Response: Incident site personnel.	***Respond Mission***
• Provide transportation • Operate telecommunications and information technology • Conduct public works and engineering • Conduct firefighting • Conduct incident management • Provide mass care, housing, and human services • Provide resource support • Provide public health and medical services • Conduct urban search and rescue • Conduct oil and hazardous materials response • Support agriculture and natural resource recovery • Support energy recovery • Provide public safety and security • Support community recovery, mitigation, and economic stabilization • Provide emergency public information and external communications • Provide transportation • Operate telecommunications and information technology • Conduct building department, public works and engineering • Conduct firefighting • Conduct incident management • Provide mass care, housing, and human services • Provide resource support • Provide public health and medical services • Conduct urban search and rescue • Conduct oil and hazardous materials response • Support agriculture and natural resource recovery • Support energy recovery • Provide public safety and security • Support community recovery, mitigation, and economic stabilization • Provide emergency public information and external communications	• Assess incident: Determine the nature of the incident, investigate the cause of the incident, assess the situation, identify critical and unmet needs, provide recommendations for protective actions, and identify and coordinate acquisition and delivery of required assets and/or resources • Minimize impact: Implement and coordinate immediate actions to contain the direct effects of an incident • Care for public: Implement immediate actions to save lives and meet basic human needs to minimize the impact of an incident and prevent further inquiry ***Recover Mission*** • Assist public: Help individuals directly impacted by an incident to return to pre-incident levels, where feasible. • Restore environment: Reestablish or bring back to a state of environmental or ecological health the water, air, and land and the interrelationship, which exists among and between water, air, and land and all living things • Restore infrastructure: Restore infrastructure in affected communities in order to return to pre-incident levels, where feasible

On March 31, 2005, DHS issued the Interim National Preparedness Goal (OSLGCP 2005a). However, the goal did not set an explicit national preparedness goal as it did in the September 2004 draft goal. Instead, the interim goal established a "national vision" and priorities as steps toward setting measurable readiness benchmarks and targets. The national vision is "to engage Federal, State, local, and tribal entities, their private and non-governmental partners, and the general public to achieve and sustain risk-based target levels of capability to prevent, protect against, respond to, and recover from major events in order to minimize the impact on lives, property, and the economy" (p. 3). The new document presented several national readiness priorities intended to establish the most urgent needs for national preparedness, and include (p. 10):

- Implement the National Incident Management System and National Response Plan,
- Expanded regional collaboration,
- Implement the Interim National Infrastructure Protection Plan,
- Strengthen information sharing and collaboration capabilities,
- Strengthen interoperable communications capabilities,
- Strengthen chemical, biological, radiological, nuclear, and explosive detection, response, and decontamination capabilities, and
- Strengthen medical surge and mass prophylaxis capabilities.

HSPD-8 calls for the establishment of national priorities. However, it called for establishing measurable readiness priorities and targets that balance the threat and magnitude of terrorist attacks, major disasters, and other emergencies with the required resources. Emphasis on the national priorities presented above appears to be an awkward fit within the entire capabilities-based planning approach. For example, the overarching priorities include implementing the National Incident Management System, National Response Plan, and Interim National Infrastructure Protection Plan. This approach appears counter to developing capabilities to meet the target capabilities list and addressing the national planning scenarios. The guidance provides limited justification for pursuing the national priorities in addition to a more systematic capability-based planning approach for the planning scenarios.

The document recounted DHS efforts to develop readiness targets, priorities, standards for preparedness assessments and strategies, and a system for assessing national preparedness. These efforts included using 1) CBP to define risk-based target levels of capability for readiness targets, 2) national priorities to guide preparedness efforts, and 3) other elements such as standards for preparedness assessments. It also reiterated the justification for using the national planning scenarios and the TCL in defining preparedness. The document emphasized that not every entity would be expected to develop and maintain every capability to the same level, recognizing that risk and the needs of different entities would require variations.

The most recent version of the TCL (OSLGCP 2005c) recommends 36 capabilities to be developed and maintained, in whole or in part, by government organizations anticipating terrorist attacks and major disasters. The complete list is shown in Table 6.

Table 6. Target Capabilities

Categories	Target Capabilities	
Common	• Planning	• Interoperable Communications
Prevent Mission Area	• Information Collection and Threat Recognition • Intelligence Fusion and Analysis • Information Sharing and Collaboration	• Terrorism Investigation and Apprehension • CBRNE Detection
Protect Mission Area	• Risk Analysis • Critical Infrastructure Protection • Food and Agriculture Safety and Defense	• Public Health Epidemiological Investigation and Laboratory Testing • Citizen Preparedness and Participation
Respond Mission Area	• On-Site Incident Management • Emergency Operations Center Management • Critical Resource Logistics and Distribution • Volunteer Management and Donations • Worker Health and Safety • Public Safety and Security Response • Firefighting Operations/Support • WMD/Hazardous Incident Response Decontamination • Explosive Device Response Operations • Animal Health Emergency Support • Environmental Health and Vector Control	• Citizen Protection: Evacuation and/or In-Place Protection • Isolation and Quarantine • Search and Rescue • Emergency Public Information and Warning • Triage and Pre-Hospital Treatment • Medical Surge • Medical Supplies Management and Distribution • Mass prophylaxis • Mass Care (Sheltering, Feeding, and Related Services) • Fatality Management
Recover Mission Area	• Structural Damage Assessment and Mitigation • Restoration of Lifelines	• Economic and Community Recovery

Each capability is comprised of critical tasks and specific performance standards, depending on conditions. The elements of capability defined in the document (p. 8) are described in Table 7. These elements are similar to the preparedness elements OSLGCP (2004a) described in September 2004, but are now descriptions of elements to achieve missions and tasks. For example, the previous "guidance" element described items such as strategies and plans, but the "planning" element emphasized policies, plans, and the like that are necessary to achieving mission and tasks.

Table 7. Elements of Capability

Element	Description
Personnel	Paid and volunteer staff who meet relevant qualification and certification standards necessary to perform assigned missions and tasks.
Planning	Collection and analysis of intelligence and information, and development of policies, plans, procedures, mutual aid agreements, strategies, and other publications that comply with relevant laws, regulations, and guidance necessary to perform assigned missions and tasks.
Organization and Leadership	Individual teams, an overall organizational structure, and leadership at each level in the structure that comply with relevant laws, regulations, and guidance necessary to perform assigned missions and tasks.
Equipment and Systems	Major items of equipment, supplies, facilities, and systems that comply with relevant standards necessary to perform assigned missions and tasks.
Training	Content and methods of delivery that comply with relevant training standards necessary to perform assigned missions and tasks.
Exercises, Evaluations, and Corrective Actions	Exercises, self-assessments, peer-assessments, outside review, compliance monitoring, and actual major events that provide opportunities to demonstrate, evaluate, and improve the combined capability and interoperability of the other elements to perform assigned missions and tasks to standards necessary to achieve successful outcomes.

According to OSLGCP (2005a), still to come are identifying the level of capabilities various types of jurisdictions should have for national preparedness. For Fiscal Year 2006, the focus is on performance improvement for seven national priorities, with states and urban areas required to update their homeland security preparedness strategies for the seven national priorities. For Fiscal Year 2007, critical risk-based priorities within the set of the 36 capabilities defined in the Target Capabilities List (OSLGCP 2005a, p. iv). The final Goal and new Target Capabilities List are to be issued on October 1, 2005, and will include 1) readiness targets, priorities, standards for preparedness assessments and strategies, and a system for assessing the nation's overall level of preparedness. The TCL will define levels of capability to address the impact for all scenarios. As part of that process, DHS will 1) define specific responsibilities to develop and maintain capabilities among levels of government and 2) apportion responsibility among groups of jurisdictions, or tiers, with different target levels of capabilities based on differences in risk factors such as total population, population density, and critical infrastructure.

Finally, at the end of April 2005, DHS issued the National Preparedness Guidance (OSLGCP 2005d). The concise document stated its purpose as providing instructions and guidance on how to implement the Interim National Preparedness Goal. It

summarized progress to date, including development of the Goal, use of capabilities-based planning, use of the national planning scenarios, development of the universal task list and target capabilities list, and explained the national priorities, and set out a timeline for HSPD-8 implementation. Scenarios were to be tailored to local conditions, with jurisdictions to identify other possible threats and hazards. The guidance called for state working groups to develop a prioritized list of capabilities—specific to that state—and a risk determination for addressing the national priorities. Expanded regional collaboration was to build national capabilities for major events. Much of its focus is implementing the seven national priorities, with the targeting of capabilities to these priorities.

This chapter's description of DHS CBP implementation highlights both progress and difficulties encountered over the many months. The model for the homeland security national preparedness goal and related capabilities is the Department of Defense's CBP approach. The next chapter describes the defense community's approach and the components considered important for effective CBP implementation, followed by a comparison of the DHS approach and that of the defense community. The comparison presents opportunities for improving the homeland security implementation of CBP.

V. DEFENSE COMMUNITY: CAPABILITIES-BASED PLANNING

A. DEFENSE COMMUNITY CBP PROCESS

The DoD CBP model used by DHS reflects allies' adoption of CBP. All member nations of the defense community's Technical Cooperation Program (TCP)—Australia, Canada, New Zealand, United Kingdom, and United States—are using the concept of capability as the basis for the long-term planning of future defense force structures (The Technical Cooperation Program 2004). This chapter describes the defense community's CBP process and components important for effective CBP implementation.

Drawing on several sources (Kendall 2002; Pogue and Vallerand 2003; Kiefer 2004a, 2004c; The Technical Cooperation Program 2004), CBP for the defense community can be defined as

> a competitive approach to create the right blend of plans, people, equipment, and activity—capabilities—with distinct asymmetric abilities useful across a broad spectrum of potential challenges and circumstances in different theaters against diverse foes while addressing uncertainty, risk, and resource choices.

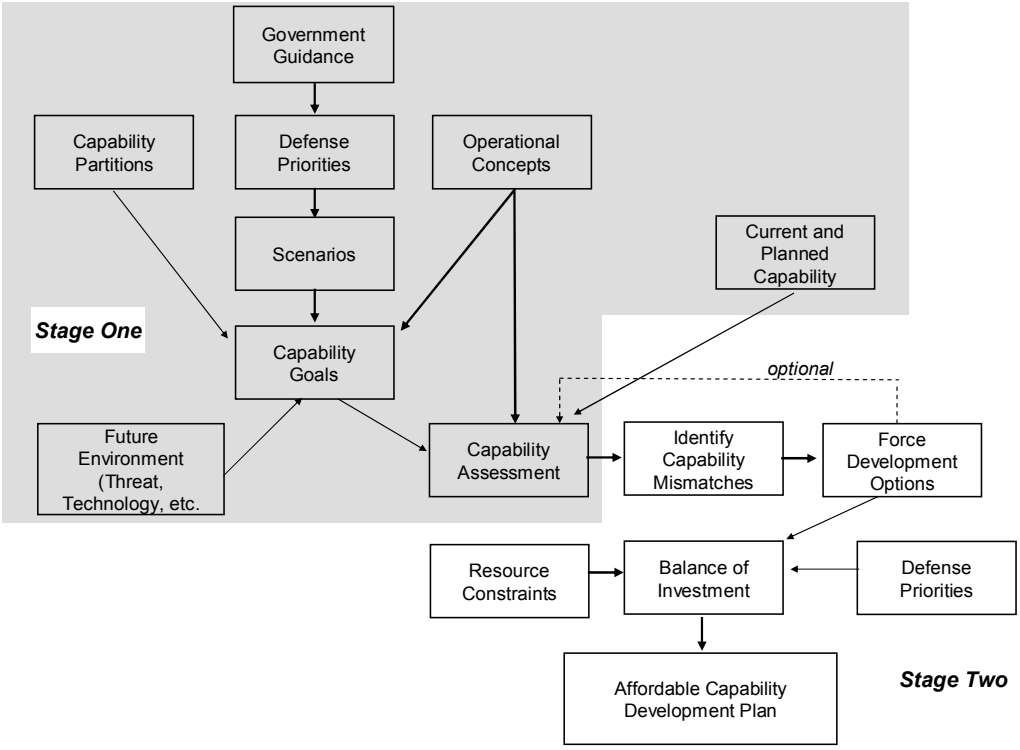
The central audience for CBP is the "combatant commander" who must achieve specific missions. Accordingly, several key CBP elements are identified to meet the commander's needs. These elements are all integral to a mission capability package, described by Kiefer (2004a) as a mission statement consisting of a purpose (objectives, effects, end-state) and associated tasks linked to candidate resources. He (2004a, 2004c) writes that central CBP elements include:

- Capabilities. A capability is the ability to achieve an effect to a standard under specified conditions through multiple combinations of means and ways to perform a set of tasks.
- Tasks that make up each capability. A task is an action or activity derived from mission analysis, doctrine, standard procedures, or concepts that may be assigned to an individual or organization.
- Concepts of operations (CONOPS). CONOPS is the overall picture and broad flow of tasks within a plan by which a commander maps capabilities to effects, and effects to an end-state for a specific scenario.

- Mission. The mission is the purpose (objectives and end-state) and tasks assigned to a commander.
- Capability effects achieving a desired end-state. A capability effect is a change to a condition, behavior, or degree of freedom. An end-state is the set of conditions, behaviors, and freedoms that defines achievement of the commander's mission.
- Measures. A measure is the quantitative or qualitative basis for describing the quality of task performance.

CBP is characterized by a straightforward decision-making process. The Technical Cooperation Program (2004, p. 4) describes a generic process chart of CBP, shown in Figure 6, with similar elements and concepts seen in the Davis (2002) approach described earlier. Under this process, CBP starts with overarching guidance, identifies capability gaps, explores options, and ends with an affordable investment plan.

Figure 6. Generic CBP Process Chart



Stage one in the process determines, as Taylor (2004) describes, "where are we?" The second stage determines what is to be done to address capability needs. Taylor and The Technical Cooperation Program (2004) describe inputs to CBP as five major components. These are 1) objectives that are the top-level strategic guidance that sets clear priorities, objectives to be associated with different scenarios, and planning assumptions, 2) context which is future allied and adversary capabilities, endorsed scenarios, and agreed upon operational concepts, 3) constraints such as cash flow, scheduling, and balancing capabilities, 4) a framework to collect input information for capability development and a capability partition scheme, and 5) force characteristics of current and planned force elements, including lessons learned.

B. IMPLEMENTATION COMPONENTS

Drawing on these sources and other defense community CBP literature and presentations, the following sections present several components important for effective CBP implementation. These are summarized in Table 8.

Table 8. Components for Defense CBP Implementation

Components	Description
Business Case for CBP Adoption	Justify organizational commitment and investment
Strategic, Cascading Policy Goals	Use top-level government guidance that cascade goals into strategic policy and operational documents and into CBP.
Stakeholder Ownership	Ensure stakeholder involvement, collaboration, and perspective-sharing.
Top Leader Ownership	Ensure top leader support, involvement, and decision-making.
Specific Management Decision-Making Process	Design and implement CBP decision process that captures mission tasks and capabilities, their priority, how they relate, and solutions.
Risk Assessment Approach	Use risk assessment in the CBP management process to determine investments.
Different Planning Horizons	Incorporate different planning horizons into CBP to stage the development of capabilities.
Mission-Based, Phased Scenarios	Have the right scenarios on which to base planning and/or exercises.
Capability Development and Standard Categories	Provide guidelines to craft capabilities and develop standard capability categories that fully reflect what effects the capabilities should generate.
Decision Rules for Lists	Establish clear rules for the development of task lists and capability lists.
CBP Evolution	Evolve CBP depending on planning applications and developing maturity.
CBP Enablers	Consider organizational and cultural enablers to support CBP adoption.

1. Business Case for CBP Adoption

As with any new approach, CBP adoption requires a strong business case to justify the organizational commitment and investment. This is especially important given the transformational impact of CBP on organizational decision-making and the complexity of the approach. In the defense communities, the strong business case for CBP adoption grew primarily out of the need to shift defense planning from a "threat-based" model to a "capabilities-based" model (Department of Defense 2001). Instead of planning for large conventional wars in a few distant theaters under the threat-based model, the 2001 Quadrennial Defense Review proposed identifying capabilities to deter and defeat adversaries that relied on surprise, deception, and asymmetric warfare (Department of Defense 2001).

According to Schilling (2004), DoD has used threat-based planning since DoD instituted the Planning, Programming, and Budgeting System (PPBS) in 1962. However, threat-based planning meant strong response to a few situations while largely ignoring all other potential challenges. The result is that defense forces were created that may be limited in responding to changing conditions. According to Davis (2003), DoD's threat-based approach and illustrative official planning scenarios for major theater wars served as specifications, defining necessary and sufficient characteristics of the force structure, thereby leading to consistent support of current programs. The approach only considered conventional-wisdom threats and point-in-time versions of detailed scenarios, as though the circumstances of future conflict could be predicted.

In the foreword to the Joint Operations Concepts (Department of Defense 2003), Secretary Rumsfeld said a capabilities-based approach would focus more on how the United States would defeat an adversary's broad array of capabilities instead of identifying who the adversaries were and where they might threaten joint forces or United States' interest. According to Davis (2003), capabilities-based planning generates capabilities usable for different purposes and circumstances. For each name-level scenario (for example, China invades a unified Korea), planners should evaluate capabilities for broad range of operational circumstances that would stress capabilities in

very different ways. Dimensions might include political-military scenario details, objectives, strategies, tactics, forces, force effectiveness, environment, and other modeling assumptions.

While addressing the limitations of threat-based planning was the primary business case for DoD's adoption of CBP, other reasons existed. For example, The Technical Cooperation Program (2004) said that CBP was developed as an attempt to break down traditional single-service stovepipes so that systems and concepts from multiple services could be used to achieve capabilities. A joint focus encourages decision-makers to make capability decisions with broad defense force goals in mind instead of considering their own service. CBP provides the means to compare different options for achieving the same capability and to do so in an integrated fashion. Joint Staff/J-7 (2004), describing DoD's previous requirements and acquisition process, said requirements often were developed, validated, and approved as stand-alone solutions to counter specific threats or scenarios, not as part of a system of elements. As a result, systems integration was forced at the end of the process; duplication existed, particularly in smaller programs; spiral acquisition practices were not well institutionalized; and joint warfighting needs were not prioritized. CBP, according to Taylor (2004), also links procurement decisions to strategic goals and provides an audit trail for accountability.

More subtly, Kendall (2002) argues that the defense drawdown in the 1990s forced military services to develop capabilities intended to protect each service's institutional functions and infrastructure while trying to structure the force. In other words, attempts to protect force size drove threat-based planning. CBP removes some of the "cover" for protecting force size by focusing on mission needs and effects, and competition among overall capability options.

2. Strategic, Cascading Policy Goals

While the business case provides the rationale and incentive for change in the strategic thrust of an organization, another component is establishing specific strategic policy goals. What is needed for CBP, according to The Technical Cooperation Program (2004), are high-level capability objectives derived from top-level government guidance. These policy goals support the use of top-level doctrine or some overarching operational

concepts that consider the way a force will fight. Moreover, these goals cascade into strategic policy and operational documents, and then into the CBP process and its planning outputs.

For example, according to the Canada Department of National Defence (2002a), the foundation for Canada's CBP was an early White Paper that defined governmental expectations, leading to a Strategy 2020 document that articulated the national defense vision. In turn, the Canadian Forces concept of force employment was crafted to describe how the national defense vision would be delivered. Force planning scenarios illustrated where and when the concept of employment would be applied, finally leading to Canada's capability goals matrix and Canada Joint Task List (CJTL) for CBP. In the United Kingdom, according to the United Kingdom Ministry of Defence (2004), a defense white paper also set out the need to defend against future principal security challenges such as international terrorism, weapons of mass destruction (WMD) proliferation, and weak and failing states. The Australia Department of Defence (2000) also relied on a white paper on the future of Australia's defense force.

A similar process occurred in DoD in planning for joint processes and in individual services. DoD (2001) built its strategic framework to defend the nation and secure a viable peace around four defense policy goals—assuring allies and friends, dissuading future military competition, deterring threats and coercion against US interests, and if deterrence failed, decisively defeating any adversary. These strategic policy goals are further defined in other documents. For example, within DoD joint force decisionmaking, according to Joint Staff/J-7 (2004) and Kiefer (2004a), concepts (Joint Operations Concepts, Joint Operating Concepts, Joint Functional Concepts, and Joint Integrating Concepts) are translated into a capability level of detail, often using a time frame of 10 to 20 years into the future. Military judgment is applied to those concepts to validate what collection of attributes and measures are needed, and thus a standard for critical functional areas. Current programs are mapped against that standard to compare current capabilities against the standard, propose alternatives, choose a specific capability, and then move that decision into the investment strategy.

3. Stakeholder Ownership

A third component is ensuring stakeholder ownership, especially important for joint planning and operations. The Technical Cooperation Program (2004) says that one of the first requirements for successful implementation of CBP is stakeholder involvement, described in collaborative terms. Stakeholders generally control the information, resources, and authority required to support CBP, and their requirements must be considered from the outset. Key stakeholders—those responsible for identifying and deploying the capability envelopes—will eventually control the CBP process, and it is important that they have ownership of it. Each stakeholder should have an understanding of the perspectives of other stakeholders and an appreciation of different, if not competing, requirements. For example, Taylor (2004) notes that CBP success requires engaging defense planners at all levels.

As with other components, the decision-making process can help build in stakeholder ownership. For example, the United States Air Force uses its decision process to secure "joint acceptance" of capability selections.

4. Top Leader Ownership

Another component is top leader support, involvement, and decision-making—ownership—for the CBP process. According to Kiefer (2004a), DoD's Joint Integrating Concepts (Joint Concepts) are delivered with a detailed scenario, concept of operations (CONOPS), and a list of tasks with measures for a Functional Capabilities Board (Board) to a perform capabilities based assessment on each Joint Concept and perform a data call to services to match Joint Concept tasks to current, programmed, and planned systems.

According to Joint Staff/J-7 (2004), each Board is a key decision-making body. Only the high-level Joint Requirements Operation Council can charter a Board. The Boards ensure new capabilities are conceived and developed in a joint warfighting context and proposals are consistent with an integrated joint force. They also organize, analyze, and prioritize capabilities proposals, oversee the development and updating of functional concepts, and ensure integrated architectures reflect the functional areas. Each Board assesses the Joint Concept against the baseline scenario provided by the author, and then may run it against additional Defense planning scenarios to refine the conditions

and standards for each task and aggregate capability. The CBP output is a weighted list of capability needs, gaps, and excesses.

According to Feaga (2004), in 2000, the United States Air Force (USAF) began developing six CONOPs to support its contribution to the joint defense strategy. All USAF operations, programming, and budget decisions in turn are designed to support the capabilities defined by the CONOPs. Six new CONOPS divisions on the USAF Air Staff in the Operations Requirements Directorate were created to connect CBP around these CONOPS. Each of the USAF's six CONOPS has an assigned advocate called a Champion responsible for the capabilities the USAF has, or needs to develop. The CONOPS Champions play a key role in mitigating risk throughout CONOPS development. They are charged with overseeing the entire development process and for communicating issues to senior leadership. CONOPS assessment and analysis is conducted by subject matter experts under the critical jurisdiction of each Champion. CONOPS Champions will integrate priorities among capabilities for review by the USAF corporate structure and participate in the Joint Requirements Oversight Council via USAF challenges. Oversight action and challenges ensure all CONOPS capabilities are addressed at the Boards to help ensure all programs are jointly accepted.

5. Specific Management Decision-Making Process

Another component is a well-designed and implemented decision process for CBP. This process should capture tasks and capabilities needed to carry out missions and their priority, how they relate, solutions to meet those needs, and allocation of resources. For example, according to the Joint Chiefs of Staff (2004a), the Joint Capabilities Integration and Development System (JCIDS), the Defense Acquisition System, and the Planning, Programming, Budgeting, and Execution process form DoD's three principle decision support processes to transform the military forces to support the National Military Strategy and the Defense Strategy. According to Joint Staff/J-7 (2004) and the Joint Chiefs of Staff (2004b), the JCIDS provides an enhanced methodology to identify and describe gaps and redundancies in capabilities, prioritize capability proposals, and improve collaboration with other departments and agencies. The goal is to ensure that

the joint force has the capabilities necessary to perform across the range of military operations.

JCIDS analysis begins with a Functional Area Analysis that identifies the operational tasks, conditions, and standards needed to achieve military objectives. As input, it uses the national strategies, Joint Operating Concepts, Joint Functional Concepts, Joint Integrating Concepts, Integrated Architectures, the Universal Joint Task List, and the anticipated range of broad capabilities that adversaries might employ. Output consists of the tasks to be reviewed in the follow-on Functional Needs Analysis that assesses the ability of the current and programmed joint capabilities to accomplish the tasks that the functional area analysis identified, under the full range of operating conditions and in compliance with designated standards. The needs analysis produces a list of capability gaps or shortcomings that require solutions and indicates the time frame in which those solutions are needed. A Functional Solution Analysis follows, which is an operationally-based assessment of potential approaches to solving (or mitigating) one or more of the capability gaps (needs) identified in the Functional Needs Analysis.

A capabilities review and risk assessment (CRRA) step following a functional needs analysis is the most important step for the Air Force, according to Feaga (2004). In the CRRA, capability measures are developed from a variety of analysis tools such as current intelligence estimates, modeling and simulation, and wargaming. Measures of effectiveness are assigned to all levels of required capabilities within a master capabilities list to score how well the USAF performs. Scenarios are selected to assess the USAF's ability to deliver effects needed. Scenarios from the Defense planning scenarios are used and further refined by guidelines in the National Security Strategy and the National Military Strategy. The scenarios also are modified by more demanding requirements known as stressors to craft broad spectrum capabilities. Analysis determines a definition of problems and capability shortfalls, presented to USAF senior leadership for decision-making and resource allocation.

6. Risk Assessment Approach

A sixth component is using risk assessment in the CBP management process. A key tenet of CBP is addressing affordability and sustainability, which means that not all

capabilities can be deployed or maintained. Affordability and sustainability requires addressing risk tolerances and priorities for capability development and deployment, and assessing capabilities and their impacts over time. Taylor (2004) writes that balancing investments in CBP will require deletions and additions in elements such as force development as part of risk and priority setting.

For example, the Department of Defense (2001) developed a broad approach to risk management intended to ensure the defense establishment is sized, shaped, postured, committed, and managed to accomplish defense policy goals. Managing risk means changes in operating practices and military and civilian personnel systems, business practices, and infrastructure. These dimensions reflect DoD's experiences over the last decade in attempting to balance strategy, force structure, and resources. The risk management framework gives DoD the ability to consider capability tradeoffs among fundamental objectives and fundamental resources constraints.

The framework is made of four related dimensions: force management, operational, future challenges, and institutional. Force management is the ability to recruit, retain, train, and equip sufficient numbers of quality personnel and sustain the readiness of the force while accomplishing operational tasks. Operational is the ability to achieve military objectives in a near-term conflict or other contingency, with risk management considering not just additional force structure, but also assessing changes in capabilities, concepts of operations, and organizational designs to help reduce risk. A future challenge is the ability to invest in new capabilities and develop new operational concepts needed to dissuade or defeat mid-to long-term military challenges. The last dimension is institutional, the ability to develop management practices and controls that use resources efficiently and promote the effective operation of the defense establishment.

Periodic assessment of existing and planned capabilities is part of ongoing risk assessment. The Technical Cooperation Program (2004) notes some nations that are practicing CBP will assess capabilities three or four times over an approximate 15-year period. For example, the Canada Department of National Defence (2002a, p. 22) uses a capability goals matrix to rank capabilities. There are four levels in the Canadian

matrix—military strategic, operational, and tactical, with the operational level divided to identify goals in the domestic and international context. As is shown in Table 9, the capability areas are rated as to importance (high, medium, and low) to the Department of National Defence and the Canadian Forces to achieve their overarching defense mission.

Table 9. Canada Capability Goals Matrix

Level	Command and Control		Operations			Sustain	Generate	Corporate Policy and Strategy
	Command	*Info and Intel*	*Conduct*	*Mobility*	*Protect*			
Military Strategic	High	High	Low	High	Low	Low	Medium	High
Operational (Domestic)	High	High	Medium	Medium	Medium	Medium	Medium	Medium
Operational (International)	Medium	Medium	Low	Low	Low	Medium	Low	Medium
Tactical	Medium	Medium	Medium	Medium	Medium	Medium	Medium	High

To reach high capability, the Department of National Defence and the Canadian Forces must be capable of exerting effective, unilateral defense ability in the majority of the applicable Canadian Joint Task List sub-tasks associated with that capability area. The capability must be high and unilateral because it cannot be delegated to another nation or because experience and strategic circumstances dictate that high is the minimum acceptable level for overall success and risk management.

Medium level capability goals, less easily defined, are those where an effective capability in most of the applicable sub-tasks is considered important and may also result from a conscious decision to assume some risk in that capability area. For example, the Canadian Forces need to conduct joint and combined operations effectively and possess interoperability with major allies. Canada's risk assessment considers joint and combined operations as separate concepts. Jointness is the art of combining capabilities from different military services to create an effect that is greater than the sum of the parts. However, not all military functions or capabilities need to be joint: some will be combined. Canadian units more frequently will be combined—interoperate—with the units of another nation of similar capabilities, producing a larger formation and complementary capabilities coordinated in a specific situation. Units may also need to assume a significant leadership role for medium capability goals, although this will not normally be necessary.

A low capability goal indicates a minimum level of capability, depending on a specific strategic situation or an assessment of benefits in seeking a higher capability level for an assigned defense mission compared to costs. Under a low capability goal, Canadian units must be able to take part in joint or combined operations, but not assume a leadership role.

7. Different Planning Horizons

An additional component is incorporating different planning horizons into CBP to stage the development of capabilities, although Taylor (2004) observes CBP can be used against a single future time frame or set of timeframes. Taylor also notes that timeframes should cover a sufficient span for action and changes to take effect, and then allow an assessment of risk over time.

To illustrate, the Canada Department of National Defence (2002a) envisions three planning horizons, each with a different focus for CBP. Horizon One is for a maximum of five years and seeks to deliver capability in already identified ways. Horizon Two is for five to 15 years and focuses on delivering already identified capabilities in better ways. Horizon Three is for 10 to 30 years and determines if capabilities are needed in the anticipated future, in addition to exploring radically new ways of delivering capabilities. The time period is deliberately overlapping for Horizons Two and Three.

Canada describes the first horizon as the most detailed because it executes an already developed plan and shapes near term program aspects. It requires detailed programming of resources, determining if plans are unfolding as required, and developing the appropriate level of capability. The second horizon optimizes how best to do what already is generally understood and ensure that introducing a more effective way of delivering a known capability transitions seamlessly into the more detailed plans from Horizon One. The third horizon is the most challenging as it deals with introducing fundamental changes in the way a capability will be delivered and determining what developments promise to deliver the future necessary capabilities.

Similarly, the U.S. Department of Defense (2001) describes the need for a two-pronged view of implementing CBP—maintaining a military advantage in key areas while developing new areas of military advantage and denying asymmetric advantages to

adversaries. Thus, it entails adapting existing military capabilities to new circumstances, while experimenting with the development of new military capabilities. More specifically, Kiefer (2004a, 2004c) describes force development planning as solving future capabilities by asking what top-down investment guidance is needed to address future strategic challenges. Force development decisions also consider what DoD can provide in achievable technologies and methods of the future force. In contrast, force employment decisions involve planning for today's events, such as strategic decisions as to how best manage and posture DoD assets to support national interests and mitigate risks.

8. Mission-Based, Phased Scenarios

The eighth component is having the right scenarios on which to base planning and/or exercises. Taylor (2004) and The Technical Cooperation Program (2004) stress that defense capability should be assessed using plausible situations encapsulated in planning scenarios. These scenarios provide the context of CBP and should cover the full spectrum of military activities. The scenarios help develop realistic capability goals and the provision of a defense force meeting government requirements at a minimum cost. In addition, as mentioned earlier, scenarios should provide a series of time frames to facilitate capability assessment through time as part of risk assessment, rather than at a single arbitrary point in the future. Scenarios also should be used in combination to assess simultaneous operations.

Scenario types can be on a spectrum, ranging from real world planning scenarios to generic scenarios. Whichever type of scenarios are used, the scenarios should reflect the type of tasks that the government may want its defense force to undertake. In addition, scenarios used for CBP should be common across the defense force and detailed enough so that re-interpretation of the scenario does not occur.

Gori, Chen, and Pozgay (2004) write that Australia uses one or more strategic scenarios to identify a capability requirement and then operational scenarios determine the operational requirements for a proposed capability. Strategic scenarios represent strategically endorsed scenarios, high-level descriptions of situations with a brief history of preceding events and their context. Each scenario typically will describe a conflict

situation, an opposing force, a military setting, a theatre of operations and the events leading up to the conflict situation. They specify the international setting and the attitudes of allies, allies of the enemy and neutrals. They also detail the political aims of the Australian government and its military strategic objectives. All strategic scenarios, taken together, in principle largely define overall defense requirements.

Australia's strategically derived operational scenarios are reference scenarios that have been extended from strategic scenarios, to provide sufficient detail for rigorous evaluation and descriptions of defense requirements for and use of capabilities. One scenario example is evicting an enemy from an overseas territory with phases representing the buildup, the establishment of sea and air dominance, lodgement, the tactical battle, and the post-battle phase. The Australian operational scenarios are more detailed extensions of the strategic scenarios, often detailing a force structure with equipped capabilities to be applied to achieve the particular mission. Strategic and operational scenarios form a link between strategic planning, futures analysis, experimentation, capability development, force development, contingency planning and preparedness.

The United Kingdom Ministry of Defense (2004) builds in what it calls "concurrency" in its use of scenarios for force structure development. The Ministry of Defense establishes what is needed for a particular operational scenario and then maps the conclusions against a number of operations that should be conducted at any one time. For example, the United Kingdom should be able to respond to a medium scale operation at the same time as an enduring small scale operation and a one time small scale intervention operation.

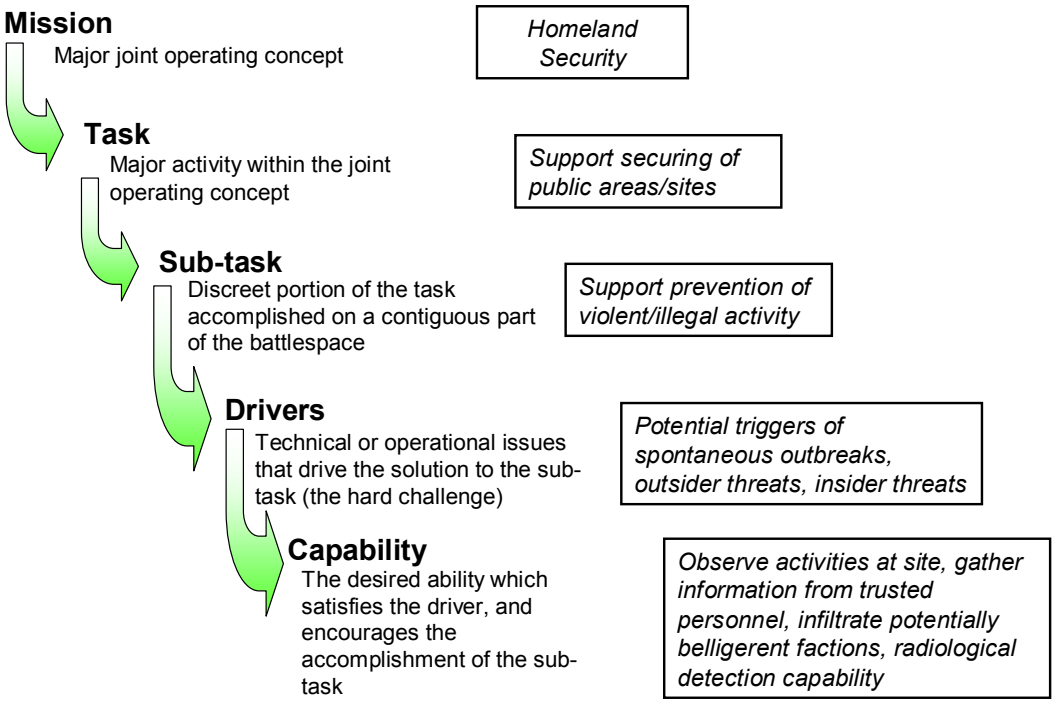
The Canada Department of National Defence (2002a) uses operational research tools in a scenario operational capability risk assessment model to identify how often different types of capabilities are called upon in the scenarios. While there are arguments for using a broad range of scenarios in CBP to thoroughly test force structure for a wide range of situations, the Department of National Defence argues for a small number. The Department believes that while a more comprehensive list of scenarios may theoretically

add more precision to the force planning process, they may not as there are so many uncertainties.

9. Capability Development and Standard Categories

A ninth component is providing guidelines to craft capabilities and develop standard capability categories that fully reflect what effects the capabilities should generate. For example, the Battlespace Awareness Functional Capabilities Board (Joint Chiefs of Staff 2004c) provides guidelines to craft capability descriptions, saying (pp. 4-5) they must indicate 1) what the capability is to do, such as "track" or "determine," 2) identify a target or subject, such as a person on a battlefield, 3) the size or range of the subject, such as a large vessel, 4) the domain of the target systems, such as air-breathing targets, 5) the area of action, and 6) the range to area, or the distance over which effects must be made or action taken. Capabilities are seen as the end of a "waterfall" of lower levels of mission used in functional area analysis, illustrated in Figure 7.

Figure 7. Battlespace Awareness Waterfall Example



Regarding categories, The Technical Cooperation Program (2004) recommends using standard groupings such as capability clusters or capability partitions to make the CBP process more manageable. There are many ways to define the boundaries between capability partitions. These partitions are based on the ability to perform tasks, or to deliver effects, such as the control and denial of underwater battle space. A key enabler for successful CBP is getting the partitions agreed to by the key stakeholders and account for synergies and dependencies across partitions. Taylor (2004) cautions that the capability partitions should not be aligned to inappropriate organizations. If they are aligned, than organizational stovepiping is encouraged.

Kiefer (2004c) defines at least two fundamental military capability categorization options that can be used independently or in combination. One is functional or means-focused. These capabilities would include battlespace awareness, command and control, logistics, and force management. Another option is operational or ends-focused.

Operational categories might include strategic deterrence, homeland defense, civil support, and land combat operations. Each category then would be further defined. To illustrate, force management would include force employment and force deployment. Homeland defense would include capabilities such as continuity of operations, securing domestic approaches and territory, and population protection.

The defense communities have taken similar approaches to capability categorization. For example, as described by the United Kingdom Ministry of Defence (2003, 2004), military tasks provide a framework for detailed defense planning for the size, shape, and capabilities of the Unied Kingdom's Armed Forces. The military tasks reflect the broad types of tasks and operations in which the United Kingdom is likely to be involved and then provide an output-focused framework for developing force structure requirements. The 18 military tasks are in the four areas of 1) standing strategic commitments, such as nuclear deterrent and strategic intelligence gathering, 2) standing home commitments, such as security at home in support of other government departments, 3) standing overseas commitments, such as commitments to international alliances and partners, and 4) contingent operations overseas, such as humanitarian assistance and peace support operations. Military capability is divided into six key capability elements, such as maritime, land, and logistics. The Canada Department of National Defence (2002a) divides military tasks into eight capability areas, such as Command, Information and Intelligence, and Corporate Policy and Strategy.

10. Decision Rules for Lists

In another component, the defense communities establish clear rules for the development of task lists and capability lists. These rules include the source for compiling the lists, what criteria will be used in selecting candidates for the list, and how they should be arrayed. For example, Kiefer (2004b) notes that the universal joint task list for DoD's CBP is the result of 14 years of spiral development. He (2004c) says many sources of information from the task list to individual service sources to interagency information regarding tasks, conditions, and standards are being filtered for DoD's universal capability library. The library structure consists of a capability library—a

master database of capabilities linked to current, planned, and roadmapped forces, units, and equipment—and a task library. The task library is the master database of all doctrinal and conceptual tasks.

The Australia Department of Defence (2003) has followed several principles for designing its Australian Joint Essential Tasks (Joint Tasks): joint, enduring, essential, and containing relevant and current content. Joint tasks are those that require the contribution of two or more forces working together to achieve the desired outcome. Essential tasks are required for the conduct of an operation. Enduring tasks capture how the Australian Defense Force operates currently and might undertake joint operations in the future. Essential tasks capture what are required for the conduct of an operation.

In addition to the design principles, Australia Department of Defence (2003) has set two further design goals for future Joint Task development—uniqueness and hierarchical. For any given level of command, a task only appears once in the task hierarchy. No tasks should be duplicated although some related tasks might appear in more than one place. The requirement for uniqueness is analogous to the United States' UJTL requirement that tasks be mutually exclusive, that is, that any task performed by any joint organization or service unit will fit into only one place in the task structure. Thus common tasks were abstracted out of their natural parent task and were grouped together.

In addition, the Joint Tasks, similar to other defense agencies, are intended to maintain a hierarchical structure. For a high level task, its subordinate tasks, taken together, comprehensively define all of the activities in the higher-level task. For example, the Australian Joint Tasks and Canada's joint task list have three levels of joint tasks—strategic, operational, and tactical. The tasks within each level are further disaggregated into two additional layers of sub-tasks with each layer more detailed and specific.

However, opinions differ about hierarchical and uniqueness design for the lists. For example, Kiefer (2004c) recommends that, at least for DoD, hierarchies should not be imposed because these require preconceived notions about what criteria are more

valuable or useful for segregating data. He also notes that hierarchies require frequent changes or alternate versions of lists. Further, he recommends that mutual exclusivity should not be required, at least at the operational level. His point is that no real force, unit, equipment, or system falls entirely within any one category.

11. CBP Evolution

Another component is evolving CBP depending on planning applications and maturity. Each defense organization used as an example in this paper is in various stages of implementing CBP, both on a national joint and individual service level. However, each organization has tailored CBP and taken a staged approach to implementation. For example, as described by the Australia Department of Defence (2003), allied CBP approaches are similar, but emphasize different outcomes over time:

- The United Kingdom has primarily focused on immediate operations and long term planning. The United Kingdom has used a list of essential joint tasks as an analysis tool for exercises with more recent efforts to integrate the tasks into mission analysis and operational planning.
- Canada's tasks are closely linked into force planning scenarios and future planning and are used in joint department structuring so each department uses the same criteria for operations and to translate tasks into capability. Canada uses its joint task list for force employment and capability development and has developed 11 force planning scenarios to link their capability development and planning.
- The United States joint task list has aided in the development of planning requirements for joint exercises since 1993. The joint task list was developed specifically for training but is now linked into readiness and preparedness reporting and capability development.

CBP also will progress at a different pace in the organization, creating different levels of maturity overall. Thus, some capabilities needed for the defense community of a nation may be delayed compared to others. The Canada Department of National Defence (2002a) points out that over time CBP improves commonality among defense planners by introducing a common way of describing and discussing capability elements. As the different national defense organizations in Canada adopt the common terminology, it becomes easier to link different plans providing various capability components. In the beginning, certain plans will be more mature or more vital for integrated planning. Canada's long-term plan for major equipment is the most mature in

employing CBP. The development of long-term plans for personnel resources, research, concepts, information technology and infrastructure is likely necessary before more encompassing capability planning can be done in Canada.

12. CBP Enablers

The last component is additional organizational and cultural enablers for effective CBP adoption. These are other necessary and sufficient factors, which along with components already mentioned, such as stakeholder ownership, create and sustain the environment for implementation. Many practitioners and students of CBP have highlighted considerations for CBP design and deployment that cover a wide range of factors, from mindset changes to the practicalities of resourcing CBP planning and execution.

Davis and Jenkins (2002) write that CBP's complexity requires a passion for adaptiveness and substantial analysis leading to a combination of incentives, standards, and policies for CBP. They cite the need for major studies on how to modify economic and other incentives to encourage more adaptive and recoverable systems. Feaga (2004) recommends developing new languages in risk management and effects once it is known what capability proficiency and sufficiency levels are needed. Gori, Chen, and Pozgay (2004), writing about the Australian experience, indicate attention is needed to address conflicting processes, the lack of suitable analytical tools, excessively prescriptive requirements, and the recognition of functional linkages and dependencies between related capabilities.

Similarly, the Department of Defense (2003) recommends a broad and long-term strategic perspective, a greater appreciation of the operational and strategic environmental factors, and a rigorous analysis of the capabilities needed to achieve defense policy goals. The Technical Cooperation Program (2004) lists the need for consistent cost estimates and resource provision for both the development and execution of the CBP process. Moreover, joint force personnel will require a joint and expeditionary "mindset" reflecting a greater level of deployability and versatility to avoid organizational stovepiping. Canada's Department of National Defence (2002a) identifies the challenge of developing and maintaining capabilities to conduct operations

independently in domestic situations and alongside alliance and coalition partners for international obligations. Canada believes the focus must remain on combat-capable units because these units can be employed in other security activities, such as peacekeeping, while those with non-combat capabilities cannot meet combat needs.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. HOMELAND SECURITY CBP OBSERVATIONS

A. INTRODUCTION

The previous chapters highlighted CBP concepts and approaches, a description of the DHS adoption of CBP for HSPD-8 requirements, and the defense community's experiences and identification of key CBP components. This chapter broadly assesses the DHS approach against the defense community's components and identifies potential issues for homeland security's CBP process in creating the national preparedness goal. Finally, it discusses difficulties in transferring the practicing defense community components to homeland security and provides additional comments for improvement not directly assessed as part of the CBP component analysis.

B. COMPARISONS

Table 10 summarizes general observations of DHS progress when compared to the defense community components.

Table 10. DHS Progress and the Defense Components

Components	DHS Progress
Business Case for CBP Adoption: *Justify organizational commitment and investment*	Business case stated in terms of national preparedness in HSPD-8 and now in legislation; clear business case still to be made for adopting CBP.
Strategic, Cascading Policy Goals: *Use top-level government guidance that cascade goals into strategic policy and operational documents and into CBP.*	Multiple sources of policy goals including national strategies, HSPD-8 and other presidential directives, the National Response Plan, and the National Incident Management System; integrated, single-source policy document for homeland security and national preparedness not yet available.
Stakeholder Ownership: *Ensure stakeholder involvement, collaboration, and perspective-sharing.*	Inconsistent attention paid to state and local entities as primary stakeholders; primarily federal approach used in consultation with, not collaboration with those entities. Private sector stakeholders yet to be closely involved.
Top Leader Ownership: *Ensure top leader support, involvement, and decision-making.*	Federal leadership within DHS appears supportive; top leadership from other stakeholders still evolving. Decision-making processes not transparent and apparently fragmented.
Specific Management Decision-Making Process: *Design and implement CBP decision process that captures mission tasks and capabilities, their priority, how they relate, solutions, and resource allocation.*	Process has evolved over time but is not formally structured with clear responsibilities, decision-making roles, and integration into stakeholders strategic planning, budgeting, program evaluation, and corrective action. Interim documents extend the process.
Risk Assessment Approach: *Use risk assessment in the CBP management process to*	Risk assessment is not well-defined and presented as an integral part of DHS CBP decision-making similar to the

Components	DHS Progress
determine investments.	defense communities.
Different Planning Horizons: *Incorporate different planning horizons into CBP to stage the development of capabilities.*	No expression of planning horizons to date; DHS has promised to evolve CBP and planning horizons may be part of the evolvement.
Mission-Based, Phased Scenarios: *Have the right scenarios on which to base planning and/or exercises*	Selection of 15 scenarios for planning; concern the scenarios are much too focused on terrorism in contrast to a clearer all-hazards approach and do not include different timeframes, including very long term.
Capability Development and Standard Categories: *Provide guidelines to craft capabilities and develop standard capability categories that fully reflect what effects the capabilities should generate.*	Limited guidance on how to develop capabilities; capability categories still in process; no clear direction provided as to what is the best way to structure the capabilities for use by most entities.
Decision Rules for Lists: *Establish clear rules for the development of task lists and capability lists.*	Rules for development not explicit; changing categories and elements.
CBP Evolution: *Evolve CBP depending on planning applications and developing maturity.*	Policy timeframes have precluded a more evolutionary approach to CBP and addressing differing maturity in capability areas.
CBP Enablers: *Consider organizational and cultural enablers to support CBP adoption.*	Enablers may be recognized but have not been adequately addressed; process characterized by rapid spiral development with extremely limited timeframes for consideration.

1. Business Case for CBP Adoption

The defense community experience suggests the adoption of CBP requires a strong business case to justify the organizational commitment and investment, such as flexibility in addressing current and future adversaries and their strategies. For homeland security, the business case is stated in terms of national preparedness in HSPD-8 and now in legislation for measurable readiness priorities and targets. However, as the DHS experience shows, much more work is needed to make the case for CBP as the right approach to implement HSPD-8. The business case is particularly important given the complexity and the skills required for implementing and sustaining CBP over time across many organizations and for many different contingencies. Moreover, there remains confusion as to whether the focus is primarily counter-terrorism, with all-hazards a secondary emphasis.

2. Strategic, Cascading Policy Goals

Specific policy goals, derived from top-level government guidance, should cascade into strategic policy and operational documents, and then into the CBP process and its planning outputs. For homeland security, there are multiple sources of policy

goals including national homeland security-related strategies, HSPD-8 and other presidential directives, federal agency strategic plans, regulations and policy guidance, the National Response Plan, and the National Incident Management System. In large part, these are statements of federal perspectives because no clear mechanism exists to produce top-level "national" guidance that is accepted and applicable across all levels of government, non-governmental organizations, and the private sector. Unlike what appears to be the case in the defense communities, these various federally-developed national policy documents stand alone. They have not been systematically integrated into a cohesive policy whole. That may be the role envisioned for the national preparedness goal and related guidance, but its current construction will not meet that need. In some cases, there are conflicting objectives and requirements across the policy documents. A single-source policy document for homeland security and national preparedness is not yet available. One is needed.

3. Ownership of Stakeholders

Involvement of stakeholders is critical in because they generally control the information, resources, and authority required to support CBP. The defense community experience shows that the stakeholders should own the process and take responsibility for its use and outputs. For homeland security, DHS has attempted to involve stakeholders such as state and local government officials, national associations, and other federal agencies involved in homeland security. However, this involvement has been more characteristic of a consultative relationship rather than a partnering, collaborative relationship marked by ownership of CBP. Given tight timeframes to meet HSPD-8 objectives and perhaps even its requirement for federal development in consultation with others, the DHS response has been primarily to develop complex CBP material with limited stakeholder involvement. The consultative process relies more on reaction and requirements for rapid comment from stakeholders than partnership in developing the CBP approach. The end result has been "push back" from key stakeholders, confusion about intent and requirements, and lack of understanding of CBP and what it is intended to do.

4. Top Leader Ownership

The defense community experience demonstrates that top leadership support, involvement, and decision-making are critical to CBP success. For defense, support has truly started at the top of cabinet departments and ministries and been sustained. Top military and civilian officials are responsible for CBP and are held accountable for its operation. In contrast, while federal leadership within DHS appears supportive; top leadership involvement, and even the means to secure top leader ownership from other stakeholders, is still a work in progress for homeland security CBP. Decision-making processes are not transparent and, at least in the early stages of CBP adoption, appear fragmented among various DHS groups and organizations at lower authority levels.

5. Specific Management Decision-Making Process

The defense community experience also indicates another element for success is a well-designed and implemented decision process for CBP. This process should capture tasks and capabilities needed to carry out missions and their priority, how they relate, and solutions for meeting those needs. Homeland security, however, does not yet have a process similar, for example, to DoD's Joint Capabilities Integration and Development System. The homeland security CBP process at this point is not formally structured with clear responsibilities, decision-making roles, defined steps and expected inputs and outputs, and melding into formal organizational planning, budgeting, and procurement decisions. It is not clear how CBP will be seamlessly integrated with existing management approaches for government agencies, non-governmental organizations, and private sector companies. The linkage from results expectations to budgeting is particularly problematic, for funders such as board of directors, city councils, state legislatures, and Congress must accept and act on CBP's analytical framework and its products for decision-making.

Moreover, developing mission capability packages for homeland security will require extensive collaboration and the combination of capabilities across stakeholders, no matter the source of funding. It is unclear how that will be accomplished through current disparate management systems. Finally, DHS has relied on a series of interim

documents that are not complete, further complicating and extending decision-making processes.

6. Risk Assessment Approach

The defense community experience pointed out that risk assessment is part of the CBP management process. Risk assessment addresses affordability and sustainability, and thus risk tolerances and priorities for capability development and deployment and their impacts over time. Assessment of risk is built into scenarios, capabilities review, and a consideration of benefits and costs. Measurement systems are viewed as very important. Other than scenario development and directions for states and localities to consider what is appropriate for their jurisdictions, risk assessment is not well-defined and presented as an integral part of homeland security CBP decision-making. Measures and evaluation systems are still in development. Moreover, it will be difficult to develop and implement regional approaches where core capabilities can be supported and supplemented by other jurisdictions in the region. Political considerations may encourage jurisdictions to have a complete set of core preparedness activities rather than rely on other entities. As a result, many jurisdictions will be engaged in parallel activities within their own risk decisions, and there may be little opportunity to learn from one another or share resources as part of an overarching risk management approach.

7. Different Planning Horizons

The defense community incorporates different planning horizons into CBP to stage the development of capabilities for the near, medium, and long term. The homeland security approach at this stage does not appear to have any similar expression of planning horizons. The 15 homeland security planning scenarios address an event in the "here and now" (bombings and bioterrorism) with an emphasis on national priorities. DHS has promised to constantly assess and change CBP and thus the needed planning horizons may yet be addressed. However, lack of attention to capabilities for varying horizons may result in implementing capabilities that may be appropriate next year, but not five years from now. The result is poor investment portfolio planning and creating capabilities that may be obsolete or require extensive updating in a short time period. The focus on national priorities may obscure or delay an emphasis on more valued planning horizons that anticipate possible future scenarios.

8. Mission-Based, Phased Scenarios

The defense community emphasizes that defense capability should be assessed by using plausible situations in planning scenarios to cover the full spectrum of military activities. In addition, scenarios used for CBP should be common across the defense force and detailed enough so that re-interpretation of the scenario does not occur. Many state and local officials are concerned that the national planning scenarios focus too much on terrorism and, as mentioned above, the scenarios do not include different timeframes, including very long term.

The homeland security CBP approach makes the assumption that preparing for terrorist events, representing the vast majority of the planning scenarios, will prepare jurisdictions for all-hazards events. Many would argue that it might make more sense to develop capabilities for more probable all-hazards that can be "ramped up" for large-scale terrorist events or large-scale natural or non-intentional human-caused disasters. As a result, capabilities would cover a full spectrum of homeland security activities. Capabilities then could be scaled to what is affordable and sustainable (and more likely to be used) at the state and local level, and then supplemented by regional and/or federal capabilities if an event overwhelms those capabilities. This approach anticipates that in most catastrophic situations, even a full complement of capabilities at the local or regional level will be quickly overcome.

9. Capability Definition and Standard Categories

The defense community experiences indicate that an important component is providing guidance on crafting capability descriptions and developing standard capability categories fully reflecting what effects the capabilities should generate. DHS policies and guidance do generically define a capability, but guidance is lacking as to how to craft a capability description. The homeland security capability categories should be agreed to by key stakeholders and account for interrelationships across the capability categories.

At present, there does not appear to be a clear sense and rationale as to the best way to partition the homeland security capabilities for use by most entities. The task list categories, still in draft, initially indicated capabilities will reflect primarily an indirect organizational categorization—federal, state, and local responsibilities, and then later on

those for the private sector, nongovernmental organizations, and citizens. This may have created organizational stovepiping of capabilities, which the defense community cautioned against. The latest draft documents use "mission areas" for emphasis—prevention, protection, response, and recover. The IED prototype uses mission areas with critical tasks drawn from the organizational tasks lists, adding to the confusion of what categories are in play or may be the final form. The categorization across task lists and capability areas should be clarified, justified, and stabilized.

10. Decision Rules for Lists

The defense communities establish clear rules for the development of task lists and capability lists, such as uniqueness and hierarchy. For homeland security, publicly available documents indicate a lack of explicit rules for decision-making. Explicit decision rules should help the further development and revision of the detailed and lengthy lists over time. For example, a rule regarding uniqueness would ensure developers would independently assess each task and whether its description is similar to or actually part of another task.

11. CBP Evolution

Another defense community component is evolving CBP to reflect planning applications. CBP also will progress at a different pace in different parts of the organization, creating different levels of maturity. For homeland security, current policy timeframes have precluded a more evolutionary approach to CBP and imposed extremely limited turnaround time for stakeholder comments on various draft products. DHS does plan to keep enhancing the approach, but it will be very hard to dismantle earlier structures once the homeland security grant process "institutionalizes" around capability categories and tiered requirements. A comprehensive CBP system is expected to be up and running in a timeframe of months. While adoption initially will be based on one scenario—explosive devices—for initial planning, federal funding guidance indicates that in less than two years, all scenarios will be part of state and local planning. In addition, the CBP as currently being adopted does not directly address differing maturity in capability areas that may impede overall progress in homeland security preparedness.

12. CBP Enablers

The last component from the defense experience is additional organizational and cultural enablers for effective CBP adoption. The defense experience indicates many facilitative factors come into play for effective CBP, many analytical and skill-based, but others such as incentives, the rationality of processes, and a deliberative approach. For homeland security, enablers such as these may be recognized but have not been adequately addressed, perhaps because they are the difficult "softer" issues or the assumption is that they will be dealt with by stakeholders individually. In addition, the rapid spiral development process has forestalled more careful consideration of CBP and what is needed to support its successful implementation.

C. SUMMARY OF OBSERVATIONS

For virtually every component, the DHS progress falls short of the components that the defense community indicates are important to CBP implementation success. Many of the difficulties described in Chapter IV might have been avoided or mitigated if these components had been addressed. For example, a clear business case might have encouraged stakeholder support early in the process. A specific management decision-making process would have better defined homeland security mission needs, priorities, and linkages to performance-based budgeting. Different planning horizons would have phased the building of capabilities. Attention to organizational and culture enablers would have also furthered CBP adoption.

The next chapter builds on these observations to discuss factors impacting the success in further adopting the defense community components to homeland security.

VII. CONSTRAINTS ON CBP COMPONENT TRANSFERABILITY TO HOMELAND SECURITY

A. KEY FACTORS

In earlier chapters, this thesis has presented the defense community CBP experiences as good practices recommended for homeland security. Bardach (2000), commenting on adopting good practices from outside an organization, observed that one has to ask if the good practice will work in the new organizational context. With that in mind, four key factors differentiate homeland security and the national defense mission that may constrain transferability of CBP practices.

1. Mission Scope and Coverage

A first constraint is mission related. In defense, the **mission scope** is more clearly defined for national defense, most often military action and civil support. While many rightly argue that the national defense mission has broadened considerably in recent years, for homeland security, the mission is arguably broader for prevention, vulnerability reduction, and response and recovery responsibilities. Actions are required at home and abroad, from dealings with individual citizens to negotiations with nation-states as border protection is extended overseas. Homeland security also stresses all-hazards preparedness, requiring attention to a wide range of events, from small-scale earthquakes to catastrophic terrorist events. CBP should allow homeland security to consider these multiple and diverse missions, the common and unique capabilities they require, and what tradeoffs in priorities and resourcing might be necessary.

In addition, the defense experiences emphasize **full mission coverage**. At present, it is not clear if the homeland security CBP approach is emphasizing prevention and deterrence. While draft DHS task lists have included prevention efforts such as intelligence development and providing strategic and threat intelligence, the task lists focus much more attention on vulnerability reduction and response and recovery. Emergency response—after an event—appears to take the lion's share of analysis and preparation with clear emphasis on first responder roles and responsibilities.

The constrained homeland security mission scope and coverage may be the result of several factors. Gilman (2004) observed that there has been a major DHS focus on weapons of mass destruction and terrorism, and not on all hazards and events that happen all that time, such as explosions. Prevention has been "under the radar screen" for DHS as it might be considered the purview of other agencies, such as the Department of Justice or the Central Intelligence Agency, or state and local law enforcement officials. In addition, DHS's Office of Domestic Preparedness has had a mission of emergency management, not other aspects of homeland security, and it would be normal to see this office maximize its area of strength or understanding. Perhaps more importantly, since September 11, first responders have been front and center, their needs expounded, and the results in terms of new equipment and capabilities much more visible.

2. Organizational Perspectives

A second constraint involves organizational perspectives. One perspective is a **federal department versus a national view.** The defense community normally contains decisions within a cabinet department and White House sphere, with input from other federal agencies and to a lesser extent, international partners. In contrast, homeland security is presented as national in scope, not a federal responsibility of primarily just one executive department or agency. A national perspective requires a much more collaborative approach, particularly in a federalist system and a fairly clear distinction between public and private spheres.

Moreover, even within the federal homeland security establishment there is fragmentation. Federal agencies other than DHS can act autonomously, buoyed by their own sources of support and direction. Even when collaborative decisions are made, the vehicles for enforcement are very limited or unwanted. The homeland security organizations represent different disciplines and perspectives, levels of public, private, and nongovernmental organizations, and even horizontal relationships such as the involvement of different federal, state, or local cabinet agencies. Defense has a central core of military services that perform its activities that share a common culture and perspective to support and deploy the warfighter. CBP should allow homeland security

to change its unit of analysis from organizations and requirements to capabilities and their delivery.

In addition, **chain of command and exercise of authority** are different. Defense normally has a top-down command and control structure with a highly disciplined attention to authority. The homeland security CBP approach at present does not adequately guide analysis when assets and capabilities to accomplish a mission are not under one jurisdiction, may be unknown, or may ebb and flow over time. The draft national preparedness rating scheme indicates that a group of organizations can be rated collaboratively under a mutual aide or an assistance compact to perform prevention, response, or recovery tasks for a specific scenario.

For CBP, it is crucial that relationships are driven by strategic alliances among equal partners where all stakeholders—strategic partners—are identified, their needs clearly represented in collaborative decision-making, and incentives provided for decisions to not unravel. Capability planning is always tied to sustainability analyses and funding support favors multiple-use capabilities and multiple sources of capabilities to reduce the funding burden on any one organization. Additional work is needed to better understand how to apply the framework where there are networks of organizations that work homeland security issues or are discrete sets of organizations that handle specific homeland security functions. Contingency planning is necessary in the event individual organizations or sectors will not meet their capability obligations. This will be even more important when the CBP framework is expanded to address private sector and nongovernmental organizations who are critical players in prevention, vulnerability reduction, and response and recovery strategies and actions.

3. Resource Development and Leveraging

A third constraint is the resources that can be brought to bear for homeland security in contrast to the defense community. To start, resource leveraging requires the **understanding of assets** that compose capabilities and in general what they can accomplish. Capabilities include a diverse selection of elements, such as plans, procedures, personnel, equipment, and activities. Defense organizations have paid considerable attention to the assets that can be combined for capabilities, where they are

deployed, what their maintenance or skill condition is, and when they will become obsolete or require renewal. This is not yet the case in homeland security, where asset identification and control is dispersed to thousands of organizations who may or may not have a complete and accurate inventory. Many homeland security contingency plans draw on mutual aid or regional agreements, often without full identification of assets and how they will work together. CBP provides a mechanism for asset identification, but initially CBP will be hampered as homeland security officials gather and assess this information and their contribution to capability planning.

In addition, resources include **planning resources, skills, tools, and experiences**. Defense communities normally have decades, if not centuries, of planning experience for concrete events and contingencies. These communities bring to bear a wide range of tools such as wargaming, exercises, and simulations, and a small army of skilled and experienced planners devoted to such work. Exercises and actual field experience are rapidly fed back to planners. In contrast, homeland security is in the early stages of planning and is often not well-resourced with dedicated staff, particularly in smaller jurisdictions. Tools and skills are still in development in government organizations. While emergency exercises have been the norm for a number of years, a systematic collection, evaluation, and dissemination of lessons learned and better practices has only recently picked up speed. The private sector in some critical infrastructure areas and for some companies may have the requisite resources, skills, tools, and experiences, or can draw on combined sector practices, but not all. Non-governmental organizations, with limited resources, may also have difficulty in adopting CBP. It can be expected there will be a slower identification of current and required capabilities and under what scenarios they are effective.

A tiered CBP approach in homeland security may not adequately address the very wide variety of structures, skills, and processes for homeland security activities across the nation. For example, Gilman (2004) noted that DHS does not understand, or chooses not to understand, that there is a major difference in homeland security or emergency preparedness operations and capacities between the rural and urban areas in a state or region. He said that many homeland security and emergency management contacts are in

rural areas, and many are volunteers or handle homeland security along with many other tasks. These officials often have limited infrastructure support, such as access to good communication services. Rural areas also have more difficulty forming mutual aid compacts and, if they do, may get limited help because of geography or limited regional assets and liabilities. Rural areas may have to wait many hours for mutual aid help to arrive because of the distances involved.

4. Target Audience

Finally, there are differences in the target audiences for CBP. For the defense community, the clear customer for CBP outputs is the combatant commander who must carry out the defense missions and relies on mission capability packages. For homeland security, the target audience at present is broadly described by DHS as the "homeland security community," which can cover federal, state, local, private, and nongovernmental organizations, and even to the level of the individual citizen. Thus, there is not a discrete set of homeland security "combatant commanders" under the current DHS CBP approach. This has added to the complexity and confusion surrounding CBP that will require further attention.

Federal national policy is primarily directed at state and local jurisdictions at this time, with some attention paid to limited regional compacts. It may be that CBP development over time will clarify that the combatant commander should be those state and local government officials responsible for direct prevention, vulnerability reduction, and response and recovery activities. While private sector and non-governmental officials have direct homeland security responsibilities as well, the CBP process may need to stop at the governmental level. Governmental CBP outputs can be planning inputs to these other jurisdictions for their own planning processes.

Instead of supporting the combatant commander, the capabilities-based approach might get bogged-down in a checklist mentality of responding to lists of many tasks represented by the UTL and a targeted list for critical capabilities. "Checking off" the tasks forces attention to discrete activities, and not to capabilities and homeland security results for an organization and its homeland security partners. State and local officials at the October 2004 capabilities workshop noted that the task lists and defined capabilities

easily can become a standard of care to which they will become individually accountable. A defensive posture might be to manage to the lists, and not to the overall results that must be achieved within a risk assessment decision-making process. As a result, developing envelopes of capability for specific operational challenges for the combatant commander will be lost.

VIII. A MELDED APPROACH

A. REHABILITATION OF HOMELAND SECURITY CBP

As the chapters to this point have highlighted, continuing to implement CBP through the current approach is fraught with difficulty. The defense community CBP implementation experiences point to practices that the homeland security community should adopt or tailor to homeland security. The differences between defense community and homeland security characteristics point to major issues in expecting there will be a seamless—and effective—transfer of CBP from defense to homeland security. These issues also should be addressed as the HSPD-8 implementation moves forward.

Some may argue that CBP presents too many implementation challenges and that DHS should consider some other approach in crafting a national preparedness goal and related objectives and measures. The fact remains, however, that CBP does incorporate strong features in meeting homeland security results expectations and the DHS commitment to its implementation remains strong. This chapter presents additional integration opportunities DHS might consider to "rehabilitate" CBP for the homeland security community. These integration opportunities include 1) using a current national management standard as the overarching framework, 2) expanding capability coverage to more fully incorporate National Strategy for Homeland Security mission areas, and 3) building performance partnership and collaborative approaches and methods.

1. National Management System Standard

The first opportunity is using a national management system standard for an all-hazards, risk-based approach for homeland security. Standards for homeland security focus on jurisdictional capabilities that can meet multiple possible terrorist events and impacts (Yim, 2003; Yim and Caudle, 2004). DHS's current approach does not clearly start with local and state threats and risk-based responses. Instead, DHS has taken a "top-down" approach that identifies major preparedness events. However, the events stressed for preparedness are well-defined catastrophic terrorist events, not all-hazards, and they are not risk-based at a jurisdictional level. The interim national goal and related national preparedness guidance discuss state and regional tailoring, but the underlying thrust is

that the basic capabilities lists are considered minimum capabilities necessary for carrying out core competencies and essential tasks. The assumption is that preparing for catastrophic terrorist events, represented in the vast majority of CBP planning scenarios prepares each jurisdiction for an all-hazards event in their jurisdiction and for the support of other jurisdictions or the nation in the event of a catastrophic event.

The CBP lists are useful tools for planning, but should not be mandated. It makes more sense for jurisdictions to select, implement, and sustain core capabilities contingent on their own risk assessment as to what is appropriate for all-hazards in the individual jurisdiction and agreements they actually have with other jurisdictions. Contingency plans and mutual aid agreements would define capabilities needed if the core capabilities are overwhelmed by an event. Core capabilities would be scaled to what is affordable and sustainable (and more likely to be used) at the state, local, and private level. These may, or may not be, dependent on population size.

Using a national standard, a full risk assessment would define what is appropriate for each jurisdiction and what it has agreed to support for other jurisdictions. It is not practical, or necessary, for all jurisdictions to have capabilities, no matter how limited, to respond to a catastrophic event. Jurisdictions should be required to have action plans and mutual aid agreements that activate regional, state, and/or federal capabilities if core capabilities are insufficient. Nor should they be required to have a national focus. For example, it is not justifiable to expect Tonopah, Nevada to have basic capabilities to meet a nuclear detonation in Los Angeles or a biological attack in Washington, DC. Using a national standard framework also would preclude jurisdictions from merely taking a "checklist" approach that does not address the inherent uncertainty of possible major events.

The current voluntary standard for homeland security and national preparedness is the National Fire Protection Association 1600 (NFPA 1600). It is a standard that could be used in conjunction with CBP. The NFPA 1600 standard provides a common set of criteria for disaster management, emergency management, and business continuity programs. NFPA 1600 is intended to provide those with responsibility for these programs with the criteria to assess current programs or to develop, implement, or

maintain a program to mitigate, prepare for, respond to, and recover from disasters and emergencies in an all-hazards approach. The standard covers elements such as program administration and evaluation; hazard identification, risk assessment, and impact analysis; hazard mitigation; mutual aid; resource management; planning; and operations and procedures. Examples of standards include 1) establishing performance objectives and conducting periodic evaluations, 2) identifying hazards, the likelihood of their occurrence, and the vulnerability of people, property, the environment, and the entity itself to those hazards, 3) developing and implementing a strategy to eliminate hazards or mitigate the effects of hazards that cannot be eliminated, and 4) develop the capability to direct, control, and coordinate response and recovery operations (NFPA, 2004).

Working with DHS, the American National Standards Institute recommended to the 9/11 Commission that the NFPA 1600 standards, with adjustments recommended by a working group, be recognized as the national preparedness standard (ANSI, 2004). The planned adjustments include 1) emphasizing an all-hazards approach, 2) emphasizing prevention and deterrence, 3) expanding mitigation strategies, 4) leveraging existing preparedness programs and capabilities, and 5) including partnership relationships and incentives, particularly those outside the organization involved in an interdependent, coordinated, and networked relationships (ANSI-HSSP Workshop, 2004). In its final report, the 9/11 Commission recommended the adoption of the national preparedness standard and has urged DHS to promote its adoption. However, DHS has been generally silent on its use in implementing HSPD-8, referring only to the Emergency Management Accreditation Program, which is based on NFPA 1600. Because it is the national preparedness standard, NFPA 1600 can provide the general requirements for homeland security results management. CBP planning can be used across the standard, such as identifying risks, establishing performance objectives, crafting strategies, and targeting capabilities—using DHS's UTL and capabilities lists to meet jurisdictional needs or those developed in concert with partners.

2. National Strategy for Homeland Security Mission Areas

A second opportunity is full prevention, vulnerability reduction, and response and recovery mission coverage, such as that represented in the mission areas of the National

Strategy for Homeland Security. The DHS documents stress that CBP is intended to address national preparedness to maximize the ability to prevent, respond to, and recover from major events. In addition, CBP is to produce readiness measures and elements such as standards for preparedness assessments and strategies and a system for assessing the nation's overall preparedness to respond to major events. On their face, the ODP documents assume mission coverage of prevention, response, and recovery. However, the more detailed CBP documents, such as capability lists and scenarios, tell another story. It is clear that CBP's "point of the spear" is preparedness for response after an event, with much less attention paid to prevention, protection, and recovery. Emphasizing response, while much easier to do than the other homeland security mission areas, is much too limited for a national preparedness goal, which should start with prevention.

One solution is for DHS to much more strongly emphasize the fundamental focus of the National Strategy for Homeland Security. Although some, such as Goure' (2004), have argued that the National Strategy provides relatively little, strategy, it does provide reasonable goal and mission areas as a framework for national preparedness. The National Strategy defines the full scope of homeland security from prevention to response and recovery (this is consistent with the goals from the DHS 2004 Strategic Plan). As discussed earlier, under the National Strategy, prevention means action at home and abroad to deter, prevent, and eliminate terrorism. Vulnerability reduction means identifying and protecting critical infrastructure and key assets, detecting terrorist threats, and augmenting defenses, while balancing the benefits of mitigating risk against economic costs and infringements on individual liberty. Response and recovery means managing the consequences of attacks, and building and maintaining the financial, legal, and social systems to recover. These are similar to the DHS strategic goals of awareness, prevention, protection, response, and recovery.

As mentioned earlier, the National Strategy provides six critical mission areas (intelligence and warning, border and transportation security, domestic counterterrorism, critical infrastructure and key asset protection, catastrophic threat defense, and emergency preparedness and response) that might serve to balance the attention in the

CBP mission scope and related capabilities for federal, state, local, and private jurisdictions. The latest homeland security federal budget request emphasizes that the federal government is using the National Strategy for Homeland Security to guide its homeland security goals and budgets.

In the President's fiscal year 2006 budget proposal, agencies categorize their funding data based on the critical mission areas defined in the National Strategy (United States Government 2005). Updating the National Strategy descriptions, the budget proposal describes the **intelligence and warning mission area** as covering activities to detect terrorist threats and disseminate terrorist-threat information. The category includes intelligence collection, risk analysis, and threat-vulnerability integration activities for preventing terrorist attacks. It also includes information sharing activities among federal, state and local governments, relevant private sector entities (particularly custodians of critical infrastructure), and the public at large. The major requirements addressed in the intelligence and warning mission include: 1) unifying and enhancing intelligence and analytical capabilities to ensure officials have the information they need to prevent attacks, and 2) implementing the Homeland Security Advisory System and other information sharing and warning mechanisms to allow federal, state, local, and private authorities to take action to prevent attacks and protect potential targets.

The **border and transportation security mission area** covers activities to protect border and transportation systems, such as screening airport passengers and detecting dangerous materials at ports overseas and at U.S. ports-of-entry. The strategy aims to make the U.S. borders "smarter"—targeting resources toward the highest risks and sharing information so that frontline personnel can stay ahead of potential adversaries—while facilitating the flow of legitimate visitors and commerce.

The **domestic counterterrorism mission area** covers federal and federally-funded supported efforts to identify, thwart, and prosecute terrorists in the United States. The major requirements in the mission area are 1) developing a proactive law enforcement capability to prevent terrorist attacks, 2) apprehending potential terrorists, and 3) improving law enforcement cooperation and information sharing to enhance domestic counterterrorism efforts across all levels of government.

The **mission area of protecting critical infrastructure and key assets** includes the efforts of the U.S. government to secure the nation's infrastructure, including information infrastructure, from terrorist attacks. Major requirements include 1) unifying disparate efforts to protect critical infrastructure across the federal government, and with state, local, and private stakeholders, 2) building and maintaining a complete and accurate assessment of America's critical infrastructure and key assets and prioritizing protective action based on risk, 3) enabling effective partnerships to protect critical infrastructure, and 4) reducing threats and vulnerabilities in cyberspace.

The **mission area of defending against catastrophic attacks** covers activities to research, develop, and deploy technologies, systems, and medical measures to detect and counter the threat of chemical, biological, radiological, and nuclear (CBRN) weapons. The major requirements in this mission area include 1) developing countermeasures, including broad spectrum vaccines, antimicrobials, and antidotes, and 2) preventing terrorist use of CBRN weapons through detection systems and procedures, and improving decontamination techniques.

The **emergency preparedness and response mission area** covers agency efforts to prepare for and minimize the damage from major incidents and disasters, particularly terrorist attacks that endanger lives and property or disrupt government operations. The major requirements in this mission area include 1) establishing measurable goals for national preparedness and ensuring that federal funding supports these goals, 2) ensuring that federal programs to train and equip states and localities meet national preparedness goals in a coordinated and complementary manner, 3) encouraging standardization and interoperability of first responder equipment, especially for communications, 4) building a national training exercise, and evaluation system, 5) implementing the National Incident Management System, 6) preparing health care providers for a mass casualty event, and 7) augmenting America's pharmaceutical and vaccine stockpiles.

These budget proposal details could serve as better categories for capability development at all levels of government, the private sector, and non-governmental organizations.

3. Partnership Approaches

Finally, DHS's approach to CBP does not adequately recognize or provide incentives for partnerships in tailoring and sustaining capabilities as part of a joint approach and at a strategic alliance level. The DHS documents do discuss mission area assessments for entities operating individually or together. However, there are no incentives for partnering. In addition, the current CBP lists are designed for individual jurisdictions at the federal, state, and local levels, with scorecards for each jurisdiction, and subsequent lists planned for the private sector, nongovernmental organizations, and even citizens. Such an approach further exacerbates any thought of partnerships and creates organizational stovepiping of capabilities. Further, state and local governments have sovereignty in our federalist system and the private and non-governmental sector are under no obligation (other than what the federal government might create through law or regulation) to meet capability requirements.

In practice, given federal funding mechanisms, individual entity budgeting and funding requirements, and liability concerns, entities will not normally build in formal partnerships for response to a major event, particularly if they consider a major event unlikely. Mutual aid agreements often call for reimbursement and liability assignment, both barriers to partnerships. In a recent report, GAO (2004d) observed that historically, the American governance system, divided into federal, state, and local jurisdictions, does not provide a natural vehicle for addressing public policy issues from a regional, multi-jurisdictional perspective. There are different operational structures and civic traditions of states and municipalities. Strategic plans in regional coordination efforts can result in mutually agreed upon problems and solutions. GAO observed that regional approaches have been recognized a key way to address the threat of terrorism as in many urban areas, the threat of terror is regionwide and resources for responding to the threat are distributed among many jurisdictions.

Achieving strategic alliances for homeland security will require considerable effort by all partners. Klitgaard and Treverton (2004) write that partnerships stretch from partial collaboration on one end to virtual integration on the other. Partnerships evolve as

partners move from limited and wary collaboration to realizing they have more common interests and joint possibilities. At the integrative stage, the alliance becomes strategic and the boundaries between the organizations begin to blur. The partnership comes to resemble an integrated joint venture that is critical to the strategies of both partners and can respond to the changing environment. Homeland security strategic partnerships will be particularly important given the differences in jurisdictional planning resources, skills, tools, experiences, and level of commitment that can be brought to bear in adopting capabilities.

However, there are many partnership and incentive approaches that can be considered for homeland security to complement CBP. Radin (2000) discusses several different approaches that have been taken within federal agencies to deal with issues of performance. One that is particularly attractive for homeland security is performance partnerships. Performance partnerships include combining resources from both players to achieve a pre-specified end-state. The performance partnerships entered into by the U.S. Environmental Protection Agency and states have been among the most visible of these arrangements. States and EPA determine on an annual basis what and how work will be performed.

As described by Metzenbaum (2005), EPA and states cooperated to produce the National Performance Partnership System (NEPPS). EPA and the states reach agreement on a common set of performance measures every state would report for purposes of national environmental assessments. Each state participating in the partnership system identifies appropriate state-specific environmental performance goals and measures. The states would work with EPA in an equal partnership to select, test, develop, adopt, and update the measures. States are expected to conduct self-assessments and share them with the public. Based on both the state's and EPA's assessment of environmental conditions and state program performance, each state and EPA would sign an agreement regarding appropriate national and state-specific environmental goals, program performance indicators, state commitments for specific deliverables and activities to address identified needs, disinvestments, and federal commitments.

The same approach could be taken in partnerships between federal and state governments, and state governments and local governments for homeland security expectations. CBP could be one tool used to define the capabilities, but these would not be nationally mandated. Instead, each state and DHS would enter into an agreement regarding federal and state-specific homeland security goals, measures, and activities. Each partner would have defined commitments for developing capabilities to meet the homeland security goals. A good example is the environmental approach used for the Chesapeake Bay in the Mid-Atlantic region. Several states and the federal government entered into an agreement with clear goals and targets to protect and restore the Bay (Chesapeake Bay Program 2000).

B. CONCLUSION

The present DHS approach to homeland security CBP has considerable merit. Its focus on capability packages anticipating uncertainty and a wide range of possible events sets outcome expectations. Measurement will focus on outputs and processes that reasonably can be expected to comprise preparedness.

However, the approach also has challenges, many resulting from the scope of the effort, the many stakeholders involved, resource constraints, and the many decision processes that are impacted. Without considering the melded approach presented above, the specific capability packages to make the homeland more secure still require definition, particularly the differentiating joint and combined capabilities of public and private organizations. Federal, state, local, and private leadership is apparent, but that leadership needs to be better defined and exercised in homeland security CBP efforts. The target audience—a clear homeland security combatant commander—should be defined.

In addition, resource leverage, while rhetorically championed, is often lost in the morass of budgeting and funding systems across the country and the difficulty in working out formal mutual aid agreements or informal understandings. Capability options will be difficult to assess for costs and effectiveness. Some, such as Carafano and others (2005) argue that the capabilities-based model is open-ended despite the fact it is not practical to budget for every desired capability. There will be differences of opinion as to what

should be the precise homeland security goals to define capabilities. Risk management for CBP now relies on limited near-term, terrorist-centric scenarios, necessitating additional work for all-hazards preparedness and much longer-term efforts. Federal tools and programs responsive to HSPD-8 and CBP still are in their infancy, but will be expected to create cost-effective homeland security approaches for homeland security. Lastly, CBP should create the assessment tools to address preparedness for addressing the spectrum of current and future threats, but that assessment process, supported by robust analytical tools, may be years off.

The continued identification and resolution of national preparedness goal issues should be addressed as CBP is implemented over the next several years. The defense community experience indicates that there can be many variations from the generic CBP model for defense planning. Without a focus on robust homeland security mission areas, a more flexible approach such as that available through a national management standard system, and the use of performance partnerships, CBP will not easily be institutionalized. Over time, the melded approach provides a more robust and flexible framework to make difficult choices about what homeland security expectations should be when faced with uncertainty and an environment of fiscal constraints.

BIBLIOGRAPHY

American National Standards Institute. (2004). *9-11 commission presented with recommendation on emergency preparedness.* News release, April 29, 2004.

ANSI-HSSP Workshop on Private Sector Emergency Preparedness and Business Continuity. (2004). *Recommendations to the NFPA 1600 Committee*. Internal document dated March 22, 2004.

Aristigueta, M. (1999). *Managing for results in state government*. Westport, CT: Quorum Books.

ASIS International (2003). *General security risk assessment guideline.* Alexandria, VA: ASIS International.

Association of State and Territorial Health Officials (ASTHO). (2004). *Letter to Ms. C. Suzanne Mencer*. Lexington, KY: October 15, 2004.

Australia Department of Defence. (2000). *Defence 2000: Our future defence force.* Canberra, Australia: Department of Defence.

Australia Department of Defence. (2003). *Joint warfare capability assessment-final report: Australian joint essential tasks volume 1.* Canberra, Australia: Department of Defence.

Bardach, E. (2000). *A practical guide for policy analysis*. New York: Chatham House Publishers.

Bea, K. (2005). *The national preparedness system: Issues for the 109th Congress.* Washington, DC: Congressional Research Service (March 10, 2005).

Bryson, J. (1995). *Strategic planning for public and nonprofit organizations.* Revised edition. San Francisco: Jossey-Bass Publishers.

Canada Department of National Defence. (2002a). *Capability based planning for the Department of National Defence and the Canadian forces.* Montreal, Canada: Department of National Defence (May 27, 2002).

Canada Department of National Defence. (2002b). *Capability outlook 2002-2012.* Montreal, Canada: Department of National Defence (July 2002).

Carafano, J., J. Spencer, and K. Cudgel. (2005). *A congressional guide to defense transformation: Issues and answers.* Backgrounder No. 1847. Washington, DC: Heritage Foundation (April 25, 2005).

Caudle, S. (2004). *Record of analysis: DHS capabilities workshop 10/12-14/04*. Author: October 15, 2004.

Chesapeake Bay Program. (2000). Chesapeake 2000, http://www.chesapeakebay.net/agreement.htm. (accessed May 10, 2005).

Council on Foreign Relations. (2003). *Emergency responders: Drastically underfunded, dangerously unprepared.* New York: Council on Foreign Relations.

David, R. (2002). *Homeland security: In pursuit of the asymmetric advantage.* Paper presented at the Committee on National Security Systems 2002 annual conference, April 9-11, 2002.

Davis, P. (2002). *Analytical architecture for capabilities-based planning, mission-system analysis, and transformation.* Santa Monica, CA: RAND.

Davis, P. (2003). Uncertainty-sensitive planning. In *New challenges, new tools for defense decisionmaking*, ed. S. Johnson, M. Libicki, and G. F. Treverton, 131-155. Santa Monica, CA: RAND Corporation.

Davis, P. and B. Jenkins. (2002). *Deterrence and influence in counterterrorism: a component in the war on al Qaeda.* Santa Monica, CA: RAND National Defense Research Institute.

Department of Defense. (2001). *Quadrennial defense review report.* Washington, DC: Department of Defense (September 30, 2001).

Department of Defense. (2003). *Joint operations concepts.* Washington, DC: Department of Defense (November 2003).

Department of Homeland Security. (2004a). *National incident management system.* Washington, DC: Department of Homeland Security (March 1, 2004).

Department of Homeland Security. (2004b). *Securing or homeland: U.S. Department of Homeland Security Strategic Plan.* Washington, DC: Department of Homeland Security (February 2004).

Dubois, R. (2004). *U.S. Coast Guard performance*. Presentation at the Government Integration Group, Washington, DC, January 12, 2004.

Falkenrath, R. (2001). Problems of preparedness: U.S. readiness for a domestic terrorist threat. *International Security*, Vol. 25, No. 4 (Spring 2001): 147-186.

Feaga. K. (2004). The USAF capabilities based CONOPS construct. Academic research paper, U.S. Army War College.

General Accounting Office. (1997). *Performance budgeting: Past initiatives offer insights for GPRA implementation*. GAO/AIMD-97-46. Washington, DC: U.S. General Accounting Office (March 27, 1997).

General Accounting Office. (2004a). *Evaluation of selected characteristics in national strategies related to terrorism*. GAO-04-408T. Washington, DC: U.S. General Accounting Office (February 3, 2004).

General Accounting Office. (2004b). *Homeland security: Selected recommendations from Congressionally chartered commissions and GAO*. GAO-04-591. Washington, DC: U.S. General Accounting Office (March 31, 2004).

Government Accountability Office. (2004c). *Homeland security: Observations on the national strategies related to terrorism*. GAO-04-1075T. Washington, DC: U.S. Government Accountability Office (September 22, 2004).

Government Accountability Office. (2004d). *Homeland security: Effective regional coordination can enhance emergency preparedness.* GAO-04-1009. Washington, DC: U.S. Government Accountability Office (September 15, 2004).

Gilman, J. (2004). *Using a performance management system for homeland security funds to demonstrate accountability and improve organizational effectiveness*. Presentation to the Advanced Learning Institute's Performance Measurement for Homeland Security conference, Arlington, VA (December 1, 2004).

Gilmore Commission. (2003). *V. Forging America's new normalcy*. Fifth Annual Report to the President and the Congress, Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. Arlington, VA: Rand Corporation.

Goure', d. (2004). Homeland security. In *Attacking terrorism: Elements of a grand strategy,* ed. A. Cronin and J. Ludes, 261-284. Washington, DC: Georgetown University Press.

Gori, R., P. Chen, and A. Pozgay. (2004). "Model-based military scenario management for defence capability," proceedings, Defence Experimentation Symposium 2004, March 29-April 2, 2004, Edinburgh, UK.

Gruber, C. (2004a). *HSPD-8 national preparedness*. Presentation to the National Homeland Security Consortium, Arlington, VA (December 8, 2004).

Gruber, C. (2004b). *Collaboration to communities: The issues and challenges surrounding preparedness*. Presentation at the National Press Club, Community Preparedness Briefing, Washington, DC (December 7, 2004).

Hatry, H. (1999). *Performance measurement: Getting results.* Washington, DC: The Urban Institute Press.

Homeland Security Council. (2004). *Planning scenarios: Executive summaries*. Washington, DC: Executive Office of the President, July 2004.

J-7 Joint Staff. (2004). *Joint capabilities integration and development system*. Presentation to the Military Operations Research Capabilities-Based Planning Conference, Alexandria, VA, (October 18-21, 2004).

Joint Chiefs of Staff. (2004a). *Chairman of the joint chiefs of staff instruction: Joint capabilities integration and development system*. Washington, DC: Department of Defense (March 12, 2004).

Joint Chiefs of Staff. (2004b). *Chairman of the joint chiefs of staff manual: Joint capabilities integration and development system*. Washington, DC: Department of Defense (March 12, 2004).

Joint Chiefs of Staff. (2004c). *Battlespace awareness functional capabilities board: Functional area analysis*. Washington, DC: Department of Defense (March 29, 2004).

Kelley, C., P. Davis, B. Bennett, E. Harris, R. Hundley, E. Larson, R. Mesic, and M. Miller. (2003). *Metrics for the quadrennial defense review's operational goals*. Santa Monica, CA: RAND National Defense Research Institute.

Kendall, J. (2002). Capabilities-based planning: The myth. Course 5605 Seminar L paper, National Defense University, National War College.

Kettl, D. (2002). *Promoting state and local government performance for homeland security*. New York: The Century Foundation Homeland Security Project.

Kiefer, T. (2004a). Capabilities based planning & concepts, http://www.dtic.mil/jointvision/capabilities.htm. (accessed October 15, 2004).

Kiefer, T. (2004b). Capabilities framework, http://www.dtic,mil/jointvision/capabilities.htm. (accessed October 15, 2004).

Kiefer, T. (2004c). *Capabilities based planning framework*. Presentation to the Military Operations Research Capabilities-Based Planning Conference, Alexandria, VA (October 18-21, 2004).

Klitgaard, R. and G. Treverton. (2004). Assessing partnerships: New forms of collaboration. In *Collaboration: Using networks and partnerships*, ed. J. M. Kamensky and T.J. Burlin, 61-102. Lanham, MD: Rowman & Littlefield Publishers, Inc.

McClellan, D. (2004). *Delivering strategic intent*. Presentation to the World Future Society, Washington, DC (August 2, 2004).

McLaughlin, J. and G. Jordan. (2004). Using logic models. In *Handbook of practical program evaluation*, ed. J. S. Wholey, H. P. Hatry, and K. E. Newcomer, 7-32. 2nd ed. San Francisco: Jossey-Bass.

McLaughlin, J. and G. Jordan. (1998). *Logic models: A tool for telling your program's performance story*. http://www.pmn.net/education/Logic.htm (accessed September 28, 2000).

Metzenbaum, S. (2005). Strategies for using state information: Measuring and improving program performance. In *Managing for results 2005*, ed. J. M. Kamensky and A. Morales, 277-349. Lanham, MD: Rowman & Littlefield Publishers, Inc.

Millar, A., R. Simeone, and J. Carnevale. (2001). Logic models: a systems tool for performance management, *Evaluation and Program Planning*, Vol. 24 (2001): 73-81.

National Academy of Public Administration. (2004). *Advancing the management of homeland security: Managing intergovernmental relations for homeland security.*

National Emergency Management Association (NEMA). (2004). *Letter to Sue Mencer*. Lexington, KY: October 29, 2004.

National Fire Protection Association (NFPA). (2004). *Standard on disaster/emergency management and business continuity programs 2004 Edition*. Quincy, MA: National Fire Protection Association.

Newcomer, K. (1997). Using performance measurement to improve programs. In K. E. Newcomer (Ed.). *Using performance measurement to improve public and nonprofit programs* (pp. 5-14). New Directions for Evaluation, no. 75, San Francisco: Jossey-Bass Publishers.

9/11 Commission. (2004). *The 9/11 commission report*. Final Report of the National Commission on Terrorist Attacks Upon the United States. Washington, DC: U.S. Government Printing Office.

Office for Domestic Preparedness (ODP). (2004a). *Request for input on universal task list*. Washington, DC: Office for Domestic Preparedness, Department of Homeland Security, July 12, 2004.

Office for Domestic Preparedness. (2004b). *Request for input on universal task list*. Washington, DC: Office for Domestic Preparedness, Department of Homeland Security, August 13, 2004.

Office for Domestic Preparedness. (2004c). *Department of Homeland Security: Homeland security presidential directive/HSPD-8 "national preparedness*." Washington, DC: Office for Domestic Preparedness, Department of Homeland Security, April 16, 2004.

Office for Domestic Preparedness. (2004d). *Universal task list manual version 1.0*. Washington, DC: Office for Domestic Preparedness, Department of Homeland Security, October 2004.

Office for Domestic Preparedness. (2004e). *Universal task list: Responses to frequently asked questions*. Washington, DC: Office for Domestic Preparedness, Department of Homeland Security, October 2004.

Office for Domestic Preparedness. (2004f). *Fiscal Year 2005 homeland security grant program: program guidelines and application kit*. Washington, DC: Office for Domestic Preparedness, Department of Homeland Security, December 2004.

Office for Domestic Preparedness. (2004g). *Universal task list 2.0*. Washington, DC: Office for Domestic Preparedness, Department of Homeland Security, December 21, 2004.

Office of Homeland Security. (2002). *National strategy for homeland security*. Washington, DC: Executive Office of the President, July 2002.

Office of State and Local Government Coordination and Preparedness (OSLGCP). (2004a). *Draft national preparedness goal*. Washington, DC: Office of State and Local Government Coordination and Preparedness, Department of Homeland Security, September 2004.

Office of State and Local Government Coordination and Preparedness. (2004b). *Capabilities-based planning process: Explosives scenario prototype*. Washington, DC: Office of State and Local Government Coordination and Preparedness, Department of Homeland Security, October 2004.

Office of State and Local Government Coordination and Preparedness. (2004c). *Follow-up to capabilities workshop*. Washington, DC: Office of State and Local

Government Coordination and Preparedness, Department of Homeland Security, November 10, 2004.

Office of State and Local Government Coordination and Preparedness. (2004d). Letter to Homeland Security Partners. Washington, DC: Office of State and Local Government Coordination and Preparedness, Department of Homeland Security, December 17, 2004.

Office of State and Local Government Coordination and Preparedness. (2005a). *Interim national preparedness goal*. Washington, DC: Office of State and Local Government Coordination and Preparedness, Department of Homeland Security, March 31, 2005.

Office of State and Local Government Coordination and Preparedness. (2005b). *Universal task list 2.1*. Washington, DC: Office of State and Local Government Coordination and Preparedness, Department of Homeland Security, April 8, 2005.

Office of State and Local Government Coordination and Preparedness. (2005c). *Target capabilities list: Version 1.1*. Washington, DC: Office of State and Local Government Coordination and Preparedness, Department of Homeland Security, April 6, 2005.

Office of State and Local Government Coordination and Preparedness. (2005d). *National preparedness guidance*. Washington, DC: Office of State and Local Government Coordination and Preparedness, Department of Homeland Security, April 27, 2005.

Pogue, C. and A. Vallerand. (2003). "A conceptual model of military capabilities and an integrating functional architecture to facilitate military capability-based planning," proceedings, Summer Computer Simulation Conference, July 2-24, 2003, Montreal Canada: 230-243.

Radin, B. (2000). Intergovernmental relationships and the federal performance movement. *Publius: The Journal of Federalism,* Vol. 30 Nos. 1-2, Spring 2000: 143-158.

Schilling. D. (2004). Strategic intelligence to meet institutional planning needs of the twenty first century. Masters thesis. U.S. Army War College.

Schwartz, P. and J. Ogilvy. (1998). *Chapter 4: Plotting your scenarios*. In *Learning from the future: Competitive foresight scenarios*, ed. L. Fahey and R. M. Randall, 57-80. New York: John Wiley & Sons, Inc.

Spivak, S. and F. Brenner. (2001). *Standardization essentials: Principles and practices.* NY: Marcel Dekker.

Swiss, J. (1995). Performance monitoring systems. In D. N. Ammons (Ed.). *Accountability for performance: Measurement and monitoring in local government* (pp. 67-97). Washington, DC: International City/County Management Association.

Taylor, B. (2004). *Guide to capabilities-based planning*. Presentation to the Military Operations Research Capabilities-Based Planning Conference, Alexandria, VA (October 18-21, 2004).

The Technical Cooperation Program. (2004). *TTCP technical report: Guide to capability-based planning.* http://www.mors.org/meetings/cbp/cbp_presentations.htm (accessed October 19, 2004).

Treasury Board of Canada (2001). *Integrated risk management framework*, http://www.tbs-sct.gc.ca.

United Kingdom Ministry of Defence. (2004). *Delivering security in a changing world: Future capabilities.* Norwich, United Kingdom: The Stationary Office (July 2004).

United Kingdom Ministry of Defence. (2003). *Delivering security in a changing world: Supporting essays.* Norwich, United Kingdom: The Stationary Office (December 2003).

United States Government. (2005). *Analytical perspectives, budget of the United States government, fiscal year 2006.* Homeland Security Funding Analysis. Washington, DC: U.S. Government Printing Office.

The White House. (2003). *Homeland security presidential directive/Hspd-8*. Washington, DC: The White House (December 17, 2003).

Wholey, J. (2002). Making results count in public and nonprofit organizations: Balancing performance with other values. In K. Newcomer, E. T. Jennings, C. Broom, and Al Lomax (Eds.). *Meeting the challenges of performance-oriented government.* (pp. 13-35). Washington, DC: American Society for Public Administration/Center for Accountability and Performance.

Yim, R. and Caudle, S. (2004). Homeland security: Using standards to improve national preparedness. *ISO Management Systems*. *4*(1): 15-18.

Yim, R. (2003). *Homeland security: The need for national standards*. Testimony before the National Commission on Terrorist Attacks Upon the United States, November 19, 2003, Princeton, NJ.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, VA

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, CA

3. Norm Rabkin
   U.S. Government Accountability Office
   Washington, DC

4. Randall Yim
   Homeland Security Institute
   Analytical Services, Inc.
   Arlington, VA