
National Preparedness Guidance

Homeland Security Presidential Directive 8: *National Preparedness*



Homeland
Security

April 27, 2005

THIS PAGE INTENTIONALLY LEFT BLANK

PREFACE

I. The Transformation of Homeland Security

Fundamental to the mission of the U.S. Department of Homeland Security is the mitigation of threats, vulnerabilities, and consequences that stem from acts of terrorism, major disasters, and other emergencies. This is a shared responsibility and a shared commitment of Federal, State, local, and tribal governments, as well as the private sector. The Interim National Preparedness Goal (or Goal) summarizes the initial results of significant work completed since December 17, 2003, when President Bush issued Homeland Security Presidential Directive 8: *National Preparedness* (HSPD-8). This approach transforms how the Federal government proposes to strengthen the preparedness of the United States to prevent, protect against, respond to, and recover from terrorist attacks, major disasters, and other emergencies, and how the Federal government proposes to invest homeland security resources in order to achieve the greatest return on investment for our Nation's homeland security. It is animated by a sense of urgency and by a commitment to risk-based priorities.

II. What We Have Done So Far

The Interim Goal establishes the national vision and priorities that will guide our efforts as we set measurable readiness benchmarks and targets to strengthen the Nation's preparedness and should be utilized in conjunction with two planning tools:

- ***National Planning Scenarios:*** A diverse group of experts drafted a set of fifteen scenarios describing plausible terrorist attacks and natural disasters that would stretch the Nation's prevention and response capabilities. The objective was to develop the minimum number of credible, high-consequence scenarios needed to identify a broad range of prevention and response requirements. The set of fifteen scenarios, while not exhaustive, is meant to be representative of a broad range of potential terrorist attacks and natural disasters. Collectively, they yield core prevention and response requirements that can help direct comprehensive preparedness planning efforts. The Executive Summaries of the National Planning Scenarios can be viewed at <https://odp.esportals.com> or <https://www.llis.gov>.
- ***Target Capabilities List:*** The Target Capabilities List (TCL) is a set of thirty-six essential capabilities that should be developed and maintained, in whole or in part, by various levels of government to prevent, protect against, respond to, and recover from terrorist attacks and major disasters. This list was derived by utilizing the National Planning Scenarios to identify the critical tasks that would need to be performed across the fifteen scenarios. The TCL can also be viewed at <https://odp.esportals.com> or <https://www.llis.gov>.

III. Honoring the Principle of Federalism

An essential commitment of this undertaking was to ensure that the results were national products, not just Federal products. Of course, our country consists of thousands of sovereign governments who all play a part – some larger than others – in securing our homeland. As a result, we have

developed the Goal, National Planning Scenarios, and Target Capabilities in coordination with the heads of other appropriate Federal departments and agencies, in consultation with State, local, and tribal governments, and in partnership with the private sector and non-governmental organizations. Hundreds of entities and thousands of individuals at all levels of government, as well as people from outside the government, reviewed and contributed to the development of these documents. As we further refine the Goal and planning documents, we will continue to work closely with our Federal, State, local, tribal, private sector, and non-government stakeholders.

These documents are not micro-level plans that tell first responders or public officials how to do their work and execute their missions. These documents focus on the capabilities collectively needed to prevent, protect against, respond to, or recover from a terrorist attack or natural disaster. With that in mind, these documents are not intended to impose a specific array and number of assets on each community. Each governmental entity possesses varying levels of equipment, trained personnel, and resource tools – including mutual aid agreements – that can be used to deploy appropriate capabilities. Finally, these documents are not funding formulas. The documents do identify core capabilities we want to possess as a Nation and, therefore, will drive how we prioritize our Federal investments.

IV. The Road Ahead

Much work remains to be done to build upon these products. The National Preparedness Guidance includes detailed instructions on how communities can use the Interim Goal and a description of how the Interim Goal will generally be used in the future to allocate Federal preparedness assistance. Over the next several months, we will work closely with all of our stakeholders to identify the levels of capabilities that various types of jurisdictions should possess in order for the Nation to reach the desired state of national preparedness – knowing that our environment is constantly changing. Once the levels are identified, we will augment these documents to provide those recommended capability levels.

For Fiscal Year (FY) 2006, our focus initially will be on significantly improving performance relative to the seven National Priorities listed in the Interim Goal. These seven priorities are a limited number of the critical capabilities and cross-cutting initiatives that should drive near-term planning and resource allocation efforts. States and Urban Areas will develop addenda to update their Homeland Security Strategies. They will submit addenda through their established Federal reporting mechanisms, to reflect how they will address the seven National Priorities in order to receive further Federal preparedness assistance. For FY 2007, our focus will broaden to address other critical risk-based priorities within the thirty-six capabilities. States and Urban Areas will revise their Homeland Security Strategies and submit the fully updated strategies pursuant to the Final Goal in order to receive further Federal preparedness assistance. As we develop Federal assistance programs in FY 2006 and beyond, our focus will be to leverage our homeland security resources in order to achieve the highest possible readiness. To do that, we will utilize the information provided by States and Urban Areas to close the capability gap between where we are today and where we want to be tomorrow. We believe that this prioritized, capabilities-based approach will allow us to improve substantially our ability to prevent, protect against, respond to, and recover from a terrorist attack or natural disaster.

TABLE OF CONTENTS

1.0	INTRODUCTION.....	1
1.1	Background.....	1
1.2	Purpose.....	1
1.3	Value.....	2
2.0	CAPABILITIES-BASED PLANNING OVERVIEW	3
2.1	Stage 1: Defining Target Levels of Capability	5
2.2	Stage 2: Achieving Target Levels of Capability.....	10
2.3	Stage 3: Assessing Preparedness	13
3.0	NATIONAL PRIORITIES	15
3.1	Overarching Priorities.....	17
3.1.1	Implement the National Incident Management System & National Response Plan	17
3.1.2	Expanded Regional Collaboration	19
3.1.3	Implement the Interim National Infrastructure Protection Plan	23
3.2	Capability-Specific Priorities.....	27
3.2.1	Strengthen Information Sharing and Collaboration Capabilities.....	27
3.2.2	Strengthen Interoperable Communications Capabilities	30
3.2.3	Strengthen CBRNE Detection, Response, and Decontamination Capabilities.....	33
3.2.4	Strengthen Medical Surge and Mass Prophylaxis Capabilities	36
4.0	STANDARDS FOR ASSESSMENTS AND STRATEGIES.....	39
4.1	Preparedness Assessments.....	39
4.2	Preparedness Strategies Addendum.....	43
4.3	Schedule.....	44
5.0	PRIVATE AND NON-GOVERNMENTAL ENTITIES AND CITIZENS.....	45
5.1	Private Sector.....	45
5.2	Non-Governmental Organizations.....	46
5.3	Citizens	47
6.0	ANNUAL STATUS REPORTS.....	49
7.0	CONCLUSION	50
	APPENDIX A—TERMS AND DEFINITIONS.....	A-1
	APPENDIX B—ACRONYMS AND ABBREVIATIONS	B-1
	APPENDIX C—NATIONAL PREPAREDNESS IMPLEMENTATION TIMELINE.....	C-1
	APPENDIX D—REQUIREMENTS CHECKLISTS.....	D-1

LIST OF FIGURES

Figure 1:	Defining Target Levels of Capability.....	3
Figure 2:	Achieving Target Levels of Capability	4
Figure 3:	Assessing Preparedness.....	4
Figure 4:	Target Capabilities	7
Figure 5:	Elements of Capability	8
Figure 6:	Priority/Capability Matrix	16
Figure 7:	Notional Capability Worksheet.....	41
Figure 8:	Schedule for Preparedness Assessments and Strategies.....	44

Questions, comments, and suggested improvements related to this document are encouraged.
Inquiries, information, and requests for additional copies should be submitted to:

U.S. Department of Homeland Security
Office of State and Local Government Coordination and Preparedness
(ATTN: Office for Policy, Initiatives, and Analysis)
810 7th Street, NW
Washington, DC 20531

The National Preparedness Guidance will be made available on the
Office for Domestic Preparedness (ODP) Secure Portal (<https://odp.esportals.com>)
and the Lessons Learned Information Sharing system (<https://www.llis.gov>).

For more information on HSPD-8 implementation, go to
<http://www.ojp.usdoj.gov/odp/welcome.html>

1.0 INTRODUCTION

1.1 Background

The homeland security challenges of the 21st century require a coordinated national approach to national preparedness. To address these challenges, the President issued Homeland Security Presidential Directive 8 (HSPD-8) on December 17, 2003. HSPD-8 directs the Secretary of Homeland Security to coordinate the development of an all-hazards National Preparedness Goal (the Goal) that establishes measurable priorities, targets, standards for preparedness assessments and strategies, and a system for assessing the Nation's overall level of preparedness. The Department of Homeland Security (DHS) issued an Interim Goal on March 31, 2005, that reflects the Department's progress to date to develop each of those elements in coordination with other entities. It will remain in effect until superseded by the Final National Preparedness Goal on October 1, 2005.

The vision for the Interim Goal 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.

1.2 Purpose

The National Preparedness Guidance is a companion document to the Interim National Preparedness Goal that provides instructions and guidance on how to implement the Goal. National Preparedness Guidance will be reissued periodically as needed to reflect changes in the National Priorities and/or further development of the Capabilities-Based Planning process and tools.

The Guidance supplements but does not supplant existing Federal planning guidance. This document provides:

- A summary of the Interim Goal;
- An explanation of how existing requirements will support achievement of the Interim Goal;
- A step-by-step explanation of Capabilities-Based Planning and how it supports achievement of the Interim Goal;
- An introduction to the National Planning Scenarios, including the purpose, user instructions, and proposed future modifications;
- An introduction to the Universal Task List (UTL), including the purpose, user instructions, and proposed future modifications;

-
- An introduction to the Target Capabilities List (TCL), including the purpose, user instructions, and proposed future modifications;
 - A description of each of the National Priorities;
 - An explanation of standards for assessments and strategies including templates and instructions for self-assessments and amendment of strategies; and
 - An integrated timeline for HSPD-8 Implementation.

1.3 Value

The National Preparedness Guidance is a source of information, instructions, and examples to assist Federal, State, local, and tribal entities in implementing the Interim Goal with their private and non-governmental partners and the general public. Implementing the Goal will greatly improve our Nation's ability to prevent, protect against, and, if necessary, respond to, and recover from major events or Incidents of National Significance, as defined in the National Response Plan (NRP). This will provide important first steps for homeland security stakeholders to take during FY 2005, the first year of HSPD-8 implementation.

The Interim Goal and companion Guidance will be implemented through a coordinated national approach that provides many benefits, including:

- *A new system to assess progress, manage risk, and determine the return on the national investment in preparedness* – The Guidance outlines a new framework that ties objectives and priorities to explicit metrics and provides the means to assess progress.
- *More effective use of resources* – In making preparedness investments to build capabilities that address existing capability gaps and deficiencies, resource allocation will more effectively manage risk, thereby improving the Nation's overall level of preparedness with the least cost to the economy and our way of life.
- *Improved decision-making at all levels* – Data never before available will be readily accessible to decision makers at all levels. This information will support the decision making critical to prioritizing needs and helping to ensure the best use of available resources.
- *Streamlined data collection* – Coordinated national requirements in the form of target capabilities and priorities will make it easier to streamline the collection of preparedness information.
- *Greater understanding of national preparedness* – The greatest benefit of this collaborative approach will be a comprehensive picture of preparedness at the Federal, State, local, tribal, and private sector levels that will effectively harness interdependencies or synergies between these entities.

2.0 CAPABILITIES-BASED PLANNING OVERVIEW

Strengthening the preparedness of the Nation requires revisiting our traditional approaches to defining and addressing preparedness requirements through planning. Capabilities-Based Planning is defined as planning, under uncertainty, to provide capabilities suitable for a wide range of threats and hazards while working within an economic framework that necessitates prioritization and choice. It helps to inform and optimize decision making at all levels of government by linking resource allocation to the capabilities that are most urgently needed to perform a wide range of assigned missions and tasks.

Capabilities-Based Planning involves a 10-step process, accomplished in three stages: 1) a national effort to define readiness targets for the Nation; 2) individual efforts to determine where each level of government and each group of jurisdictions organized by Tier across the country stands against those national targets, and 3) a national effort to assess preparedness, compile the assessment data into an annual report, and set national priorities. The process illustrated in Figures 1, 2, and 3 represents the comprehensive Capabilities-Based Planning methodology. Beginning at Section 2.1, specific near-term requirements to support the Interim National Preparedness Goal are identified in each step.

The first stage of the Capabilities-Based Planning process is “*Defining Target Levels of Capability*” (see Figure 1). The steps included in this stage will be performed at a national level. DHS, as the coordination lead, will involve Federal, State, local, and tribal entities and their private and non-governmental partners and the general public in the iterative development of the planning tools, which include:

- National Planning Scenarios.
- Universal Task List (UTL).
- Target Capabilities List (TCL).

Figure 1: Defining Target Levels of Capability

STAGE 1 - Defining Target Levels of Capability	
A Shared National Responsibility	
1. What should we prepare for?	The <i>National Planning Scenarios</i> highlight the scope, magnitude, and complexity of plausible catastrophic terrorist attacks, major disasters, and other emergencies.
2. What tasks need to be performed?	The <i>Universal Task List (UTL)</i> provides a menu of tasks that may be performed in major events such as those illustrated by the National Planning Scenarios.
3. Which tasks are critical?	<i>Critical Tasks</i> derived from the UTL, with associated conditions and performance standards, provide the foundation for developing measurable readiness targets and for the design and conduct of training and exercises.
4. What capabilities are needed to perform the critical tasks?	The <i>Target Capabilities List (TCL)</i> identifies the capabilities required to perform the critical tasks identified in the UTL.

5. What level of capability is needed for a major event?	The TCL will define the risk-based target levels of capability for major events.
6. How do we share responsibility to develop and maintain capabilities?	The TCL will apportion the risk-based target levels of capability among levels of government and groupings (or <i>Tiers</i>) of jurisdictions.

The second stage of the Capabilities-Based Planning process is “*Achieving Target Levels of Capability*” (see Figure 2). Federal, State, local, and tribal entities will perform these steps to determine what capabilities are required, what capabilities they currently have and need, and how to plan and allocate resources to build and maintain capability.

Figure 2: Achieving Target Levels of Capability

STAGE 2 - Achieving Target Levels of Capability	
Responsibility of Individual Levels of Government and Groups of Jurisdictions Organized by Tier	
7. What capabilities are required?	The TCL will identify the appropriate target levels of capability for each level of government and Tier.
8. Do we have adequate capabilities?	Entities at all levels of government will compare their current levels of capability to the target levels to identify capability gaps, excesses, and deficiencies.
9. How should we allocate our resources to make the greatest improvements in preparedness?	Entities at all levels of government will <i>assess needs, update preparedness strategies, and allocate resources</i> to address capability gaps and make the greatest improvements in preparedness.

The third stage of the Capabilities-Based Planning process consists of one step – “*Assessing Preparedness*” (see Figure 3). This step, led by DHS, is performed at a national level with all levels of government contributing. DHS is responsible for aggregating assessment data from all levels of government to understand the overall level of preparedness of the Nation.

Figure 3: Assessing Preparedness

STAGE 3 - Assessing Preparedness	
A Shared National Responsibility	
10. How prepared are we?	Capabilities will be demonstrated through <i>performance assessments</i> . Increases or shortfalls in national preparedness will be documented and communicated through comprehensive assessments and reports.

2.1 Stage 1: Defining Target Levels of Capability

A Shared National Responsibility

Step 1 – What Should We Prepare For?

In a world of evolving threat and terrorist tactics, it is not possible to identify the exact events for which we need to be prepared at any and every given time. Instead, utilizing a Capabilities-Based Planning process enables the identification of capabilities that will enable us to prevent, respond to, and recover from any major event. The National Planning Scenarios present a standardized set of plausible scenarios for major events or Incidents of National Significance and provide the foundation for development of capability requirements. The scenarios define a broad range of representative threats and hazards. It is not feasible or realistic to design scenarios to address every possible threat or hazard. The intent is to provide the minimum number of representative scenarios necessary to identify target capabilities. The list is not meant to be exhaustive, predictive, or prescriptive. The National Planning Scenarios provide the basis for defining tasks and the capabilities required to perform them.

Toolkit

The National Planning Scenarios describe the potential scope and magnitude of plausible major events that require coordination among various jurisdictions and levels of government.

- Scenario 1: Improvised Nuclear Device
- Scenario 2: Biological Attack – Aerosol Anthrax
- Scenario 3: Biological Disease Outbreak – Pandemic Influenza
- Scenario 4: Biological Attack – Plague
- Scenario 5: Chemical Attack – Blister Agent
- Scenario 6: Chemical Attack – Toxic Industrial Chemicals
- Scenario 7: Chemical Attack – Nerve Agent
- Scenario 8: Chemical Attack – Chlorine Tank Explosion
- Scenario 9: Natural Disaster – Major Earthquake
- Scenario 10: Natural Disaster – Major Hurricane
- Scenario 11: Radiological Attack – Radiological Dispersal Devices
- Scenario 12: Explosives Attack – Improvised Explosive Device
- Scenario 13: Biological Attack – Food Contamination
- Scenario 14: Biological Attack – Foreign Animal Disease (Foot and Mouth Disease)
- Scenario 15: Cyber Attack

Not all scenarios apply to every jurisdiction. Scenarios may be tailored to local conditions. Jurisdictions should identify other possible threats and hazards. The scenarios will be used for the near-term planning and resource allocation efforts identified in Section 2.2, centering on the seven capabilities linked to the four Capability-Specific National Priorities of the Interim Goal.

Responsibilities:

- **DHS** – DHS is responsible for maintaining the National Planning Scenarios.
- **Federal, State, Local, and Tribal** – Entities at all levels of government should use the National Planning Scenarios as a reference to help them evaluate and improve their capabilities to perform their assigned missions and tasks in major events.

Step 2 – What Tasks Need to be Performed?

To build the right mix of capabilities for the full range of major events we face, it is important to understand what tasks need to be performed, under what operating conditions, and to what national standards. The UTL is a menu of tasks for major events like those illustrated by the National Planning Scenarios. The UTL defines *what* tasks need to be performed to prevent, protect against, respond to, and recover from major events. The UTL does not address *who* performs a task or *how* to perform a task; those issues are addressed in operational policies, plans, and procedures.

Federal, State, local, and tribal entities refer only to those tasks from the UTL that apply to their assigned missions. The UTL provides the means to ensure that training and exercises address proficiency in tasks that are associated with the seven capabilities linked to the four Capability-Specific National Priorities.

Toolkit
The Universal Task List, Version 2.1 is available on the ODP Secure Portal (<https://odp.esportals.com>) and Lessons Learned Information Sharing Network (<https://www.llis.gov>).

Step 3 – Which Tasks are Critical?

Critical tasks are defined in the UTL as those prevention, protection, response, and recovery tasks that require coordination among an appropriate combination of Federal, State, local, tribal, private sector, and non-governmental entities during a major event in order to minimize the impact on lives, property, and the economy. Critical tasks, with associated conditions and performance standards, provide the foundation for developing target levels of capability.

Step 4 – What Capabilities are Required to Perform the Critical Tasks?

The Target Capabilities List (TCL) was developed with Federal, State, local, and tribal subject matter experts. The TCL identifies capabilities required to perform the critical tasks described in Step 3.

Version 1.1 of the TCL identifies 36 essential capabilities (see Figure 4). A capability provides a means to perform one or more critical task(s) under

Toolkit
The Capability Summaries contained in the Target Capabilities List describe the capability and associated outcome required to perform the critical tasks.

The initial version is available on the ODP Secure Portal (<https://odp.esportals.com>).

specified conditions and to specific performance standards. A capability may be delivered during an emergency with any combination of elements that achieves the desired outcome, namely properly planned, organized, equipped, trained, and exercised personnel (see Figure 5). Each capability in the TCL is documented in a Capability Summary. The Capability Summaries are specific enough to enable entities to evaluate alternative combinations of elements required to perform the critical tasks but general enough so as not to prejudice decisions in favor of a specific combination. This step defines the outcome for each capability.

- Responsibilities:**
- **DHS** – DHS, in coordination with stakeholders, is responsible for development and maintenance of the UTL and critical tasks.
 - **Federal** – Federal departments and agencies should use the UTL as a reference to develop homeland security training, exercises, and preparedness assistance programs.
 - **Federal, State, Local, and Tribal** – Entities at all levels of government should use the UTL as a reference to develop proficiency through training and exercises for the critical tasks that they will be required to perform in major events.

Figure 4: Target Capabilities



★ Linked to the four Capability-Specific National Priorities

Figure 5: Elements of Capability

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 guidelines necessary to perform assigned missions and tasks.
Equipment and Systems	Major items of equipment, supplies, facilities, and communication systems that comply with relevant equipment 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.

Step 5 – What Level of Capability is Needed for a Major Event?

Conditions and performance standards can vary significantly across events. This step involves a review of the Capability Summaries across the planning scenarios to examine the levels of capability required from all sources (Federal, State, local, and tribal) to achieve the desired outcomes. From the scenario specific list, a DHS-led working team will develop the final list of levels for each capability so that each Tier possesses a single level for each capability (i.e., each Tier will have one level for each capability). The impact of major events varies, so the level of capability needed to manage a major event varies as well, which is why identifying a minimum level per Tier per capability will provide the flexibility to address the unforeseen and unknowable. This step involves a comprehensive analysis to determine what level of capability (amount and proficiency) should be achieved and sustained from all sources to best manage the risks posed by major events. Many capabilities are common to all major events. The determination of the appropriate level of capability from all sources is made with the understanding that, in a resource-constrained environment, the level of capability will likely not be the highest level required for every potential major event. Hence, the final capability levels for each Tier will include a single level for each capability so that we achieve a collective minimum level of capability across the 36 capabilities to effectively prevent, respond to, and recovery from a major event.

Step 6 – How Do We Share Responsibility to Develop and Maintain Capabilities?

Capabilities may take years to develop. The need to build national capabilities for major events such as those illustrated by the National Planning Scenarios require us to share responsibility, through expanded regional collaboration and other means, to reduce or eliminate risk. In assigning levels of capability, DHS and its Federal, State, local, and tribal partners will determine how to apportion responsibility to develop and maintain capabilities among levels of government and groups (or Tiers) of jurisdictions.

Toolkit

DHS will continue to work with Federal, State, local, tribal, private sector, and non-governmental subject-matter experts to update the TCL for reissuance on October 1, 2005. The updated TCL will define levels of capability that will be apportioned among levels of government and assigned to Tiers.

Responsibility to develop and maintain levels of capability will be apportioned among Federal, State, local, and tribal governments based on their statutory authorities, roles, and responsibilities. In apportioning requirements, consideration will be given to factors such as the nature of the specific event, required response time, cost to acquire and maintain, projected frequency of use, degree of specialization, and need for lead time for research and development. HSPD-8 states that *“Federal preparedness assistance will support State and local entities’ efforts including planning, training, exercises, interoperability, and equipment acquisition for major events as well as capacity building for prevention activities such as information gathering, detection, deterrence, and collaboration related to terrorist attacks. Such assistance is not primarily intended to support existing capacity to address normal local first responder operations, but to build capacity to address major events, especially terrorism.”*

HSPD-8 also states that *“specialized Federal assets such as teams, stockpiles, and caches shall be maintained at levels consistent with the National Preparedness Goal and be available for response activities as set forth in the National Response Plan (NRP), other appropriate operational documents, and applicable authorities or guidance. Relevant Federal regulatory requirements should be consistent with the National Preparedness Goal.”*

The TCL is not one size fits all. Both the risk and the resource base vary considerably among jurisdictions across the United States. Accordingly, the TCL will be organized by Tiers, or groupings of jurisdictions. Tiers account for reasonable differences in target levels of capability (or system-specific elements of capability) among groups of jurisdictions. Tiers will also foster mutual aid among neighboring jurisdictions. State, local, and tribal officials will be able to group jurisdictions and assign them to standardized set of Tiers that best match their group scores on the risk factors, such as total population, population density, resource base, and critical infrastructure. Interstate groups will be encouraged where appropriate. States typically organize their jurisdictions into sub-State regional groupings that cover the entire State. Federal preparedness assistance will help to build and maintain the capability for assigned Tiers. This approach will help to build a national network of mutual aid.

Responsibilities:

- **DHS** – DHS is responsible for coordinating development and maintenance of the TCL including setting the risk-based target levels of performance required for each capability and assigning them to Tiers and levels of government. DHS is also responsible for coordinating the continual refinement of the Tier System.
- **Federal** – Federal departments and agencies should apply the TCL in applicable training, exercise, and preparedness assistance programs. Federal departments and agencies will also be responsible for developing and maintaining their target levels of capabilities.
- **State, Local, and Tribal** – Entities at all levels of government should use the TCL to help them understand what capabilities are needed to perform their homeland security missions and what levels of capabilities they are being asked to develop and maintain.

2.2 Stage 2: Achieving Target Levels of Capability

Responsibility of Levels of Government and Groups of Jurisdictions Organized by Tier

Capabilities-Based Planning process requires a *collaborative, region-wide effort*. The National Priority on Expanded Regional Collaboration addresses regional structures and expanded collaboration (see Section 3.1.2).

The purpose of the Capabilities-Based Planning methodology is to produce a prioritized list of required capabilities or capability elements, and a risk determination. This is accomplished through identification of capability gaps, excesses, and deficiencies against each applicable National Planning Scenario, and collectively across scenarios, beginning with the seven capabilities linked to the four Capability-Specific National Priorities.

Risk determinations should address three fundamental questions:

- *Can the assigned mission(s) and task(s) be accomplished to the required level of proficiency and are capabilities sufficient to provide a reasonable assurance of success against the specified scenario?*
- *What are the potential risks? (e.g., to lives, property, and the economy)*
- *What is the impact on planning? (e.g., address the gap through mutual aid agreements and/or pre-negotiated language for an initial request for Federal assistance)*

Step 7 – What Capabilities Are Required?

The TCL provides guidance on the specific capabilities identified in the Interim Goal. The final National Preparedness Goal will provide on the specific levels of capability that Federal departments and agencies and the States will be expected to develop and maintain (based on the work to be completed by October 1, 2005, for the steps in Stage 1). States will allocate Federal

preparedness assistance to regions and their jurisdictions to help meet the target level of capability for their Tier.

The goal of the state working group or team is to develop a prioritized list of capabilities or capability elements –specific to that state -- and a risk determination for the seven capabilities linked to the four Capability-Specific National Priorities. The seven capabilities will be reviewed across the National Planning Scenarios (described in step 1) applicable to the entity (e.g., the hurricane scenario only applies to certain regions of the Nation) to identify specific requirements for capability elements (e.g., planning, training, equipment, exercises). The working group or team should consider how the threat or hazard would develop and impact their region, and set priorities accordingly. Starting with the chronology and consequences depicted in the National Planning Scenarios, the working group or team can analyze the threat or hazard’s regional impact and determine what actions and resources (capability elements) will be required for the four capability-specific National Priorities. As specified in the Fiscal Year 2005 Homeland Security Grant Program Guidelines, in FY 2005, the working group or team will identify specific requirements for the Improvised Explosive Device (IED) scenario¹ and those related to the seven capabilities linked to the four Capability-Specific National Priorities.

The comprehensive determination of requirements and risk establishes a relative priority for a capability or capability element, which can then be matched to available assistance and resources by the team or working group or through Senior Advisory Committees (established under the FY 2005 State Homeland Security Grant Program) that coordinate preparedness assistance grant funding from Federal sources. This is particularly important since it may take several years to develop capabilities to the appropriate target levels, and this methodology allows capability building to be programmed over several annual increments.

A requirement for Federal preparedness assistance for the seven capabilities linked to the four Capability-Specific National Priorities will be validated by ensuring the need cannot be compensated for using other means; that it poses an unacceptable risk or prevents affirmatively responding to the three risk determination questions; or will result in a significant decrease in flexibility and thus unacceptably increase vulnerability. Unmet needs should also first be evaluated to identify no cost or low cost “*non-materiel*” solutions, such as changes to policy or procedures.

The seven capabilities linked to the four Capability-Specific National Priorities all require regional integration and interoperability. To ensure interoperability among these capabilities, planners should identify key interfaces and resolve applicable standards. Key interfaces are defined as those operational relationships that span organizational boundaries, are mission critical, and are difficult or complex to manage. Key interfaces include the exchange of any critical “*commodity*” (e.g., mutual aid, personnel). Once identified, regional decision-makers

¹ As specified in the *Fiscal Year 2005 Homeland Security Grant Program: Program Guidelines and Application Kit* (p. 50), each urban area or multi-jurisdictional metropolitan area or region receiving FY05 UASI [Urban Area Security Initiative] funds “must develop a multi-jurisdictional prevention and response plan based on the IED scenario and test their integrated plan(s) through a cycle of exercise activity . . . that addresses the associated tasks as outlined in the IED scenario.”

should set standards that regulate the exchange of the commodity in their mutual aid agreements or assistance compacts.

Step 8 – Do We Have Adequate Capabilities?

Near term planning and resource allocation efforts will center on the seven capabilities linked to the four Capability-Specific National Priorities. States and Urban Areas are required to develop addenda to their Homeland Security Strategies and submit them by September 30, 2005, to reflect how they will address the seven National Priorities in order to be eligible to receive Federal preparedness assistance in FY 2006.

Toolkit
The process for conducting initial capability assessments and highlights of the needs assessment process are described in Section 4.

In FY 2007, the focus will broaden to address other capabilities from the TCL. Entities at all levels of government will compare their current capabilities to the target levels of capability identified in the TCL. These assessments will identify capability gaps and deficiencies and, therefore, risk. When these capability assessments are completed, they will provide a national assessment of net capacity, needs, and projections of strategic risk. As a result of performing the capabilities assessment, resource needs will be identified and quantified. States will then prioritize these needs based on various factors, including threats, vulnerabilities, consequences, risk, and cost/benefit analysis.

- Responsibilities:**
- **DHS** – DHS is responsible for coordinating development of the capability and needs assessment processes. The DHS capability assessment will begin with a representative sample of States/sub-State regions with a comprehensive capabilities assessment process to be deployed in future years.
 - **Federal** – All Federal departments and agencies are responsible for assessing whether they possess required capabilities for agency functions, and whether their State, local, and tribal preparedness programs are supporting the achievement of target capabilities
 - **State, Local, and Tribal** – Entities at all levels of government will ultimately be required to assess capabilities against targets and define needs in manner consistent with their identified and prioritized gaps.

Step 9 – How Should We Allocate Our Resources to Make the Greatest Improvements in Preparedness?

In this step, entities at all levels of government will be asked to define their own priorities for their preparedness strategies and allocate resources to address specific gaps, excesses, and deficiencies. The Goal explicitly states that the National Capabilities-Based Planning tools: “*are not*

Toolkit
Initial requirements for updating State and Urban Area strategies are included in Section 4.

micro-level plans that tell first responders or public officials how to do their work and execute their missions” and “these documents are not intended to impose a specific array and number of assets on each community. Each governmental entity possesses varying levels of equipment, trained personnel, and resource tools -- including mutual aid agreements -- that can be used to deploy appropriate capabilities.” The needs assessment, beginning in the near term with the capability elements for the seven capabilities linked to the four Capability-Specific National Priorities, drives the development of preparedness strategies for Federal, State, local, Urban Area, and tribal entities. The Interim Goal requires that existing strategies be amended by October 1, 2005, to demonstrate alignment with the National Preparedness Goal. DHS will coordinate review and validation of these strategies to ensure that they meet the identified needs and align with the National Preparedness Goal. States and Urban Areas must meet this requirement before they can receive preparedness funding. The capability assessments and updated strategies form a framework to identify where to best apply Federal preparedness resources.

Responsibilities:

- **DHS** – DHS is responsible for coordinating issuance of guidance on the development of all-hazards State Homeland Security Strategies and coordinating Federal review and approval.
- **Federal** – HSPD-8 requires that to the extent permitted by law, Federal preparedness assistance will be predicated on adoption of all-hazards State Homeland Security Strategies.
- **State, Local, and Tribal** – As described in Section 4, States and Urban Areas, in consultation with local and tribal entities, are responsible for updating existing strategies.

2.3 Stage 3: Assessing Preparedness

A Shared National Responsibility

Step 10 – How Prepared Are We?

The Capabilities-Based Planning methodology and associated tools provide the foundation for improving the Nation’s overall level of preparedness. Entities at all levels of government

will demonstrate performance of capabilities through exercises and actual events. After Action Reports and corrective action plans will highlight and address capabilities and tasks in need of improvement. Compliance information will be captured to ensure that capability development and execution of tasks are being done in accordance with applicable requirements, such as the National Incident Management System (NIMS).

Toolkit

The process for collecting performance information is described briefly in Section 4. Further explanations of performance assessments will be included in updated versions of the Homeland Security Exercise Evaluation Program (HSEEP) and other applicable guidelines.

Progress in improving our overall national level of preparedness will be documented and communicated through preparedness assessments and reports. These will assist decision makers at all levels of government in ensuring that the appropriate balance has been achieved in allocating resources to strengthen specific capabilities prioritized in light of the potential risk posed by terrorist attacks, major disasters, and other emergencies.

In summary, Capabilities-Based Planning provides the means for the Nation to answer three fundamental questions: “*How prepared do we need to be?*”, “*How prepared are we?*”, and “*How do we prioritize efforts to close the gap?*”

Responsibilities:

- **DHS** – DHS is responsible for coordinating issuance of detailed guidance on performance assessments. Additionally, in accordance with HSPD-8, DHS is responsible for submitting to the President an annual status report on the Nation's level of preparedness, including State capabilities, the readiness of Federal civil response assets, the utilization of mutual aid, and an assessment of how the Federal first responder preparedness assistance programs support the Goal. The first report will be provided on April 1, 2006.
- **Federal** – Federal departments and agencies will be responsible for providing input into the annual status report and where applicable participating in national exercises to evaluate performance. Federal departments and agencies will also be responsible for updating their preparedness assistance programs to support achievement of the Goal.
- **State, Local, and Tribal** – Entities at all levels of government will ultimately be required to assess performance through the process described in exercise or other guidance. Leveraging the findings of these assessments, decision makers at all levels of government will be responsible for utilizing the results of preparedness reporting to guide future investments of preparedness funds.

3.0 NATIONAL PRIORITIES

HSPD-8 requires the establishment of “*measurable readiness priorities ... that appropriately 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.*” The Nation cannot immediately achieve all of the target capabilities identified for the Interim Goal. Accordingly, the Interim Goal provides National Priorities to guide the Nation’s preparedness efforts to meet the most urgent needs.

DHS established the National Priorities in consultation with homeland security stakeholders, based on review of national strategies, HSPDs, and State and Urban Area Homeland Security Strategies. The priorities have been identified based on their relevance to national strategic objectives and their utility in terms of high payoff contributions to national readiness. The priorities fall into two categories: overarching priorities that contribute to the development of multiple capabilities and capability-specific priorities that build selected capabilities from the TCL for which the Nation has the greatest need.

The National Priorities are the following:

Overarching Priorities

- **Implement the National Incident Management System and National Response Plan**
- **Expanded Regional Collaboration**
- **Implement the National Infrastructure Protection Plan**

Capability-Specific Priorities

- **Strengthen Information Sharing and Collaboration Capabilities**
- **Strengthen Interoperable Communications Capabilities**
- **Strengthen CBRNE Detection, Response, and Decontamination Capabilities**
- **Strengthen Medical Surge and Mass Prophylaxis Capabilities**

As shown in Figure 6 below, each of the seven National Priorities can be tied to one or more of the target capabilities. The Overarching Priorities will contribute to more consistent national preparedness efforts in support of:

- HSPD-5, which directed establishment of the NIMS and NRP,
- HSPD-7, which directed establishment of the National Infrastructure Protection Plan (NIPP), and
- HSPD-8, which directed establishment of the National Preparedness Goal and national programs and systems to support the Goal.

The Capability-Specific Priorities are directly linked to capabilities from the TCL. By concentrating on the development of target capabilities linked to the National Priorities, government entities will be able to manage risk through a prioritization of efforts aimed at building capabilities that are most urgently needed. As entities at all levels begin to conduct baseline capability assessments (as described in Step 8 of the Capabilities-Based Planning process), they should refer to the Capability Templates in the TCL for those target capabilities. These “linked” capabilities will help answer the question in Step 7: *What Capabilities Are Required?* The Capability Measures, Performance Measures, and Capability Elements used in the Capability Templates should be used as a guide toward the achievement of the National Priorities and will help answer the question in Step 8: *Do We Have Adequate Capabilities?*

Figure 6: Priority/Capability Matrix

OVERARCHING PRIORITIES	TARGET CAPABILITIES
Implement the National Incident Management System and National Response Plan	Applies to All 36 Capabilities
Expanded Regional Collaboration	Applies to All 36 Capabilities
Implement the National Infrastructure Protection Plan	Applies to: 5: Critical Infrastructure Protection 14: Food and Agriculture Safety and Defense 15: Information Collection and Threat Recognition 16: Information Sharing and Collaboration 17: Intelligence Fusion and Analysis 29: Risk Analysis
CAPABILITY-SPECIFIC PRIORITIES	TARGET CAPABILITIES
Strengthen Information Sharing and Collaboration Capabilities	Applies to: 16: Information Sharing and Collaboration
Strengthen Interoperable Communications Capabilities	Applies to: 18: Interoperable Communications
Strengthen CBRNE Detection, Response, and Decontamination Capabilities	Applies to: 2: CBRNE Detection 11: Explosive Device Detection and Response Operations 35: WMD/Hazardous Materials Response and Decontamination
Strengthen Medical Surge and Mass Prophylaxis Capabilities	Applies to: 21: Mass Prophylaxis 23: Medical Surge

3.1 Overarching Priorities

3.1.1 Implement the National Incident Management System & National Response Plan

Rationale

HSPD-5, “*Management of Domestic Incidents*,” mandated the creation of the National Incident Management System (NIMS) and National Response Plan (NRP). The NIMS (released in March 2004) provides a consistent framework for entities at all jurisdictional levels to work together to manage domestic incidents, regardless of cause, size, or complexity. The NRP (released in December 2004), using NIMS, is an all-discipline, all-hazards plan that provides the structure and mechanisms to coordinate operations for evolving or potential Incidents of National Significance. NIMS provides a nationwide template enabling Federal, State, local, and tribal governments, the private sector, and nongovernmental organizations to work together effectively and efficiently to prepare for, prevent, respond to, and recover from domestic incidents regardless of cause, size or complexity. The NRP in turn enhances preparedness by defining the roles of Federal, State, local, and tribal governments, as well as non-governmental organizations.

The principles of NIMS, including guidelines for command and management (including the Incident Command System, multi-agency coordination systems, and public information systems), preparedness (including planning, training, exercises, qualification and certification, equipment acquisition and certification, and publications management), resource management, communications and information management, and supporting technologies all contribute to developing target capabilities at the Federal, State, local and tribal levels. Compliance with the NIMS and compatibility with the NRP contribute to preparing for all capabilities.

The NIMS Integration Center is responsible for promoting awareness and integration of NIMS principles into all levels of government, as well as implementing the NRP. In order to prepare for potential Incidents of National Significance, it is essential that all personnel involved in homeland security fully understand the NIMS principles and use them during their everyday activities. NIMS principles need to be included in emergency operations plans and Federal preparedness grant proposals, as well as other documents dealing with Federal, State, local, and tribal preparedness. To the extent authorized by law, incident management and emergency response plans must include the following elements:

- Principles and terminology of the NIMS;
- Incident Information Reporting requirements of the NRP;²
- Linkages to key NRP organizational elements; and
- Procedures for transitioning from localized incidents to Incidents of National Significance.

² Federal, State, tribal, private-sector, and non-governmental organization emergency operations centers are either required or encouraged to report incident information to the DHS Homeland Security Operations Center (HSOC) as described in the National Response Plan (NRP) on page 46.

Linked Capabilities

All capabilities in the TCL are linked to this overarching National Priority. Elements of capability (including personnel, planning, organization and leadership, equipment and systems, training, and exercises, evaluations, and corrective actions) are all consistent with guidelines, protocols, and standards defined for NIMS.

Federal, State, Local, and Tribal Responsibilities

Beyond awareness of NIMS principles by first responders and emergency management officials at all levels of government, responsibilities for Federal, State, local, and tribal officials include:

Responsibilities:

- **DHS** – Responsible for coordinating the development and maintenance of the NIMS and NRP.
- **Federal** – Responsible for incorporating key NIMS and NRP concepts and procedures for working with NRP organizational elements when developing or updating incident management and emergency response plans.
- **State, Local and Tribal** – Jurisdictions receiving Federal funds should incorporate NIMS and NRP into existing training efforts. Local incident command systems should be fully-compliant with the NIMS-approved Incident Command System, enabling jurisdictions to work together smoothly following an incident.

Further Information

The NIMS can be found online at:

http://www.fema.gov/pdf/nims/nims_doc_full.pdf

The NRP can be found online at:

http://www.dhs.gov/interweb/assetlibrary/NRP_FullText.pdf

Additional information can be found online at:

<http://www.fema.gov/nims/>

3.1.2 Expanded Regional Collaboration

Rationale

Because major events will undoubtedly have a regional impact, there is no greater necessity than to collaborate on a regional basis to leverage expertise, share specialized assets, enhance capacity, and interoperate cohesively and effectively. Expanded Regional Collaboration supports the development of a seamless, national network of mutually-supporting capabilities to prevent, protect against, respond to, and recover from the full spectrum of threats and hazards.

Risk management principles reinforce the central observation that homeland security fundamentally depends on the commitment to secure those areas that are of the highest interest to our enemies and of the highest concern to the Nation. To date, DHS has identified and designated 57 of those areas through the Urban Areas Security Initiative (UASI).³ Initial activities under this priority focus on expanding regional collaboration associated with designated UASI Urban Areas, as well as designated multi-jurisdictional metropolitan areas identified by those States that do not have a UASI Urban Area.⁴ These are the first steps in a larger process to expand regional collaboration in all areas of the U.S.

The Department of Health and Human Services (HHS), through the Centers for Disease Control (CDC), will continue to pilot the Cities Readiness Initiative. This initiative, begun in FY 2004, targets 21 selected cities to ensure that they are prepared to provide oral medications to 100 percent of the population in case of a catastrophic terrorist attack for which pharmaceutical countermeasures are required. Response in a timely manner is of utmost importance, particularly in the case of the agent *Bacillus anthracis*, the organism that causes anthrax. In this case, antibiotics must reach the population within 24 to 48 hours to have the greatest life saving effect. This will be accomplished by the tiering of Federal, State, and local capabilities, each of which has a role in the integration of maintaining, deploying, receiving, and distributing life saving medication.⁵

Linked Capabilities

“Expanded Regional Collaboration” is an overarching priority that contributes to the development of all 36 capabilities in the TCL. This priority is a necessary precursor to the application of the Capabilities-Based Planning process (particularly the Tier System), and facilitates effective planning, resource allocation, and execution of capabilities required for major events.

³ See: http://www.ojp.usdoj.gov/odp/grants_programs.htm#fy05hsgp

⁴ The DHS FY 2005 Homeland Security Grant Program Guidance has several requirements specific to “each Urban Area receiving FY 2005 UASI funds.” The grant guidance further requires that, “if a State does not have a designated Urban Area(s), then it must identify a multi-jurisdictional metropolitan area or region...” to conduct these relevant required activities. For States without a designated Urban Area, the requirements under the priority above are meant to apply to the same jurisdictions identified to address the FY 2005 Homeland Security Grant Program Guidance requirements (see: <http://www.ojp.usdoj.gov/odp/docs/fy05hsgp.pdf>).

⁵ For further information, please consult the FY 2005 CDC Public Health Emergency Preparedness Cooperative Agreement, Appendix 3: Cities Readiness Initiative (CRI) Guidance. This can be found at <http://www.bt.cdc.gov>.

Once fully developed, the Tier System will encourage States to designate regional groupings of jurisdictions at the sub-State level that collectively cover the entire geography of the State. Where appropriate, interstate groupings will also be encouraged through the Tier System. These interstate groupings should include representatives from all affected political jurisdictions. The Target Capabilities List will assign specific levels of capability to each Tier. Since the level of risk of a major event is not the same for every area, the target level of capabilities that specific sub-State regional areas should establish will vary based on risk factors such as total population, population density, and presence of critical infrastructure. The Tier System will help ensure that areas at greatest risk and need are prioritized. Since every entity is subject to some degree of risk and can make contributions to national preparedness, it will also help ensure that a minimum level of capability exists for each sub-State area, no matter the Tier.

Federal, State, Local, and Tribal Responsibilities

The specific responsibilities under this priority are assigned to either the States or DHS. The Governor of each State⁶ has designated a State Administrative Agency (SAA) to apply for and administer the funds under the Homeland Security Grant Program (HSGP), including obligating HSGP funds to local units of government⁷ and other designated recipients. The SAA is also responsible for coordinating the process to conduct the State Homeland Security Assessment and Strategy (SHSAS) process. Since the SAA is directly responsible to DHS for all reporting and administering functions, the State requirements contained here are assigned to the SAA, who coordinates and consults with other Federal, State, local, and tribal entities.

Many States have already designated homeland security or emergency response regions (e.g., Local Emergency Planning Committees, State Homeland Security Regions, State Emergency Response Commission areas) or other sub-State regional entities; others have yet to do so. DHS strongly recommends that all States develop sub-State regions that collectively cover the entire geography of the State. Planning through existing interstate regions is also encouraged where appropriate. For purposes of this priority, States are initially required to lead an effort to assess the current geographic and jurisdictional composition of the regions associated with each designated UASI Urban Area as well as at least one designated multi-jurisdictional metropolitan area identified by those States that do not have a UASI Urban Area.

While it may encourage the development of sub-State geographic regions, a “one-size-fits-all” solution is impractical. Each State has unique regional traditions, geographic features, and political realities that will influence how it organizes into regions at the sub-State level. Therefore, rather than mandating a single approach, this guidance provides certain planning

⁶ As defined in the Homeland Security Act of 2002, the term “State” means “*any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States.*”

⁷ As defined in the Homeland Security Act of 2002, the term “local government” means “*(A) county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, or agency or instrumentality of a local government; an Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and a rural community, unincorporated town or village, or other public entity.*”

considerations for States to guide the creation or strengthening of their sub-State regions. These planning factors should be guided by one overarching strategic factor – the effects of major events and the associated required capabilities necessary to prevent and respond to such events should drive the size and jurisdictional makeup of sub-State regions. Additionally, in some locations interstate planning is critical to facilitate an integrated response.

Preventing and responding to major events (as represented by the National Planning Scenarios) will require that capabilities be drawn from a wide area. The area from which resources will be drawn may or may not expand beyond the current area served by existing constructs. In developing sub-State regions, States should consider any number of approaches. This priority requires that States conduct a stepwise process to analyze alternative options for the geographic and jurisdictional composition of their sub-State regions. States should conduct the following actions and consider the associated planning factors in the development of sub-State regions around their highest-risk areas:

1. Analyze alternative geographic and jurisdictional compositions options such as:
 - Any currently designated multi-jurisdictional area (e.g., UASI Urban Area, State Emergency Management district, State homeland security region, or Local Emergency Planning Committee);
 - The jurisdictions and entities included within a standard planning radius from the center of the core city (e.g., all counties within a 100 mile radius from the center of the core city); and
 - The entities within the Metropolitan Statistical Area (as defined by the U.S. Census Bureau and the U.S. Office of Management and Budget).⁸
2. Conduct an analysis of alternatives around the identified options in Step 1 above. Planning considerations include:
 - Compare each of the options identified above to the collective set of potential effects of major events (i.e., the potential set of major events as represented by the National Planning Scenarios);
 - For each option, using the set of potential effects as the basis, assess factors such as total population, population density, and presence of critical infrastructure; and
 - For each option, consider the resident capability present in each of the jurisdictions and tradeoffs among the options versus the collective capability needed to prevent and respond to these events.
3. Select a preferred regional geographic and jurisdictional option.

Once a preferred option is selected, efforts should begin to adjust and update plans, strengthen mutual aid, and begin regional training and exercises according to the region. Initially, evaluating and strengthening existing planning and regional collaboration structures provides the

⁸ See: <http://www.census.gov/population/www/estimates/metrodef.html>

foundation for a system of sub-State regions that cover the entire State. In the future, such regions will be required and will subsequently be assigned to the Tier System (to be included in the Final Goal to be released on October 1, 2005). To the extent possible, all States should begin in FY 2005 to assess options and consider various regional configurations that develop or modify sub-State regions to center on major population areas.

Further Information

ODP has several support mechanisms available to assist with required activities under the Expanded Regional Collaboration priority, including ODP Preparedness Officers and the Central Scheduling and Information Desk (CSID). ODP Preparedness Officers work closely with State and local officials in assigned States and Territories to assist agencies in enhancing their

Responsibilities:

- **DHS** – In the Final National Preparedness Goal to be released on October 1, 2005, DHS will include the standardized national Tier System for grouping jurisdictions/sub-State regions to account for differences in levels of capability based on risk factors such as total population, population density, and critical infrastructure. Additional instructions will be included with the Final Goal on applying the Tier System and target levels of capability.
- **States** – Each State Administrative Agency (SAA) must: 1) analyze alternative geographic and jurisdictional composition options; 2) conduct an analysis of alternatives around the identified options; and 3) select, at a minimum, a preferred regional geographic and jurisdictional option. As noted previously, this applies to each of the 57 designated UASI Urban Areas, as well as at least one (1) multi-jurisdictional metropolitan area in each State without a designated UASI area.

homeland security preparedness. Preparedness Officers will be in continuous contact with the SAAs and local officials and should be considered as the primary point of contact within ODP for addressing questions, concerns, general issues, and accessing specialized expertise. The CSID is a non-emergency resource for use by State and local emergency responders across the Nation. The CSID provides general information on all ODP programs. ODP Preparedness Officers and the CSID can each be reached through the CSID at 1-800-368-6498 or askcsid@dhs.gov. CSID hours of operation are from 8:00 a.m. - 7:00 p.m. (EST), Monday-Friday.

3.1.3 Implement the Interim National Infrastructure Protection Plan

Rationale

Critical infrastructure and key resources (CI/KR) provide the essential services that sustain our national security, economic vitality, and American way of life. Attacks on CI/KR could disrupt the direct functioning of key business and government activities, facilities, and systems, as well as have cascading effects throughout the Nation's economy and society. Furthermore, direct attacks on individual key assets could result not only in large-scale human casualties and property destruction, but also in profound damage to national prestige, morale, and confidence.

To protect our CI/KR from terrorist exploitation, we must understand the threat (e.g., terrorist intent, objectives, tactics, and techniques) as well as the overall picture of the assets to be protected: *“What are they? What are their vulnerabilities and their interdependencies? What are the potential consequences they pose and the actions that can be taken to protect them against attack or mitigate the consequences of an attack?”* Although the Federal government has been carrying out critical infrastructure protection (CIP) efforts for years, the need for a national CIP program was formally articulated in the Homeland Security Act of 2002, which assigned responsibility for the national program to the DHS. Under HSPD-7 (issued December 2003), DHS was directed to develop a national plan to frame the activities of the national CIP effort. HSPD-7 also listed the specific Federal departments and agencies that are responsible for protection activities in 17 CI/KR sectors.

In response to HSPD-7, DHS released an interim version of the National Infrastructure Protection Plan (NIPP) in February 2005. The Interim NIPP is the base plan that provides the framework and sets the direction for implementing a coordinated national CIP effort. It establishes a risk management framework that focuses resource allocation decisions on actions that will result in the greatest benefit in terms of reducing vulnerability, deterring threats, and minimizing consequences of attacks if they occur. It provides a framework for identifying critical assets, assessing vulnerabilities, prioritizing assets, and implementing protection measures within and across CI/KR sectors. It also delineates roles and responsibilities among Federal, State, local, tribal, and private sector stakeholders in carrying out these activities. The risk management framework in the NIPP is further delineated in Sector-Specific Plans (SSPs) for protecting CI/KR in each sector.

Linked Capabilities

“Implement the National Infrastructure Protection Plan” is an overarching priority that contributes to the development of the six prevention- and protection-oriented capabilities in the TCL, which are defined as follows:

- **Critical Infrastructure Protection:** The capability of public and private entities to prepare and protect those systems and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact to the country. This capability includes decision-making processes on which CI/KR assets are

secured, the assessment methods and resources used to address the security, and the cost-benefits associated with these decisions. As a result of having this capability, at-risk targets are identified; vulnerability assessments are conducted, documented, and standardized; and the threat to, and vulnerability of, high-risk targets are reduced.

- **Food and Agriculture Safety and Defense:** The capability to identify and defend against pathogens, chemical and biological contaminants, and other hazards that affect the safety of food and agriculture products. This includes the timely eradication of outbreaks of crop diseases/pests, assessments of the integrity of the food producing industry, and the removal of potentially compromised materials from the U.S. food supply. It is accomplished concurrent to protecting public health and maintaining domestic and international confidence in the U.S. commercial food supply. Additionally, the public is provided with accurate and timely notifications and instructions related to food and agriculture safety and defense.
- **Information Collection:** The capability to gather, consolidate, and retain raw data from sources including human-source intelligence, observation, qualitative and quantitative analysis of data derived from technical observation or from threat/vulnerability analysis, and open-source intelligence. By definition, intelligence is information which is deemed to possess some value to anti- or counterterrorism efforts and thus, Information Collection is the collection of only pure, unexamined data. Threat Recognition is the ability to see in this data the potential indications and/or warnings of terrorist activities or planning against U.S. citizens, land, infrastructure, and/or allies.
- **Information Sharing and Collaboration:** The capability to exchange and disseminate information and intelligence in a multi-jurisdictional as well as multidisciplinary manner, that is, among the Federal, State, local and tribal layers of government, the private sector, and citizens. The goal of Information Sharing is to facilitate the distribution of useful, relevant, and timely information and/or intelligence to the entities that need it. More simply, the goal is to get the right information, to the right people, at the right time.
- **Intelligence Fusion and Analysis:** The capability to merge data and information for the purpose of analyzing, linking, and disseminating timely and actionable intelligence with emphasis on the larger threat picture and to consolidate analytical products among the various intelligence analysis units at the Federal, State, local, and tribal levels for tactical, operational, and strategic use. This capability also includes the examination of raw data to identify threat pictures, recognize potentially harmful patterns, or connect suspicious links to discern potential indications or warnings.
- **Risk Analysis:** The capability to identify and prioritize hazards, assess vulnerabilities, and determine risks prior to and during an emergency.

Federal, State, Local, and Tribal Responsibilities

Although DHS is responsible for leading the overall national effort to enhance CI/KR protection, safeguarding our Nation requires a strong partnership between departments and agencies at all levels of government with private sector infrastructure owners and operators, and non-governmental organizations. The Interim NIPP provides the structure and starting point for

building this partnership through strong coordination between DHS and the Sector-Specific Agencies (SSAs).⁹ The results of these partnerships will be reflected in the Final NIPP, which will be released at the end of the interim period.

During this interim period, the SSAs will partner with their sector stakeholders (i.e., private sector; State, local, and tribal governments), to update and/or refine their SSPs for conducting CI/KR activities in their sector. These dialogues will take place through Sector Coordinating Councils (led by the private sector) and Government Coordination Councils (led by the SSA), which are being established to provide mechanisms for sharing information about critical assets. The NIPP risk management framework provides the sector with general guidelines but allows flexibility to build consensus for determining the most effective approach to achieving risk reduction. Because the vast majority of the Nation's CI/KR is owned or operated by the private sector, these stakeholders will be vital partners in the development of workable SSPs. During this period, DHS will also be coordinating with stakeholders within and across sectors to refine the national risk management approach, which will be reflected in the Final NIPP.

Applying the NIPP risk management framework through sector-specific actions will emphasize security and provide a focus for risk management operations in years to come. Through the development and continuous refinement of the SSPs, industry and other stakeholders will enjoy a collaborative partnership with their sector and with authorities at the Federal, State, local, and tribal levels. This partnership ensures a holistic approach to critical infrastructure protection that evolves over time with national, regional, and sector-based needs.

⁹ Sector Specific Agencies and assigned sectors as listed in the Interim National Infrastructure Protection Plan, page 3: Department of Agriculture — Agriculture, Food (meat, poultry, egg products); Department of Health and Human Services — Public health and healthcare; Food (other than meat, poultry, egg products); Environmental Protection Agency — Drinking water and wastewater treatment systems; Department of Energy — Energy, including the production, refining, storage, and distribution of oil and gas, and electric power (except for commercial nuclear power facilities); Department of the Treasury — Banking and finance; Department of the Interior — National monuments and icons; Department of Defense — Defense industrial base; and Department of Homeland Security — Information technology; Telecommunications; Chemical; Transportation systems; Emergency services; Postal and shipping; Dams; Government facilities; Commercial facilities; and Nuclear reactors, materials, and waste.

Responsibilities:

- **DHS** – DHS will undertake a major outreach effort to engage all the stakeholders necessary to utilize, refine, and continue to develop milestones and performance measures to assess national-level and sector-by-sector progress. DHS will continue to enhance its programs in information analysis and infrastructure protection and integrate these efforts under the framework of the NIPP.
- **Federal** – SSAs will complete and begin to implement the SSPs, track progress on the initiatives outlined in the SSPs, and work with all their respective stakeholders so that SSPs meet the unique challenges of each individual sector. SSAs will utilize, refine, and continue to develop milestones and performance measures to assess progress in each sector. Cross-sector coordination will occur through the NIPP Senior Leadership Council and specific parts of DHS that will be conducting interdependency analyses, developing guidance and tools, and working on a measurement system that provides important feedback to the SSAs. Supporting departments and agencies will work with the SSAs to implement the SSPs and participate in sector-specific activities through the Government Coordinating Councils.
- **State, Local, and Tribal** – State, local, and tribal entities will be engaged by DHS and the SSAs to promote awareness of and provide feedback on the NIPP framework and to solicit their involvement in the National CIP program. State, local, and tribal entities will also work with the appropriate SSAs to begin implementation of the SSPs for various sectors. As the NIPP is implemented, State, local, and tribal government agencies should expect to experience more coordinated data calls and fewer overlapping efforts to identify and assess critical assets.
- **Private Sector** – Private sector entities will be engaged by DHS, in collaboration with the relevant SSAs, to promote awareness of and feedback on the NIPP framework and to solicit their involvement in the National CIP program. Private sector entities will also work with the appropriate SSAs to begin implementation of the SSPs for their sectors. As the NIPP is implemented, private sector entities should expect more coordinated data calls from government agencies, and enhanced engagement through Sector Coordinating Councils.

Further Information

For more information, refer to the Interim NIPP or send comments and questions to NIPP@dhs.gov.

3.2 Capability-Specific Priorities

3.2.1 Strengthen Information Sharing and Collaboration Capabilities

Rationale

Information sharing and collaboration is a clear national priority. Information and/or intelligence that may forewarn of a future attack may be derived from information collected not only by Federal entities or the intelligence community, but also by State, local, and tribal government personnel through crime control and other routine activities and/or by people living and working in our local communities. Successful homeland security efforts require that Federal, State, local, tribal, and private sector entities have an effective information sharing and collaboration capability to ensure they can seamlessly collect, blend, analyze, disseminate, and use information regarding threats, vulnerabilities, and consequences.

The President and Congress have directed that an Information Sharing Environment be created in the next two years to facilitate information sharing and collaboration activities within the Federal government (horizontally) and between Federal, State, local, tribal, and private sector entities (vertically). The desired end state for this priority is effective and timely collaboration and sharing of information and intelligence across Federal, State, local, tribal, regional, and private sector entities to achieve coordinated awareness and prevention of terrorist activities. In the interim, there are a number of ongoing Federal initiatives that will help to strengthen information sharing and collaboration capabilities.

One initiative is the expansion of access to and use of the Homeland Security Information Network (HSIN), a collection of DHS systems launched in February 2004. HSIN is managed by the Homeland Security Operations Center and is the primary conduit to reach intelligence and law enforcement agencies and operations centers at the Federal, State, local, and tribal level. The centerpiece of HSIN is the family of Joint Regional Information Exchange Systems, which provide real-time collaboration and sharing on a secure system. DHS has already achieved connectivity to all 50 States, and its current goal is to deploy HSIN to all States and UASI Urban Areas to strengthen the two-way flow of real time threat information at the Sensitive-but-Unclassified level through the SECRET levels by the end of FY 2007.

Another initiative is the Department of Justice (DOJ) Law Enforcement Information Sharing Program (LEISP). LEISP reflects DOJ's commitment to transform the way they share law enforcement information with Federal, State, local, and tribal law enforcement and homeland security partners. All DOJ component information sharing initiatives and activities will be consistent with and support implementation of the LEISP Strategy. DOJ and DHS have collaborated on the LEISP strategy since its inception. LEISP serves as a key component of DOJ's and DHS's contribution to fulfilling Executive Order 13356 "*Strengthening the Sharing of Terrorism Information to Protect Americans*" and implementation of the Intelligence Reform and Terrorism Prevention Act of 2004. The LEISP Strategy also identifies how DOJ and DHS will support implementation of the National Criminal Intelligence Sharing Plan. The National Criminal Intelligence Sharing Plan was developed by the law enforcement community and

articulates the need for intelligence-based policing and a comprehensive national approach for law enforcement information sharing. DOJ will achieve its objectives by adopting new information sharing policies and practices, as well as by implementing a unified department-wide technology architecture that will enable DOJ to more easily partner with the community of Federal, State, local, and tribal law enforcement, intelligence and homeland security agencies. In this regard, the FBI's Regional Data Exchange is being used to share full-text crime information at the State and local level, while the Bureau's National Data Exchange is being designed to provide nationwide criminal reporting and terrorism-related information sharing capabilities for data derived from incident and event reports (e.g., arrest, booking and incarceration data). National Data Exchange and Regional Data Exchange are elements of the FBI's National Information Sharing Strategy, a component piece of the LEISP Strategy designed to improve the FBI's information sharing throughout the Nation.

Another critical effort contributing to strengthened information sharing and collaboration is the FBI housed National Joint Terrorism Task Force (NJTTF). The mission of the NJTTF is to enhance communications, coordination, and cooperation among Federal, State, local, and tribal agencies representing the intelligence, law enforcement, defense, diplomatic, public safety, and homeland security communities by providing a point of fusion for terrorism intelligence and by supporting FBI Joint Terrorism Task Forces (JTTFs) throughout the United States. Suspicious activity, terrorist threats, and actual incidents with a potential or actual terrorist nexus are reported immediately to a local or regional JTTF (or the NJTTF, in the case of Federal departments and agencies). Subsequently, the FBI Strategic Information and Operations Center immediately reports the terrorist threat, if the FBI deems the threat to be credible, or an actual incident, to the Homeland Security Operations Center.

In addition to these efforts, the DOJ, along with components such as FBI, lead, sponsor, or participate in a number of other key information sharing and collaboration initiatives including the Global Justice Information Sharing Initiative (Global) Advisory Committee, the National Information Exchange Model, the National Virtual Pointer System, the El Paso Intelligence Center, Law Enforcement Online, and Regional Information Sharing Systems.

Linked Capabilities

This national priority is linked to the "Information Sharing and Collaboration" Target Capability. It is focused on prevention but also supports protection, response, and recovery. Federal, State, local, and tribal entities should consult the TCL and examine the capability template for this target capability. As defined in the TCL:

"Information Sharing and Collaboration capabilities are necessary tools to enable efficient prevention, protection, response, and recovery activities. Information Sharing is the multi-jurisdictional, multidisciplinary exchange and dissemination of information and intelligence among the Federal, State, local, and tribal levels of government, the private sector, and citizens. Collaboration encompasses a wide range of activities aimed at coordinating the capabilities and resources possessed by various governmental and private sector entities. While Information Sharing seeks to foster a willingness and

ability to provide information and/or intelligence, Collaboration represents the establishment of formal relationships among various and disparate homeland security entities and systems to interact and cooperate.”

Federal, State, Local, and Tribal Responsibilities

Responsibilities:

- **DHS** – DHS will expand access to and use of the Homeland Security Information Network (HSIN). The goal is to deploy HSIN to all States and UASI areas to strengthen the two-way flow of real time threat information at the Sensitive-but-Unclassified level through the SECRET levels by the end of FY 2007.
- **DOJ/FBI** – DOJ is a committed partner to information sharing and will implement the LEISP strategy by leveraging existing capabilities and initiatives. DOJ will implement short-term solutions to enhance information sharing throughout the Federal government and with the rest of the law enforcement community (e.g., connecting Regional Information Sharing Systems, Law Enforcement Online, and HSIN). DOJ will also pursue long-term information sharing strategies to present a single, unified source for DOJ data to other Federal departments and agencies as well as State and local partners. DOJ will adopt consistent department-wide policies and procedures to protect the privacy of individuals and the security of information it shares.

Further information

Additional information on HSIN: can be found at the following web sites:

- <http://www.dhs.gov/dhspublic/display?theme=43&content=3747&print=true>
- www.swern.gov
- www.nwwarn.gov
- www.ian.gov

Additional information on FBI and related DOJ efforts in this area can be found at www.fbi.gov/terrorinfo/counterrorism/partnership.htm.

3.2.2 Strengthen Interoperable Communications Capabilities

Rationale

The lack of interoperable wireless communications systems is an issue that continues to affect public safety agencies in communities across the county. In many cases, agencies are unable to communicate or share critical voice and data information with other jurisdictions or disciplines during major events or even in day-to-day operations. Interoperable communications – the ability to provide uninterrupted flow of critical information among responding multi-disciplinary and multi-jurisdictional agencies at all levels of government – is a priority capability. Communications interoperability underpins the ability of Federal, State, local, and tribal entities to work together effectively to prevent, protect against, respond to, and recover from terrorist attacks, major disasters, and other emergencies.

Analysis of State and Urban Area Homeland Security Strategies, in addition to a number of reports on the status of interoperable communications, reflects persistent shortfalls in achieving interoperability. State, local, and tribal authorities continue to emphasize the need for statewide interoperable communications plans, a national architecture that identifies communications requirements and technical standards, and a national database of interoperable communications frequencies. Achieving interoperable communications and creating effective mechanisms for sharing information are long term enterprises that will require Federal leadership and collaborative, interdisciplinary, and intergovernmental planning.

It is important to understand that the process of achieving national interoperability cannot be completed overnight, but important interim measures that establish frameworks for achieving that priority are already in place. They include:

- Creation of the Federal Interagency Coordination Council to coordinate funding, technical assistance, standards development, and regulations affecting communications and interoperability across the Federal government;
 - Development of a Statement of Requirements, which, for the first time, defines what it will take to achieve full interoperability and provides industry requirements against which to map their product capabilities;
 - Development of a national interoperability baseline;
 - Acceleration of the development of critical standards for interoperability;
 - Establishment of a task force with the Federal Communications Commission to consider spectrum and regulatory issues that can strengthen public safety interoperability; and
 - Creation of a model process for developing statewide communications plans.
-
- Implementation of practical technology solutions that allow State and local agencies to interconnect without completely replacing the agencies' existing communications infrastructure.

SAFECOM, a program within the DHS Science and Technology Directorate, Office for Interoperability and Compatibility (DHS/S&T/OIC), is the umbrella program within the Federal government that coordinates the efforts of Federal, State, local, and tribal public safety agencies to improve public safety response through more effective, efficient, interoperable wireless communications. SAFECOM encourages a collaborative planning process to facilitate the development of other statewide strategic plans because it builds support at all levels of government. Therefore, SAFECOM developed the Statewide Communications Interoperability Planning (SCIP) methodology as an effective model that other States may adapt to their particular needs. It is available at:

http://www.safecomprogram.gov/SAFECOM/library/interoperabilitycasestudies/1223_statewidecommunications.htm

In addition to the DHS initiatives outlined above, DOJ contributes to improving interoperability among the homeland security community through several initiatives. In partnership with DHS and the Department of the Treasury, DOJ is leading the deployment of the Integrated Wireless Network (IWN), a multi-year effort to consolidate Federal law enforcement/homeland security radio infrastructure. The new infrastructure will provide inherent interoperability among the IWN partners and will greatly ease the task of connecting these Federal agencies to State and local partners. DOJ also directly assists State and local law enforcement agencies to implement interoperable communications capabilities through targeted funding, research and technical assistance provided through the Office of Community Oriented Policing Services (COPS) interoperability grants, the National Institute of Justice (NIJ) Communications Technology (CommTech) Program; and the 25 Cities project, a component of the IWN Program.

Linked Capabilities

This national priority is linked to the “Interoperable Communication” target capability. Federal, State, local, and tribal entities should consult the TCL and examine the capability template for this target capability. As defined in the TCL:

- Interoperable Communications provide the capability to provide uninterrupted flow of critical information among responding multi-disciplinary and multi-jurisdictional agencies at all levels of government.

Federal, State, Local, and Tribal Responsibilities

The FY 2005 Homeland Security Grant Program (HSGP) guidance requires grantees to develop and test a plan to achieve tactical interoperable communications. Grantees have six months from the release of this guidance to develop their tactical interoperable communications plan and one year following its submission in which to test it through multi-jurisdictional exercises.

Each Urban Area receiving FY05 UASI funds must develop and test a tactical interoperable communications plan. If a State does not have a designated Urban Area, then it must identify a metropolitan area to develop and test the plan. This metropolitan area should be the same

metropolitan area tasked with developing a multi-jurisdictional prevention and response plan as part of the HSPD-8 implementation required by the FY 2005 HSGP guidance.

Responsibilities:

- **DHS** – SAFECOM will continue to coordinate the efforts of Federal, State, local, and tribal public safety agencies to improve public safety response through more effective, efficient, interoperable wireless communications.
- **Other Federal Departments and Agencies** – Consolidate communications systems and implement emerging standards to the extent practical to ease interconnectivity with state and local systems. Coordinate and target grant and technical assistance consistent with guidance provided by SAFECOM.
- **States** – If a State does not have a designated Urban Area, then it must identify a metropolitan area to develop and test the plan. This metropolitan area should be the same metropolitan area tasked with developing a multi-jurisdictional prevention and response plan as part of the HSPD-8 implementation required by the FY 2005 HSGP Guidance. The planning and design phases of Federally-funded interoperability projects should be compliant with guidance provided by SAFECOM.
- **Urban Areas** – Each Urban Area receiving FY 2005 UASI funds must develop and test a tactical interoperable communications plan. The planning and design phases of Federally-funded interoperability projects should be compliant with guidance provided by SAFECOM

Further Information

Additional information on the requirement to develop and test a plan to achieve tactical interoperable communications is available on pages 51-53 of the FY 2005 HSGP Guidance. The ODP Interoperable Communications Technical Assistance Program (ICTAP) will also host three one-day, regional training workshops on the Tactical Interoperable Communications Planning Guidance and Template in conjunction with the Office of Community Oriented Policing Services Interoperable Communications Technology Program Workshop Series. The first of these workshops was held on April 13 in Denver, CO; the other two workshops are scheduled to be held on June 3 in Columbus, OH and on July 14 in Charlotte, NC. These workshops will provide grantees with “hands on” instruction and respond to any questions on the planning process. These workshops will also afford participants the opportunity to request support, if needed, through ODP’s Interoperable Communications Technical Assistance Program (ICTAP).

Additional questions on the ICTAP can be directed to the ODP Preparedness Officers and the Central Scheduling and Information Desk (CSID). ODP Preparedness Officers and the CSID can each be reached through the CSID at 1-800-368-6498 or askcsid@dhs.gov. CSID hours of operation are from 8:00 a.m. - 7:00 p.m. (EST), Monday-Friday.

3.2.3 Strengthen CBRNE Detection, Response, and Decontamination Capabilities

Rationale

Defending America against catastrophic threats is one of the most significant challenges facing the Nation. Chemical, Biological, Radiological, Nuclear, Explosive (CBRNE) terrorism has been repeatedly identified as one of the primary threats facing our Nation. As the *National Security Strategy* states, “*The gravest danger our Nation faces lies at the crossroads of radicalism and technology. Our enemies have openly declared that they are seeking weapons of mass destruction, and evidence indicates that they are doing so with determination.*” Since the potential number of terrorist targets is large and the threats and means of delivery varied, the Nation must develop a layered defense against weapons of mass destruction (WMD), from counterproliferation activities overseas to the deployment of systems that ensure early detection of the presence, import, transport, or manufacture of CBRNE materials, to capabilities for successful CBRNE response and decontamination.

CBRNE detection requires an effective infrastructure and the deployment of systems that are cost-effective, robust, highly sensitive, specific, and integrated into a concept of operations that considers timeliness of information and appropriate level of technical expertise to interpret the results. These defenses must include systems for both rapid detection and rapid authentication and verification of the identity and quantity of CBRNE materials. By their nature, CBRNE materials require different detection and characterization methodologies. As Federal, State, and local authorities deploy these detection technologies, it is important to ensure consistency of procedures in training, interoperability, and where appropriate, information sharing to ensure timely and effective action, reach back, and use of information generated by and for these systems. This will require the development and adoption of prescribed standards for equipment, training and operations. The Federal government, working closely with State and local governments, will analyze current capabilities (operational and technical), develop concepts of operations, and determine how the technologies and systems can be integrated and synchronized. The concept of operations and architecture will address who will receive, employ, and support the detection technologies and measurement systems.

Response includes activities to address the immediate and short-term actions to preserve life, property, environment, and the social, economic, and political structure of the community. Response will provide the capability to assess the incident, including testing and identifying hazardous substances; providing protective clothing and equipment to responders; conducting rescue operations to remove affected victims from the hazardous environment; conducting searches of suspected sources of contamination and establishing exclusion zones. There is also a category of response prior to an explosion or dispersal of hazardous material. For this period, specialized CBRNE response teams must possess the capability to detect, locate, identify, and assess potential damage, as well as isolate and disarm a weapon. Additional response capabilities are required post- release or detonation – the period in which people are in the most danger.

Decontamination issues such as containing and fully decontaminating the incident site, victims, responders and equipment; managing site restoration operations; and implementing standard evidence collection procedures need to be addressed prior to a CBRNE attack. This national priority leverages efforts throughout the government to develop robust capabilities to detect, neutralize, contain, dismantle, and dispose of CBRNE materials, and decontaminate property. In addition, the capability to rapidly decontaminate large numbers of affected persons may be critical in preventing injury or death. These capabilities must be assembled to both augment normal operational resources and support multi-jurisdiction events. The Federal government can and should take a leadership role in the development of procedures, protocols, and recommended equipment purchases for mass decontamination of the public. Effective techniques for rapid mass decontamination of affected persons are needed as well as more Federal efforts to guide the purchase of needed equipment at the local level where the first response will occur.

This national priority leverages efforts throughout government to develop robust capabilities to detect, neutralize, contain, dismantle, and dispose of CBRNE materials, and decontaminate exposed personnel and property. Medical aspects of CBRNE detection, response, and decontamination are addressed in other capabilities in the TCL.

One initiative that supports this National Priority is the requirement, referenced above in section 2.2, for each Urban Area receiving FY 2005 UASI funds to develop a Multi-Jurisdictional Prevention and Response Plan (MPRP) based on the IED National Planning Scenario. If a State does not have a designated Urban Area, then it must identify a metropolitan area to develop the plan. This metropolitan area should be the same metropolitan area tasked with developing a tactical interoperable communications plan as required by the FY2005 HSGP guidance. Detailed MPRP Guidance will be released in May 2005. Grantees will still have six months (May 2005 – November 2005) from the release of the MPRP Guidance to develop their plans.¹⁰ Following the submission of the MPRP, Urban Areas will have one year to complete a cycle of multi-jurisdictional exercise activities based on this plan. DHS/SLGCP is developing a new volume for the Homeland Security Exercise Evaluation Program (HSEEP) reference documentation. This new volume, along with associated Technical Assistance, will help State, local, and tribal entities develop prevention exercises or combined prevention and response exercises as well as their own protocols for information sharing.

Linked Capabilities

This National Priority is linked to the following capabilities, as defined in the TCL:

- Explosive Device Response Operations will provide the capability to coordinate, direct, and conduct explosive device response operations, with the goal of successfully preventing, disrupting, rendering safe, and disposing of explosives, especially improvised explosive devices (IEDs).

¹⁰ For more information on the MPRP requirement, please refer to pages 50-51 of the FY2005 HSGP Guidance, and ODP Information Bulletin 159, issued April 1, 2005.

-
- CBRNE Detection will provide the capability to protect against WMD through deployment of systems that ensure early detection of the import, transport, manufacture, or release of CBRNE materials.
 - WMD/Hazardous Materials Response and Decontamination will provide the capability to assess the incident, including testing and identifying hazardous substances; providing protective clothing and equipment to responders; conducting rescue operations to remove affected victims from the hazardous environment; conducting searches of suspected sources of contamination and establishing exclusion zones; containing and fully decontaminating the incident site, victims, responders and equipment; managing site restoration operations; and implementing standard evidence collection procedures.

Federal, State, Local, and Tribal Responsibilities

Responsibilities:

Urban Areas – FY05 HSGP guidance requires each Urban Area receiving FY05 UASI funds to develop a Multi-jurisdictional Prevention and Response Plan (MPRP) based on the IED National Planning Scenario within six months of the issuance of MPRP Guidance (to be released in May 2005). Urban Areas will then have one year following the submission of their integrated plan(s) to test their plans through a cycle of multi-jurisdictional exercise activity that address the associated tasks outlined in the IED scenario. If a state does not have a designated urban area, then it must identify a metropolitan area to develop the plan(s). This metropolitan area should be the same metropolitan area tasked with developing a tactical interoperable communications plan as required by the FY2005 HSGP guidance.

Further Information

Questions regarding the MPRP requirement and guidance can be directed to the ODP Preparedness Officers and the Central Scheduling and Information Desk (CSID). ODP Preparedness Officers and the CSID can each be reached through the CSID at 1-800-368-6498 or askcsid@dhs.gov. CSID hours of operation are from 8:00 a.m. - 7:00 p.m. (EST), Monday-Friday.

Additional information is also available on pages 50-51 of the FY 2005 HSGP Guidance.

Detailed MPRP Guidance will be released in May 2005.

3.2.4 Strengthen Medical Surge and Mass Prophylaxis Capabilities¹¹

Rationale

Public health threats and emergencies can ensue from a myriad of infectious agents, some of which can be mitigated by administration of immunizations and/or antibiotics and antiviral drugs. Although wide variation exists among the disease and prophylaxis protocols, they all share a need for rapid deployment, distribution, and administration of the countermeasures. For example, in the event of a widespread aerosolized *Bacillus anthracis* attack, officials will have 48 hours to distribute antibiotics, perhaps to entire communities, to prevent massive loss of life. In contrast, the smallpox virus has a longer incubation period in which to incorporate a vaccination program but the disease is resistant to treatment and highly infectious. Vaccination within 3 days after exposure is held to be sufficient to prevent development of disease in a given individual. In the event of an outbreak, the objective is for public health officials to make vaccination available to the entire jurisdiction within 10 days.

Because response capacity to a large-scale bioterrorist attack may be limited by the ready availability of antibiotics and/or vaccines, the Federal government has created and will maintain the Strategic National Stockpile, which is composed of ready-to-deploy medical supplies designed to augment the State and local governments' ability to treat those affected by the highest-priority disease-causing agents and deliver them to a jurisdiction upon a Federal decision to deploy.

The State, local or tribal health departments organize and direct the mass prophylaxis campaign. The critical component of the mass prophylaxis capability is to effectively reach the entire affected population in time to prevent loss of life and injury. Local public health departments have the responsibility to develop and maintain (through exercises and drills) the capability to carry out first response and ongoing (Federally-assisted) mass antibiotic dispensing and vaccination campaigns tailored to the local population. States are responsible for providing support and assuring coordinated multi-jurisdiction responses. Federal assets and resources are intended to augment local and regional first response capability.

For medical surge, a mass casualty incident brought about by terrorism or a natural disaster will likely overwhelm the medical infrastructure of an affected jurisdiction. Challenges to meet surge requirements include recruiting, mobilizing, and deploying competent health care and allied professionals; moving ambulatory and non-ambulatory patients within a venue to and among facilities; when appropriate, decontaminating victims outside of the hospital to permit subsequent treatment and at the same time protecting medical infrastructure; providing hospital and/or ambulatory care patient locations commensurate with clinical requirements; and documenting patient exposure, movement, and medical records.

The Nation's healthcare system, particularly hospitals, must be able to handle large numbers of patients requiring immediate care following a major incident. Emergency-ready hospitals,

¹¹ This National Priority includes 2 of 12 readiness objectives for State and local public health emergency preparedness. The latest version of these objectives is available at <http://www.hhs.gov/ophep/>

working collectively, must be able to handle different types of injuries, including trauma and burns, infections, bone marrow suppression, or chemical- or radiation-induced injury. The medical provider community must have the capability to rapidly accommodate an influx of supplemental healthcare assets from mutual-aid partners, as well as the State and Federal government. Additionally, local public health and public safety agencies must develop capabilities and coordination capacity throughout the local and regional health and medical community. Because most of the Nation's medical assets are privately owned, capability-building must address the public-private gaps, as well as integrate multiple disciplines and levels of government.

Federal medical surge assets, such as National Disaster Medical System (which includes Federally coordinated care in participating civilian hospitals), assets from the Strategic National Stockpile, deployable medical facilities, and US Public Health Service personnel and other Federal responders, are designed to supplement local capacity. During a major event, a unified management approach, based on the NIMS, is critical. There must be effective management across levels, from the individual healthcare facility to the integration of Federal health and medical support.

Linked Capabilities

This national priority is linked to the “Mass Prophylaxis” and “Medical Surge” Target Capabilities, as defined in the TCL:

- Mass Prophylaxis is the capability to protect the health of the population through a mass prophylaxis campaign following an event. This capability includes the provision of appropriate follow-up medical care, as well as risk communication messages to address the concerns of the public.
- Medical Surge is the capability to provide triage and then to provide medical care. This includes providing definitive care to individuals at the appropriate clinical level of care over sufficient time to achieve recovery and avoid medical complications. The capability applies to an event resulting in a number or type of patients that outstrip the day-to-day acute-care medical capacity in a given area.

The critical component of the Mass Prophylaxis capability is to effectively reach the entire affected population in a time-critical manner to prevent loss of life and injury. This capability requires public health departments to organize and direct a mass prophylaxis campaign. Emergency-ready public health departments must be able to achieve this within an extremely short time frame and deliver consistent and comprehensive risk communication messages that address the needs and concerns of the public. Supporting medical target capabilities may include isolation and quarantine, medical surge, public health epidemiology and laboratory testing, and possibly mass fatality management.

Supporting medical target capabilities for Medical Surge may include isolation and quarantine, medical supplies management and distribution, public health epidemiological investigation and

laboratory testing, triage and pre-hospital treatment, worker health and safety, environmental health and vector control, and possibly fatality management.

Federal, State, Local, and Tribal Responsibilities

Responsibilities:

- **Federal** – HHS CDC will continue to maintain the Strategic National Stockpile. In addition, HHS will continue plans to develop deployable Federal medical capability to be used in case of mass disasters
- **States** – States are responsible for providing support and assuring coordinated multi-jurisdiction responses (Federal assets and resources are intended to augment local and regional first response capability).
- **State, Local, and Tribal** – The State, local, and tribal health departments are responsible for organizing and directing the mass prophylaxis campaign.
- **Locals** – Local public health departments have the responsibility to develop and maintain (through exercises and drills) the capability to carry out first response and ongoing (Federally assisted) mass antibiotic dispensing and vaccination campaigns tailored to its local population.

Further Information

For further information on Mass Prophylaxis, please refer to the Centers for Disease Control and Prevention, Coordinating Office of Terrorism Preparedness and Emergency Response's website: <http://www.bt.cdc.gov>.

For further information on Medical Surge, please refer to the Health Resources and Services Administration Mass Casualty website: <http://www.hrsa.gov/bioterrorism/masscasualty/materials.htm>.

Compliance assessment relative to Mass Prophylaxis and Medical Surge will be collected and reported through the HHS/CDC Public Health Emergency Preparedness Cooperative Agreement and the HRSA National Bioterrorism Hospital Preparedness Cooperative Agreement. For further information, please refer to the final HHS/CDC and HRSA guidance, which should be released in April-May 2005.

4.0 STANDARDS FOR ASSESSMENTS AND STRATEGIES

In support of the National Preparedness Goal, HSPD-8 requires the development of “*standards for preparedness assessments and strategies.*” Assessments and strategies are required to report on the overall preparedness of the Nation. Developing an approach for assessing national preparedness will be iterative, using existing systems, processes, and data where possible. Careful attention will be given to effectively balancing the need to evaluate the preparedness of communities, States, regions, and the Nation while being sensitive to the burden being placed on those being assessed. Assessments of readiness are evidence-based, but may include subjective components that incorporate the judgment and experience of senior officials. Senior officials will retain the authority, responsibility, and discretion to provide additional evidence or information to the overall assessment for their respective entity.

4.1 Preparedness Assessments

National Preparedness Assessments will include four component assessments:

1. **Compliance Assessment** – assessing Federal, State, local, and tribal completion of the requirements included in the National Preparedness Guidance checklists (see Appendix D).

States, in cooperation with local and tribal entities, will be requested to review the compliance checklist and indicate which requirements have been completed prior to applying for Federal preparedness grant assistance. The completed compliance checklists will be submitted by States with the FY 2006 Homeland Security Grant Program application. Compliance assessment relative to Mass Prophylaxis and Medical Surge will be collected and reported through the HHS/CDC Public Health Emergency Preparedness Cooperative Agreement and the HRSA National Bioterrorism Hospital Preparedness Cooperative Agreement.

Toolkit

Compliance Checklists that highlight the requirements in the Interim National Preparedness Guidance are provided in Appendix D. These checklists will be submitted as part of the HSGP grant application.

Responsibilities:

- **DHS** – Coordinate review and approval of the submitted compliance checklists.
- **Federal** – Demonstrate, as appropriate, compliance with applicable requirements highlighted in the Interim National Preparedness Guidance.
- **States and Urban Areas** – Submit compliance checklists with FY 2006 Homeland Security Grant Program application.

2. Capability Assessment – assessing current capabilities against target levels of capability to be defined in the Target Capability List.

In FY 2005, the Capability Assessment will be conducted through a representative sampling of States and/or sub-State regions. This will allow the process to be tested and proven prior to a nationwide implementation. This assessment process will build upon the current grant monitoring process. ODP Preparedness Officers, HHS/CDC and HRSA Project Officers, and other subject-matter experts from the Federal, State, local, and tribal preparedness community will form assessment teams¹². These teams will work in close coordination with a cross-disciplinary team identified by the State and/or sub-State region to evaluate current capabilities. The assessment will be conducted using a capability worksheet (see Figure 7) based upon the existing capability measures in the TCL. Because target levels of capability will not be defined until October 1, 2005, the IED National Planning Scenario will be used to set the planning assumptions for this initial assessment.

The State or sub-State region selected for the representative sampling will be asked to provide evidence supporting the achievement of a specific measure. Participating states and sub-State regions will help to develop summary assessments, using weighted criteria, and an overall scoring methodology.

Toolkit

A representative sampling of capabilities will be conducted during FY 2005. The full Capability Assessment process will be defined as part of the Assessment and Reporting System to be launched by April 1, 2006.

Responsibilities:

- **DHS** – Coordinate the Capability Assessment process and map existing assessment data to the National Priorities.
- **Federal** – Support the Capability Assessment process and provide information upon request on how their grantees are utilizing Federal preparedness assistance dollars.
- **State, Local, and Tribal** – Encourage collaboration with DHS and other partners to more fully define and develop the Capability Assessment process.

¹² The assessment team concept and composition is still under development.

Figure 7: Notional Capability Worksheet

Name of Capability:						
Section 1: Emergency Operations Center (Yes, Large Extent, Small Extent, No)						
	Questions (from the TCL measures)	Answer	Explanation	Evidence/Data	Weighting	Weighted Score
1	A management plan for the EOC exists				9.1%	
2	EOC procedures are consistent with NRP, NIMS, and appropriate State, local, and tribal procedures				9.1%	
3	A procedure for staffing the EOC exists				9.1%	
4	EOC meets NIMS incident command structure requirements to perform core functions: coordination, communications, resource dispatch and tracking, and information collection, analysis, and dissemination				9.1%	
5	The management plan for the EOC includes sections on: incident action planning, situation reports, interagency coordination				9.1%	
6	All EOC-related communications systems are interoperable with surrounding jurisdictions				9.1%	
7	Mutual Aid Agreements (MAAs) and Memorandums of Understanding (MOUs) are in place				9.1%	
8	Procedures are in place to activate MAAs				9.1%	
9	Trained personnel are available to cover appropriate ESF functions				9.1%	
10	Jurisdiction has identified alternate EOC site in case first site is damaged/destroyed in the event and is not capable of operating				9.1%	
Total Capability Score	The Emergency Operations Center (EOC) is activated, staffed, and managed for a pre-planned or no-notice event; multi/interagency activities, such as communications, resource management, and mutual aid are coordinated; Incident Action Planning activities within the EOC are conducted at regular periodic intervals; and Situation Reports are produced at regular periodic intervals.				100%	0%

3. Needs Assessment – identifying and prioritizing resource needs to fill capability gaps and deficiencies.

A capabilities-based needs assessment will provide a consistent means for identifying and prioritizing homeland security resource needs in the form of capability elements (e.g., planning, training, equipment, or exercises). Beginning in FY 2006, States will be required to explain in their grant applications how current and future funds will be applied to strengthen capabilities related to the National priorities. Specific guidance related to this requirement will be issued separately.

4. Performance Assessment – evaluating the ability to perform the tasks associated with the capabilities.

Performance is captured on an ongoing basis through standardized After-Action Reports that document an organization’s performance (in specific tasks relevant to the target capability) in exercises and real-world events. The exercise evaluation process outlined in the Homeland Security Exercise Evaluation Program (HSEEP) is designed to enhance the quality and usefulness of homeland security exercises by evaluating performance against standardized criteria, enhancing data analysis, and focusing greater attention on implementation of improvements. The evaluation process recognizes those critical tasks that the exercise participants perform well and makes recommendations for improvements.

Toolkit
The HSEEP manuals are currently undergoing revision to incorporate the UTL and TCL. Upon completion they will be released to the Federal, State, local, and tribal communities.

- Responsibilities:**
- **DHS** – Update the HSEEP evaluation process in order to reflect the UTL and TCL.
 - **Federal** – Incorporate, as appropriate, the UTL, TCL, and standardized After Action Reports into the design and execution of exercises.
 - **State, Local, and Tribal** – Apply the HSEEP process and standardized After Action Reports, as appropriate, into their design and execution of exercises.

Assessing Federal Capabilities – HSPD-8 defines the primary Federal interest in providing Federal preparedness assistance to State and local entities, which is to build operational readiness and capacity for major events, especially prevention of and response to threatened terrorist attacks. HSPD-8 also defines the primary Federal responsibility in maintaining specialized Federal assets for activities as set forth in the NRP. To assess Federal capabilities information will be collected on the readiness of Federal civil response assets through the Federal Response Capability Inventory.

Responsibilities:

- **DHS** – Assess the readiness of Federal civil response assets through the Federal Response Capability Inventory.
- **Federal** – Participate in the update and maintenance of the Federal Response Capability Inventory in accordance with guidance to be provided by DHS.

4.2 Preparedness Strategies Addendum

According to HSPD-8: *“...To the extent permitted by law, Federal preparedness assistance will be predicated on adoption of statewide comprehensive all-hazards preparedness strategies. The strategies should be consistent with the National Preparedness Goal, should assess the most effective ways to enhance preparedness, should address regions facing higher risk, especially to terrorism, and should also address local government concerns and Citizen Corps efforts. The Secretary, in coordination with the heads of other appropriate Federal departments and agencies, will review and approve strategies submitted by the States. To the extent permitted by law, adoption of approved statewide strategies will be a requirement for receiving Federal preparedness assistance at all levels of government by September 30, 2005.”*

For year one of HSPD-8 implementation (FY 2005), the process will require States and Urban Areas to validate and/or update their existing FY 2003 State Homeland Security Strategies (SHSS) with an addendum. The FY 2006 SLGCP State Homeland Security Assessment and Strategy (SHSAS) process will allow States and Urban Areas to update their State Homeland Security Strategy to reflect the National Planning Scenarios, National Priorities, and local government concerns and Citizen Corps efforts, as required in HSPD-8. Specifically, States and Urban Areas will be asked to bring their existing strategic goals and objectives into alignment with the National Priorities.

More specific instruction will be provided to States and Urban Areas through information bulletins, technical assistance and other means to complete the State Homeland Security Strategy addendum.

Responsibilities:

- **DHS** – Coordinate the review and approval of State Homeland Security Strategies as a requirement of allocating Federal preparedness assistance.
- **States and Urban Areas** –
 - *Validate* existing data provided to ensure strategy discusses local government concerns and citizen preparedness, current mutual aid agreements, and reflects the National Planning Scenarios.
 - *Update* existing data provided in SHSS Section 4 – Goals, Objectives, and Implementation Steps. Update to reflect:
 - Review of goals, objectives, and steps to ensure they are up-to-date and reflect the strategic plan for the State or Urban Area;
 - If applicable, any new or revised goals, objectives, or steps;
 - Alignment of goals, objectives, and steps to National Priorities; and
 - Awareness of 36 capabilities as demonstrated through the alignment of goals, objectives, and steps to National Priorities.
 - *Submit* updated State/Urban Area Strategies to DHS/SLGCP by September 30, 2005.

4.3 Schedule

These requirements are sequenced in such a manner as to facilitate the preparation and submission of the FY 2006 HSGP application. As Figure 8 indicates, many of the activities described in this Section occur concurrently, but all support each other in building a stronger foundation in a capabilities-based approach to developing Preparedness Assessments and Strategies.

Figure 8: Schedule for Preparedness Assessments and Strategies

Date	Activity
April 2005	Interim National Preparedness Goal and Guidance Issued Representative Sampling of Capability Begins
Spring/Summer 2005	Needs Assessment Guidance Issued
September 30, 2005	States/Urban Areas Submit Strategy Addendum Representative Sampling of Capability Complete
November 2005	FY 2006 Grant Guidance Issued (dependent on Appropriations date)
January/February 2006	Anticipated FY 2006 Grant Applications Due Date (dependent on Appropriations date)
April 1, 2006	FY 2006 Annual Report to the President

5.0 PRIVATE AND NON-GOVERNMENTAL ENTITIES AND CITIZENS

HSPD-8 requirements are directed at Federal, State, local, and tribal government entities, which are responsible and accountable for improving national preparedness. The Interim Goal states: *“To prepare as a Nation, HSPD-8 recognizes that, in addition to their direct role in preparedness, government entities must find ways to encourage active participation and involvement of private and non-governmental entities and citizens in national preparedness wherever possible.”* The following sections outline potential roles and responsibilities for these important partners.

5.1 Private Sector

Private sector entities across all industries have a stake in the safety and security of the workplace and the communities they serve. As a partner in homeland security, the private sector has a responsibility in four critical areas:

- **Business Continuity Planning** – As an integral part of the economic viability of an area and a source of income and stability for their employees, businesses have a responsibility to develop business continuity plans to ensure that the valuable assets of the company are protected, to lessen the impact of a major disaster, and to facilitate the recovery process.
- **Public Education and Training** – In addition to business continuity planning, the private sector is also an important conduit to inform and to help prepare and train citizens, including employees and their families, and the surrounding community. To fulfill this important role, many companies are now offering on-site first aid and Community Emergency Response Team training; creating shelter-in-place plans; improving company alert and warning systems; strengthening employee preparedness by hosting drills and advocating the importance of disaster supplies kits and family communications plans; and sponsoring community outreach.
- **Critical Infrastructure Industries Interface and Ownership** – Businesses that own or interface with the Nation’s Critical Infrastructure have a heightened responsibility for business continuity and for security measures. Businesses in this critical arena should implement all reasonable measures to protect the safety and security of the asset or function and should be encouraged to build in redundancies and contingencies to ensure continued operations or minimal impact from disasters or attacks.
- **Information Sharing and Resource Assistance** – As a potential source for intelligence of national significance, the private sector also has a critical role to play in information sharing and must be an integral part of the information sharing system. In addition, resources held in the private sector may be of critical importance in the response and recovery stages of a large scale event. Private sector resources need to be catalogued and typed for potential use by the government, with a mechanism and process for deployment.

5.2 Non-Governmental Organizations

Nongovernmental Organizations (NGO) with disaster-related missions play a critical role in the nation's prevention, response, and recovery activities. A planned and coordinated approach is required to achieve capacity development necessary for implementation of the National Preparedness Goal. Therefore, Federal, State, local, and tribal governments are strongly encouraged to partner with NGOs to leverage expertise, share specialized assets, enhance capacity, and operate cohesively and effectively. Such partnerships will improve the response to and management of a complete spectrum of incidents and emergencies. In accordance with the NRP and the NIMS, an NGO is defined as *“An entity with an association that is based on interests of its members, individuals, or institutions and that is not created by a government, but may work cooperatively with government. Such organizations serve a public purpose, not a private benefit. Examples of NGOs include faith-based charity organizations and the American Red Cross.”*

NGOs:

- Provide vital services and possess unique planning, preparedness, and response expertise to help ensure the public's needs and expectations are met during the life cycle of a disaster;
- Mobilize and add significant resources to all-hazards disaster preparedness and response including personnel, equipment, and materials;
- Engage a broad spectrum of trained volunteers to perform their missions while working collaboratively with governmental and private sector partners; and
- Assist with managing unaffiliated and spontaneous volunteers at disasters sites.

The range of services provided by NGOs encompass a variety of activities focused on, but not limited to sheltering, feeding and related human services, as well as volunteer and donation management. For example, under the NRP, the American Red Cross serves as primary agency for Mass Care (Emergency Support Function #6) responsible for food, shelter, emergency first aid, disaster welfare information, and bulk distribution of emergency relief items. NGOs also specialize in community disaster education and disaster information dissemination to empower the public in the event of disaster. These activities lessen the burden upon the first response community and Federal, State, and local government agencies. A more prepared public ultimately reduces the economic impact and human loss associated with disasters.

Experienced NGOs have internal guidelines, standard operating procedures, and performance standards that define the scope and range of the services provided to the American public. These guidelines and procedures are designed to maximize the ability to provide disaster services without subjecting NGOs to excessive risk and legal liability. NGOs can not legally be required to provide services outside the scope of their internal operating procedures and mission. Additionally, NGOs can not be required to provide services beyond the presently defined scope of responsibility under the NRP, as agreed to by the signatories of the NRP.

NGOs with disaster-related missions should be included as integral partners in, but not limited to:

-
- Local, State, and Federal advisory councils;
 - State Homeland Security Strategies;
 - Urban Area Homeland Security Strategies;
 - Local, State, regional, and Federal response planning and training;
 - Exercise design and execution;
 - Resource allocation, where permissible, to address specific gaps, excesses, and deficiencies;
 - Real world incident response;
 - Public education and outreach;
 - Training the public in preparedness and emergency response skills; and
 - Managing volunteers during disasters.

5.3 Citizens

The American people are the ultimate stakeholders in the homeland security mission and must be an integral component of national preparedness efforts. As such, the communication, outreach, and educational components of preparedness must address the needs and meet the expectations of the American people. Additionally, roles and responsibilities for citizens will be integrated with the other stakeholder groups through the National Preparedness Goal, National Planning Scenarios, UTL, and TCL. In 95 percent of all emergencies, bystanders or victims themselves are the first to provide emergency assistance or to perform a rescue on the scene. Therefore, citizens should be trained in emergency prevention, response, and recovery skills, and they should maintain these skills to help others in a crisis.

Specifically, the American people should have:

- **A Clear Understanding of National Preparedness** – True preparedness rests not only in the hands of the preparedness community, but also with the citizens throughout the Nation. Successful prevention, protection, response, and recovery depend upon citizens having a clear understanding of what it means to be prepared, what the state of preparedness is at a national level, how to help prevent incidents from happening, and how to respond should an event occur.
- **Regular Outreach and Communication** – With an ever-changing threat environment, the American people rely upon the Federal, State, and local governments to keep them informed and protected. Regular public outreach and communication from governments and other sources, including the media, the private sector, and schools, will reiterate the importance of being informed and taking action to be better prepared. This will also facilitate coordinated response and recovery should a major event occur. To effectively reach the public, a focused and consistent message needs to be disseminated through various mediums.
- **Alerts, Warnings, and Crisis Communication** – Citizens must also have a process to be informed when a threat is imminent or when an attack or other disaster has occurred.

-
- Opportunities to Be Involved – Citizens need training in emergency skills and opportunities to be a part of the system through volunteer service to support local first responders on an on-going basis and during an event. With the added support of citizens, emergency service providers will have more time to fulfill their highly skilled responsibilities in keeping the Nation safe or in responding to an event.

To achieve the active citizen participation in preparedness called for in HSPD-8, DHS coordinates Citizen Corps, the nationwide grass roots movement to provide local preparedness information, training and volunteer opportunities, and to increase collaboration between citizens and emergency responders. The network of Citizen Corps partners includes other Federal departments and agencies, State and local governments, the private sector, NGOs, faith-based groups, and others. These entities will work together to raise public awareness concerning the importance of citizen participation, the steps everyone in America should take, and how citizens can be involved within their community, to include:

- Engaging in awareness and outreach campaigns to deliver the “*prepare, train, and volunteer*” message and motivate everyone in America to take action to reduce their vulnerability;
- Partnering with NGOs to expand citizen training and volunteer opportunities;
- Promoting DHS’s all-hazard mission and identifying key areas where citizens can assist local emergency responders;
- Focusing on unique requirements for people with disabilities, language barriers, tribal populations, youth, seniors, and other sectors;
- Developing standards, recognition incentives, and assessment and evaluation criteria for citizen preparedness and participation;
- Expanding the role of the private sector as a community stakeholder and as a delivery mechanism for citizen education, training, and volunteer service opportunities;
- Sharing lessons learned and best practices from communities around the country; and
- Integrating and institutionalizing citizen participation in all homeland security efforts, including State strategies, emergency operating plans, exercises (from local to national), critical infrastructure protection, and transportation security.

By engaging the public and by providing them with appropriate knowledge, skills, and abilities, government entities will bring the full resources of the country to bear on national preparedness.

6.0 ANNUAL STATUS REPORTS

HSPD-8 requires the Secretary of Homeland Security to provide the President with “*an annual status report of the Nation's level of preparedness, including State capabilities, the readiness of Federal civil response assets, the utilization of mutual aid, and an assessment of how the Federal first responder preparedness assistance programs support the national preparedness goal. The first report will be provided within 1 year of establishment of the national preparedness goal.*”

Reporting on the status of national readiness entails synthesizing a high volume and many different types of data:

- Data on State capabilities and utilization of mutual aid will be collected through the DHS Homeland Security Grant Program (HSGP), grant programs of other Federal departments and agencies, such as the HHS, and other sources. Data on State capabilities and utilization of mutual aid for annual reports for FY 2006 and 2007 will be based on limited re-assessment of previously collected data, and representative sampling for the capability-specific National Priorities. A comprehensive update of State Homeland Security Assessments and Strategies under the DHS HSGP using the standard planning tools for the Interim National Preparedness Goal (National Planning Scenarios, UTL, and TCL), is tentatively planned to begin in FY 2006 (pending funding); full results would be available for the annual report on assistance programs to the President in FY 2008.
- Data on the readiness of Federal civil response assets will be collected from the Federal response capability inventory required in HSPD-8 (to be completed in FY 2005).
- Data on how Federal first responder preparedness assistance programs support the National Preparedness Goal will be collected from the annual report to the Secretary of Homeland Security required in HSPD-8.

HSPD-8 states that the President is the primary audience for the annual report. However, DHS recognizes that the store of data collected as the input to the annual report will serve multiple audiences. The information collected through the reporting process will offer a wealth of information in various formats, channels, and levels of granularity to decision makers and stakeholders at all levels. In addition to the President, stakeholders include Congress, Federal, State, local, tribal, private, and non-governmental entities, and the general public.

The annual report will enable Federal, State, local, and tribal leaders to better understand the “as-is” and “to-be” state of national preparedness. The initial report will focus on the National Priorities. Ultimately, the report will provide a comprehensive portrait that details national progress in meeting the Nation’s preparedness goal, while highlighting important national readiness trends, gaps, and requirements.

7.0 CONCLUSION

The security of our homeland depends upon the thousands of men and women hard at work at all levels of government, across all disciplines, in the private and non-profit sectors, and in large and small communities throughout this great Nation. In conjunction with the Interim National Preparedness Goal, this National Preparedness Guidance is the culmination of a collaborative process involving thousands of those hardworking Americans. While much work has been done, much work remains to be done.

The strategic thrust of the Interim National Preparedness Goal and Guidance is to radically transform how we go about the long and arduous task of securing our homeland in a resource-constrained and ever-changing threat environment. By focusing on building the appropriate levels of capabilities in jurisdictions across the United States, we aim to prioritize our limited resources in a manner that achieves the highest assurances possible that our homeland is as secure as we can make it in as little time as practicable. We know we cannot be totally secure, and we know we cannot be totally prepared. But, we must strive with all of the ingenuity and industry we have to meet our solemn obligation to not just create a better prepared America, but the best prepared America we can.

APPENDIX A—TERMS AND DEFINITIONS

All-Hazards Preparedness. Refers to preparedness for domestic terrorist attacks, major disasters, and other emergencies. (Source—HSPD-8)

Capability. A capability provides the means to accomplish one or more tasks under specific conditions and to specific performance standards. A capability may be delivered with any combination of properly planned, organized, equipped, trained, and exercised personnel that achieves the intended outcome.

Critical Task. Critical tasks are defined as those prevention, protection, response, and recovery tasks that require coordination among an appropriate combination of Federal, State, local, tribal, private sector, and non-governmental entities during a major event in order to minimize the impact on lives, property, and the economy.

Emergency. As defined by the *Robert T. Stafford Disaster Relief and Emergency Assistance Act*, an emergency means any occasion or instance for which, in the determination of the President, Federal assistance is needed to supplement State and local efforts and capabilities to save lives and to protect property and public health and safety, or to lessen or avert the threat of a catastrophe in any part of the United States. (Source—NRP, December 2004)

Emergency Response Provider. Includes Federal, State, local, and tribal emergency public safety, law enforcement, emergency response, emergency medical (including hospital emergency facilities), and related personnel, agencies, and authorities. (See section 2(6), Homeland Security Act of 2002, Public Law 107-296, 116 Stat. 2135 (2002).) Also known as Emergency Responder. (Source—NIMS, March 2004)

Federal departments and agencies. Those executive departments enumerated in 5 U.S.C. 101, and the Department of Homeland Security; independent establishments as defined by 5 U.S.C. 104(1); Government corporations as defined by 5 U.S.C. 103(1); and the United States Postal Service. (Source—HSPD-8)

First responder. Local and nongovernmental police, fire, and emergency personnel who in the early stages of an incident are responsible for the protection and preservation of life, property, evidence, and the environment, including emergency response providers as defined in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101), as well as emergency management, public health, clinical care, public works, and other skilled support personnel (such as equipment operators) who provide immediate support services during prevention, response, and recovery operations. First responders may include personnel from Federal, State, local, tribal, or nongovernmental organizations. (Source—NRP, December 2004)

Incident of National Significance. Based on criteria established in HSPD-5 (paragraph 4), an actual or potential high-impact event that requires a coordinated and effective response by an appropriate combination of Federal, State, local, tribal, nongovernmental, and/or private sector entities in order to save lives and minimize damage, and provide the basis for long-term community recovery and mitigation activities. (Source—NRP, December 2004)

Jurisdiction. A range or sphere of authority. Public agencies have jurisdiction at an incident related to their legal responsibilities and authority. Jurisdictional authority at an incident can be political or geographic (e.g., city, county, tribal, State, or Federal boundary lines) or functional (e.g., law enforcement, public health). (Source—NIMS, March 2004)

Local Government. Local means “(A) a county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, or agency or instrumentality of a local government; (B) an Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and (C) a rural community, unincorporated town or village, or other public entity.” (Source—Homeland Security Act of 2002)

Major Disaster. As defined under the *Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122)*, a major disaster is any natural catastrophe (including any hurricane, tornado, storm, high water, wind-driven water, tidal wave, tsunami, earthquake, volcanic eruption, landslide, mudslide, snowstorm, or drought) or, regardless of cause, any fire, flood, or explosion, in any part of the United States, which in the determination of the President causes damage of sufficient severity and magnitude to warrant major disaster assistance under this act to supplement the efforts and available resources of States, local governments, and disaster relief organizations in alleviating the damage, loss, hardship, or suffering caused thereby. (Source—NIMS, March 2004)

Major Event. Refers to domestic terrorist attacks, major disasters, and other emergencies. (Source—HSPD-8)

National. Of a nationwide character, including the Federal, State, local, and tribal aspects of governance and polity. (Source—NIMS, March 2004)

Performance goal. A statement of the intended result, effect, or consequence to be achieved by carrying out a program or activity.

Performance measure. A quantitative or qualitative characteristic used to gauge the results of an outcome compared to its intended purpose (e.g., percentage, time, or amount).

Performance metric. A particular value or characteristic used to measure the outcome (e.g., “100,” “25,” or “partially”) that is generally expressed in terms of a baseline and a target.

Preparedness. The range of deliberate, critical tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, respond to, and recover from domestic incidents. Preparedness is a continuous process involving efforts at all levels of government and between government and private-sector and nongovernmental organizations to identify threats, determine vulnerabilities, and identify required resources. (Source—NRP, December 2004)

Prevention. Actions to avoid an incident or to intervene to stop an incident from occurring. Prevention involves actions taken to protect lives and property. It involves applying intelligence and other information to a range of activities that may include such countermeasures as deterrence operations; heightened inspections; improved surveillance and security operations; investigations to determine the full nature and source of the threat; public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and, as appropriate, specific law enforcement operations aimed at deterring, preempting, interdicting, or disrupting illegal activity and apprehending potential perpetrators and bringing them to justice. (Source—NIMS, March 2004)

Recovery. The development, coordination, and execution of service- and site-restoration plans, the reconstitution of government operations and services; individual, private-sector, nongovernmental, and public assistance programs to provide housing and promote restoration; long-term care and treatment of affected persons; additional measures for social, political, environmental, and economic restoration; evaluation of the incident to identify lessons learned; post incident reporting; and development of initiatives to mitigate the effects of future incidents. (Source—NIMS, March 2004)

Region. As used in this document, “region” generally refers to a geographic area consisting of contiguous State, local, and tribal entities located in whole or in part within a designated planning radius of a core, high threat Urban Area. The precise boundaries of a region are self-defined.

Response. Activities that address the short-term, direct effects of an incident. Response includes immediate actions to save lives, protect property, and meet basic human needs. Response also includes the execution of emergency operations plans and of mitigation activities designed to limit the loss of life, personal injury, property damage, and other unfavorable outcomes. As indicated by the situation, response activities include applying intelligence and other information to lessen the effects or consequences of an incident; increased security operations; continuing investigations into the nature and source of the threat; ongoing public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and specific law enforcement operations aimed at preempting, interdicting, or disrupting illegal activity, and apprehending actual perpetrators and bringing them to justice. (Source—NIMS, March 2004)

Risk. Risk is the product of threat, vulnerability, consequence, and likelihood of occurrence.

State Government. State means “any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States.” (Source—Homeland Security Act of 2002)

System. A combination of facilities, equipment, personnel, procedures, and communications integrated into a common organizational structure to achieve a mission or outcome.

Target Capabilities List. Provides guidance on the specific capabilities and levels of capability that Federal, State, local, and tribal entities will be expected to develop and maintain.

Tier. Groupings of jurisdictions that account for reasonable differences in expected capability levels among entities based on assessments of total population, population density, critical infrastructure, and other significant risk factors.

Universal Task List. A menu of tasks from all sources that may be performed in major events such as those illustrated by the National Planning Scenarios. Entities at all levels of government should use the UTL as a reference to help them develop proficiency through training and exercises to perform their assigned missions and tasks in major events.

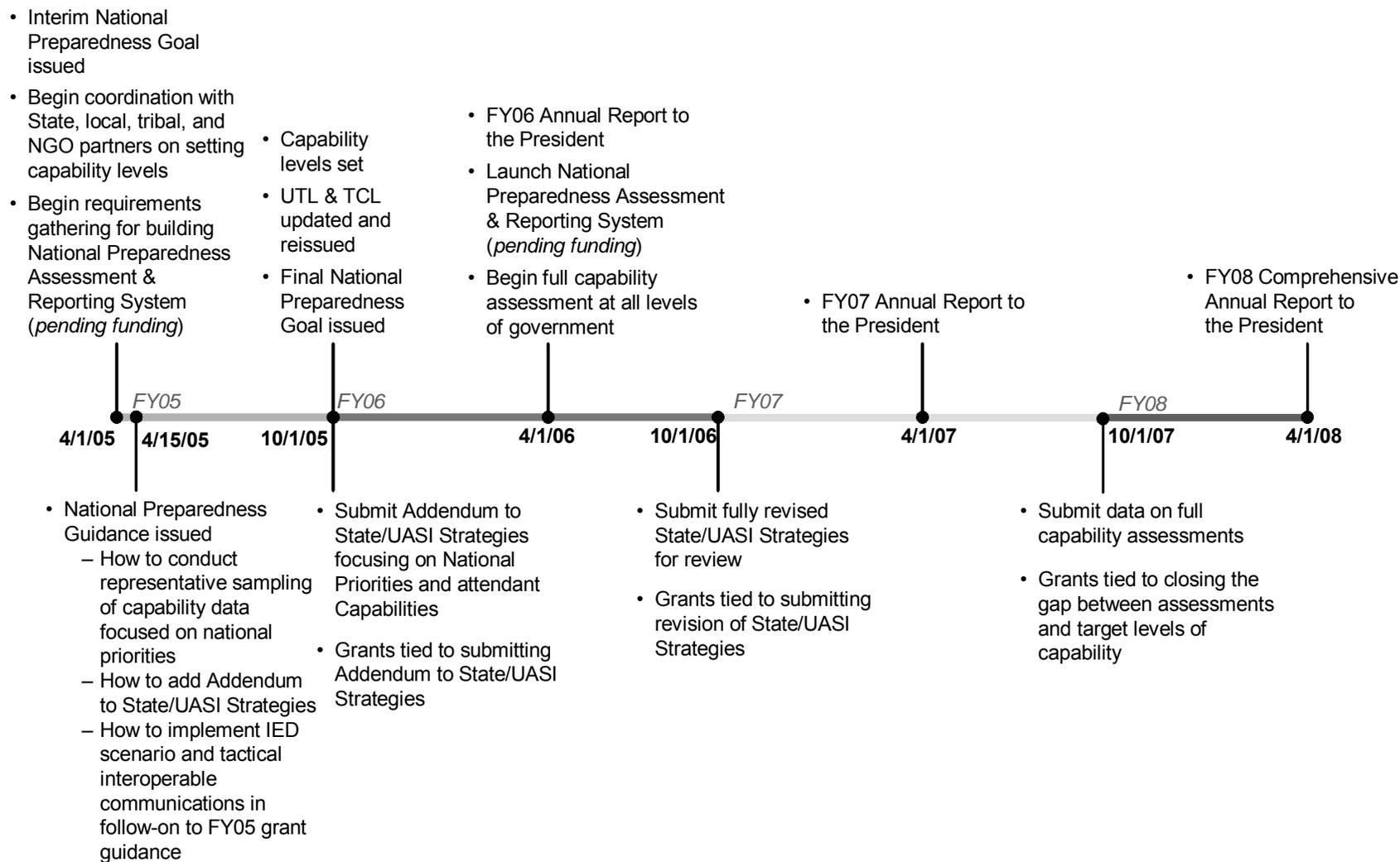
Volunteer. Any individual accepted to perform services by an agency, which has authority to accept volunteer services when the individual performs services without promise, expectation, or receipt of compensation for services performed (See, for example, 16 U.S.C. 742f(c) and 29 CFR 553.101.) (Source—NIMS, March 2004)

APPENDIX B—ACRONYMS AND ABBREVIATIONS

CBRNE	Chemical Biological Radiological Nuclear Explosive
CDC	Centers for Disease Control and Prevention (HHS)
CIP	Critical Infrastructure Protection
CI/KR	Critical Infrastructure and Key Resources
COPS	Office of Community Oriented Policing Services (DOJ)
CSID	Central Scheduling and Information Desk
DHS	Department of Homeland Security
DOJ	Department of Justice
EMS	Emergency Medical Service
EOC	Emergency Operations Center
ESF	Emergency Support Function
FBI	Federal Bureau of Investigation (DOJ)
FEMA	Federal Emergency Management Agency (DHS)
FY	Fiscal Year
HHS	Department of Health and Human Services
HRSA	Health Resources and Services Administration (HHS)
HSEEP	Homeland Security Exercise and Evaluation Program
HSGP	Homeland Security Grant Program
HSPD	Homeland Security Presidential Directive
ICS	Incident Command System
IED	Improvised Explosive Device
IWN	Integrated Wireless Network
JTTF	Joint Terrorism Task Force
LEISP	Law Enforcement Information Sharing Program
LLIS	Lessons Learned Information Sharing System
MAA	Mutual Aid Agreement
NIJ	National Institute of Justice (DOJ)
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NJTTF	National Joint Terrorism Task Force
NRP	National Response Plan
ODP	Office for Domestic Preparedness (DHS)

SAA	State Administrative Agency
SAFECOM	Safety Interoperable Communications Program
SHSAS	State Homeland Security Assessment and Strategy
SHSS	State Homeland Security Strategy
SLGCP	Office of State and Local Government Coordination and Preparedness (DHS)
SSA	Sector Specific Agency
SSP	Sector-Specific Plan
TCL	Target Capabilities List
UASI	Urban Areas Security Initiative
UTL	Universal Task List
WMD	Weapon of Mass Destruction

APPENDIX C—NATIONAL PREPAREDNESS IMPLEMENTATION TIMELINE



THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D—REQUIREMENTS CHECKLISTS

D.1 Federal Requirements CHECKLIST			
#	Item	Yes	No
Capabilities-Based Planning			
	Is DHS maintaining the National Planning Scenarios?		
	Has DHS coordinated the development and maintenance of the TCL including setting the risk-based target levels of performance required for each capability and assigning them to Tiers and levels of government? Has DHS also coordinated the continual refinement of the Tier System?		
	Has DHS, in coordination with stakeholders throughout the preparedness community, developed and maintained the UTL and critical tasks?		
	Has DHS coordinated full development of the capability and needs assessment processes?		
	Has DHS coordinated issuance of guidance on the development of State Homeland Security Strategies, and coordinated Federal review and approval?		
	Has DHS coordinated issuance of detailed guidance on performance assessments?		
	Has DHS submitted to the President an annual status report of the Nation's level of preparedness, including State capabilities, the readiness of Federal civil response assets, the utilization of mutual aid, and an assessment of how the Federal first responder preparedness assistance programs support the national preparedness goal? (The first report is to be on April 1, 2006)		
	Have Federal departments and agencies used the UTL as a reference to develop homeland security training, exercise, and preparedness assistance programs?		
	Have Federal entities used the UTL as a reference to develop proficiency through training and exercises for the critical tasks that they will be required to perform in major events?		
	Have Federal entities used the National Planning Scenarios as a reference to help them evaluate and improve their capabilities to perform their assigned missions and tasks in major events?		
	Have Federal departments and agencies applied the TCL in applicable training, exercise, and preparedness assistance programs? Have Federal departments and agencies developed and maintained certain target levels of capabilities?		
	Have all Federal departments and agencies assessed whether they possess the required capabilities assigned to them?		
	As required by HSPD-8, has Federal preparedness assistance been predicated on adoption of all-hazards State Homeland Security Strategies?		
	Have all Federal departments and agencies provided input into the annual status report, and where applicable, participated in national exercises to evaluate performance?		
	Have Federal departments and agencies updated their preparedness assistance programs to better support achievement of the Goal?		
National Priority: Implement the NIMS and NRP			
	Have Federal departments and agencies incorporated key NIMS and NRP concepts and procedures for working with NRP organizational elements when developing or updating incident management and emergency response plans?		

D.1 Federal Requirements CHECKLIST			
#	Item	Yes	No
National Priority: Expanded Regional Collaboration			
	In the Final National Preparedness Goal released October 1, 2005, did DHS include the standardized national Tier System for grouping jurisdictions/sub-State regions to account for differences in levels of capability based on risk factors, such as total population, population density, and presence of critical infrastructure?		
National Priority: Implement the Interim NIPP			
	Has DHS undertaken an outreach effort to engage all the stakeholders necessary to utilize, refine, and continue to develop milestones and performance measures to assess national-level and sector by-sector progress? Has DHS also continued to enhance its programs in information analysis and infrastructure protection and integrate these efforts under the framework of the NIPP?		
	Have the SSAs begun implementing the SSPs, tracking progress on the initiatives outlined in the SSPs, and working with all their respective stakeholders?		
	Have the SSAs utilized, refined, and continued to develop milestones and performance measures to assess progress in each sector?		
	Have supporting departments and agencies worked with the SSAs to implement the SSPs and participate in sector-specific activities through the Government Coordinating Councils?		
National Priority: Strengthen Information Sharing and Collaboration			
	Has DHS expanded access to and use of the Homeland Security Information Network (HSIN)? The goal is to deploy HSIN to all States and UASI Urban Areas to strengthen the two-way flow of real time threat information at the Sensitive-but-Unclassified level through the classified SECRET levels by the end of FY 2007.		
	Has DOJ implemented the LEISP strategy?		
	Has DOJ implemented short-term solutions to enhance information sharing throughout the Federal government and with the rest of the law enforcement community (e.g., connecting Regional Information Sharing Systems, Law Enforcement Online, and HSIN)?		
	Has DOJ pursued long-term information sharing strategies to present a single, unified source for DOJ data to other Federal departments and agencies as well as State and local partners (e.g., R-DEX and N-DEX)?		
	Has DOJ adopted consistent department-wide policies and procedures to protect the privacy of individuals and the security of information it shares?		
National Priority: Strengthen Interoperable Communications			
	Has SAFECOM continued to coordinate the efforts of Federal, State, local, and tribal public safety agencies?		
	Have Federal departments and agencies consolidated communications systems and implemented emerging standards to ease interconnectivity with State and local systems?		
	Have Federal departments and agencies coordinated and targeted grant and technical assistance consistent with guidance provided by SAFECOM?		
Preparedness Assessments and Strategies			
	Has DHS coordinated review and approval of the submitted compliance checklists?		
	Have Federal entities demonstrated, as appropriate, compliance with applicable requirements highlighted in the National Preparedness Guidance?		

D.1 Federal Requirements CHECKLIST

#	Item	Yes	No
	Has DHS Coordinated the Capability Assessment process and mapped existing assessment data to the National Priorities?		
	Have Federal entities supported the Capability Assessment process and provided information upon request on how their grantees are utilizing Federal preparedness assistance dollars?		
	Has DHS updated the HSEEP evaluation process in order to reflect the UTL and TCL?		
	Have Federal entities incorporated, as appropriate, the UTL, TCL and standardized After Action Reports into the design and execution of exercises?		
	Has DHS assessed the readiness of Federal civil response assets through the Federal Response Capability Inventory?		
	Have Federal entities participated in the update and maintenance of the Federal Response Capability Inventory in accordance with guidance to be provided by DHS?		
	Has DHS coordinated the review and approval of State Homeland Security Strategies as a requirement of allocating Federal preparedness assistance?		

D.2 State Requirements CHECKLIST

#	Item	Yes	No
Capabilities-Based Planning			
	Have State entities used the National Planning Scenarios as a reference to help them evaluate and improve their capabilities to perform their assigned missions and tasks in major events?		
	Have State entities used the UTL as a reference to develop proficiency through training and exercises for the critical tasks that they will be required to perform in major events?		
	Have State entities used the TCL to help them understand what capabilities are needed to perform their homeland security missions and what levels of capabilities they are being asked to develop and maintain?		
	Have State entities assessed capabilities against targets and defined needs in a manner consistent with their identified and prioritized gaps?		
	Has the State, as described in Section 4, in consultation with local and tribal entities, updated existing strategies?		
	Have State entities assessed performance through the process described in exercise or other guidance? Leveraging the findings of these assessments, have State decision makers utilized the results of preparedness reporting to guide future investments of preparedness funds?		
National Priority: Implement the NIMS and NRP			
	Are State entities adopting NIMS and NRP?		
	Are States ensuring that jurisdictions receiving Federal funds incorporate NIMS and NRP into existing training efforts?		
National Priority: Expanded Regional Collaboration			
	Did each State Administrative Agency (SAA): Analyze alternative geographic and jurisdictional composition options? Conduct an analysis of alternatives around the identified options? Select, at a minimum, a preferred regional geographic and jurisdictional option? (This applies to each of the 57 designated UASI Urban Areas, as well as at least one (1) multi-jurisdictional metropolitan area in each States without a designated UASI Urban Area.)		
National Priority: Implement the Interim NIPP			
	Have State entities been engaged by DHS and the SSAs to promote awareness of and provide feedback on the NIPP framework and to solicit their involvement in the National CIP program?		
	Have State entities worked with the appropriate SSAs to begin implementation of the SSPs for various sectors?		
National Priority: Strengthen Interoperable Communications			
	Did States that do not have a designated Urban Area identify a metropolitan area to develop and test a tactical interoperable communications plan? (This metropolitan area should be the same metropolitan area tasked with developing a Multi-Jurisdictional Prevention and Response Plan as part of the HSPD-8 implementation required by the FY 2005 HSGP guidance)		

National Priority: Strengthen Medical Surge and Mass Prophylaxis		
	For further information, please see the final HHS/CDC and HRSA guidance, which should be released in April-May 2005.	
Preparedness Assessments and Strategies		
	Have State entities submitted compliance checklists with FY 2006 Homeland Security Grant Program application?	
	Have State entities encouraged collaboration with DHS and other partners to more fully define and develop the Capability Assessment process?	
	Have State entities applied the HSEEP process and standardized After Action Reports as appropriate into their design and execution of exercises?	
	Have State entities validated existing data to ensure that the State Homeland Security Strategy discusses local government concerns and citizen preparedness, current mutual aid agreements, and reflects the National Planning Scenarios?	
	<p>Have State entities updated existing data provided in SHSS Section 4 – Goals, Objectives, and Implementation Steps – to reflect:</p> <ul style="list-style-type: none"> ▪ Review of goals, objectives, and steps to ensure they are up-to-date and reflect the strategic plan for the State or Urban Area? ▪ If applicable, any new or revised goals, objectives, or steps? ▪ Alignment of goals, objectives, and steps to National Priorities? ▪ Awareness of 37 capabilities as demonstrated through the alignment of goals, objectives, and steps to National Priorities? 	
	Have State entities submitted updated State Strategies to DHS/SLGCP by September 30, 2005?	

D.3 Urban Area Requirements CHECKLIST			
#	Item	Yes	No
Capabilities-Based Planning			
	Has the Urban Area, as described in Section 4, in consultation with local and tribal entities, updated its existing strategy?		
National Priority: Implement the NIMS and NRP			
	Are Urban Areas receiving Federal funds incorporating NIMS and NRP into existing training efforts?		
National Priority: Strengthen Information Sharing and Collaboration			
	As required by the FY 2005 Homeland Security Grant Program, did each Urban Area receiving UASI funds develop a Multi-Jurisdictional Prevention and Response Plan based on the IED National Planning Scenario by November 2005?		
	Within one year of the submission of the Multi-Jurisdictional Prevention and Response Plan, did each Urban Area complete a cycle of multi-jurisdictional exercise activities based on this plan?		
National Priority: Strengthen Interoperable Communications			
	Did the Urban Area receiving FY 2005 UASI funds develop and test a tactical interoperable communications plan?		
Preparedness Assessments and Strategies			
	Have Urban Area entities validated existing data to ensure that the Urban Area Homeland Security Strategy discusses local government concerns and citizen preparedness, current mutual aid agreements, and reflects the National Planning Scenarios?		
	Have Urban Area entities submitted compliance checklists with FY 2006 Homeland Security Grant Program application?		
	Have Urban Area entities encouraged collaboration with DHS and other partners to more fully define and develop the Capability Assessment process?		
	Have Urban Area entities applied the HSEEP process and standardized After Action Reports as appropriate into their design and execution of exercises?		
	Have Urban Area entities updated existing data provided in SHSS Section 4 – Goals, Objectives, and Implementation Steps – to reflect: <ul style="list-style-type: none"> ▪ Review of goals, objectives, and steps to ensure they are up-to-date and reflect the strategic plan for the State or Urban Area? ▪ If applicable, any new or revised goals, objectives, or steps? ▪ Alignment of goals, objectives, and steps to National Priorities? Awareness of 37 capabilities as demonstrated through the alignment of goals, objectives, and steps to National Priorities?		
	Have Urban Area entities submitted updated Urban Area Strategies to DHS/SLGCP by September 30, 2005?		

D.4 Local Requirements CHECKLIST

#	Item	Yes	No
Capabilities-Based Planning			
	Have local entities used the National Planning Scenarios as a reference to help them evaluate and improve their capabilities to perform their assigned missions and tasks in major events?		
	Have local entities used the UTL as a reference to develop proficiency through training and exercises for the critical tasks that they will be required to perform in major events?		
	Have local entities used the TCL to help them understand what capabilities are needed to perform their homeland security missions and what levels of capabilities they are being asked to develop and maintain?		
	Have local entities assessed capabilities against targets and defined needs in a manner consistent with their identified and prioritized gaps?		
	Have local entities assessed performance through the process described in exercise or other guidance? Leveraging the findings of these assessments, have decision makers utilized the results of preparedness reporting to guide future investments of preparedness funds?		
National Priority: Implement the NIMS and NRP			
	Are local jurisdictions receiving Federal funds incorporating NIMS and NRP into existing training efforts?		
	Is the Incident Command System used at the local level fully-compliant with the NIMS-approved ICS, enabling jurisdictions to work together smoothly following an incident?		
National Priority: Implement the Interim NIPP			
	Have local entities been engaged by DHS and the SSAs to promote awareness of and provide feedback on the NIPP framework and to solicit their involvement in the National CIP program?		
	Have local entities worked with the appropriate SSAs to begin implementation of the SSPs for various sectors?		
National Priority: Strengthen Medical Surge and Mass Prophylaxis			
	For further information, please see the final HHS/CDC and HRSA guidance, which should be released in April-May 2005.		
Preparedness Assessments and Strategies			
	Have local entities encouraged collaboration with DHS and other partners to more fully define and develop the Capability Assessment process?		
	Have local entities applied the HSEEP process and standardized After Action Reports as appropriate into their design and execution of exercises?		

D.5 Tribal Requirements CHECKLIST			
#	Item	Yes	No
Capabilities-Based Planning			
	Have tribal entities used the National Planning Scenarios as a reference to help them evaluate and improve their capabilities to perform their assigned missions and tasks in major events?		
	Have tribal entities used the UTL as a reference to develop proficiency through training and exercises for the critical tasks that they will be required to perform in major events?		
	Have tribal entities used the TCL to help them understand what capabilities are needed to perform their homeland security missions and what levels of capabilities they are being asked to develop and maintain?		
	Have tribal entities assessed capabilities against targets and defined needs in a manner consistent with their identified and prioritized gaps?		
	Have tribal entities assessed performance through the process described in exercise or other guidance? Leveraging the findings of these assessments, have decision makers utilized the results of preparedness reporting to guide future investments of preparedness funds?		
National Priority: Implement the NIMS and NRP			
	Are tribal entities receiving Federal funds incorporating NIMS and NRP into existing training efforts?		
National priority: Implement the Interim NIPP			
	Have tribal entities been engaged by DHS and the SSAs to promote awareness of and provide feedback on the NIPP framework and to solicit their involvement in the National CIP program?		
	Have tribal entities worked with the appropriate SSAs to begin implementation of the SSPs for various sectors?		
National Priority: Strengthen Medical Surge and Mass Prophylaxis			
	For further information, please see the final HHS/CDC and HRSA guidance, which should be released in April-May 2005.		
Preparedness Assessments and Strategies			
	Have tribal entities encouraged collaboration with DHS and other partners to more fully define and develop the Capability Assessment process?		
	Have tribal entities applied the HSEEP process and standardized After Action Reports as appropriate into their design and execution of exercises?		