



Interim

National Preparedness Goal

Rollout Conference



**Homeland
Security**

Using Capabilities-Based Planning

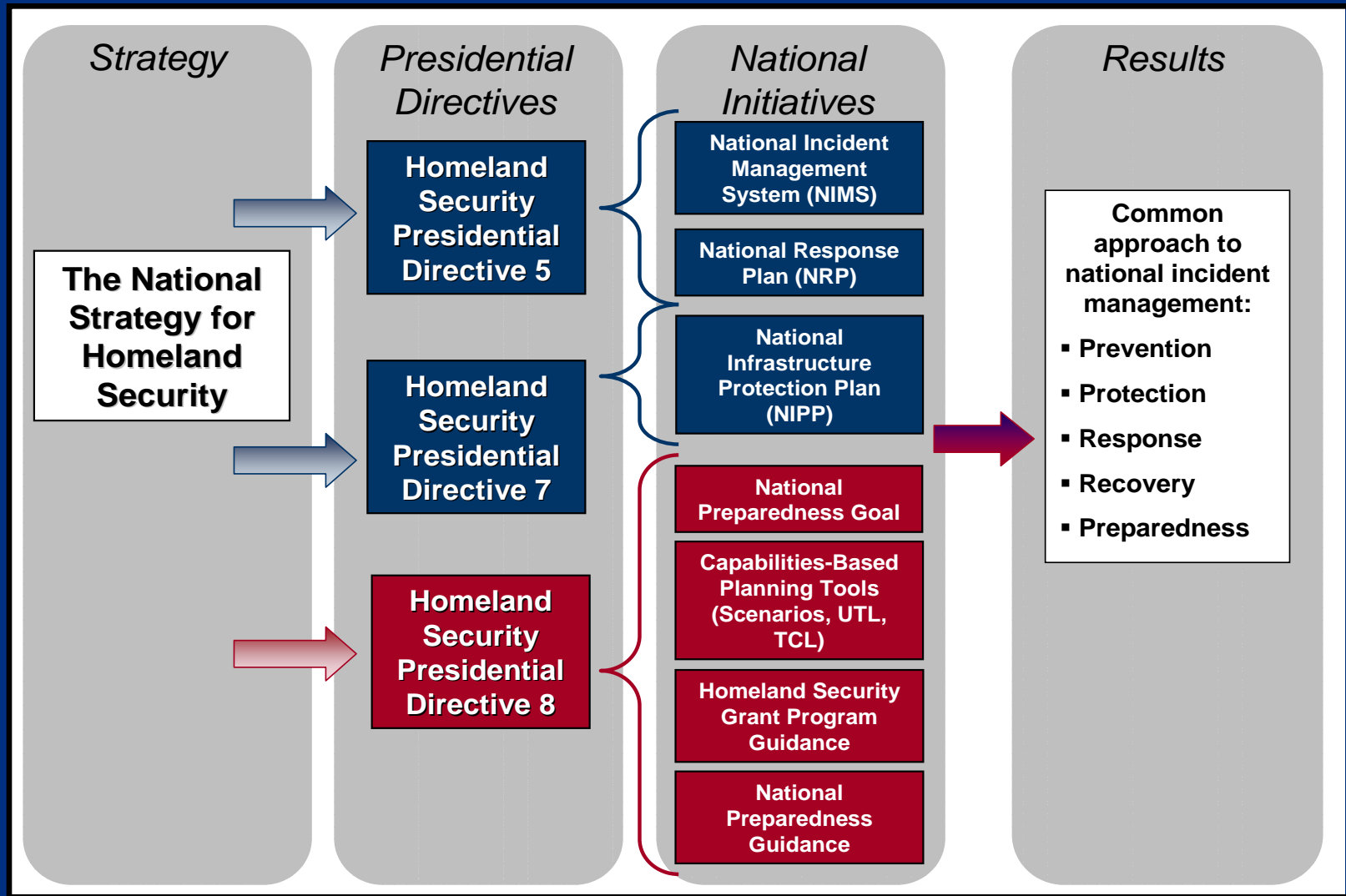
Lisa Weldon

Chief, Policy and Planning Branch, Office of State and
Local Government Coordination and Preparedness



**Homeland
Security**

HSPD-8 in Context



What is the Goal?

- Vision
- Target Capabilities List (TCL)
- National Priorities

The Vision

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.

The Target Capabilities

Common

Planning

Interoperable Communications ★

Prevent Mission Area

Information Collection and Threat Detection

Intelligence Fusion and Analysis

Information Sharing and Collaboration ★

Terrorism Investigation and Apprehension

CBRNE Detection ★

Protect Mission Area

Risk Analysis

Critical Infrastructure Protection

Food and Agriculture Safety and Defense

Public Health Epidemiological Investigation and Testing

Citizen Preparedness and Participation

Respond Mission Area

On-Site Incident Management

Emergency Operations Center Management

Critical Resource Logistics and Distribution

Volunteer Management and Donations

Worker Health and Safety

Public Safety and Security Response

Respond Mission Area (cont)

Firefighting Operations/Support

WMD/Hazardous Incident Response and Decontamination ★

Explosive Device Response Operations ★

Animal Health Emergency Support

Environmental Health and Vector Control

Citizen Protection: Evacuation and/or In-Place Protection

Isolation and Quarantine

Search and Rescue

Emergency Public Information and Warning

Triage and Pre-Hospital Treatment

Medical Surge ★

Medical Supplies Management and Distribution

Mass Prophylaxis ★

Mass Care (Sheltering, Feeding, and Related Services)

Fatality Management

Recover Mission Area

Structural Damage Assessment and Mitigation

Restoration of Lifelines

Economic and Community Recovery

National Priorities

Overarching Priorities

- Implement the NIMS and NRP
- Expanded Regional Collaboration
- Implement the National Infrastructure Protection Program (NIPP)

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



CBP: A 10-Step National Process

① What should we prepare for?

② What tasks need to be performed?

③ Which tasks are critical?

④ What capabilities are needed to perform the critical tasks?

⑤ What level of capability is needed to perform critical tasks for all scenarios?

⑥ How do we share responsibility to develop and maintain capabilities?

⑦ What capabilities are required?

⑧ Do we have adequate capabilities?

⑨ How should we allocate our resources to make the greatest improvements in preparedness?

⑩ How prepared are we?

What do we need as a Nation?

Where do we each stand?

How does it all fit together?



**Homeland
Security**

Where Do We Stand as a Nation?

1. **What should we prepare for?**
 - *National Planning Scenarios*
2. **What tasks need to be performed?**
 - *Universal Task List (UTL)*
3. **What tasks are critical?**
 - *UTL identifies critical tasks*
4. **What capabilities are needed to perform the critical tasks?**
 - *Target Capabilities List (TCL)*
5. **What level of capability is needed to perform the critical tasks for all scenarios?**
 - *TCL will define risk-based target levels of capability*
6. **How do we share responsibility to develop and maintain capabilities?**
 - *TCL will apportion levels of capabilities among levels of government and Tiers*



Where Do We Each Stand?

- 7. What capabilities are required?**
- *The TCL is organized by level of government and Tier*
 - *State, local, and tribal officials will identify groups of jurisdictions*
 - *Groups of jurisdictions will be assigned to Tiers*
- 8. Do we have adequate capabilities?**
- *Form working groups*
 - *Conduct capability assessments*
- 9. How should we allocate our resources to make the greatest improvements in preparedness?**
- *Conduct needs assessment*
 - *Amend preparedness strategy*
 - *Allocate resources*



How Does it All Fit Together?

10. How prepared are we?

- *Performance Assessment*
- *Consolidated Assessment (Compliance, Capability, Performance)*
- *Reporting (local to national)*

Capabilities-Based Planning

Capabilities-Based Planning IS:

- An iterative process
- All-hazards planning
- Risk-based
- Performance-based
- A better way to use existing resources

Capabilities-Based Planning IS NOT:

- A one-time event
- Planning for *every* hazard
- One size fits all
- A prescriptive resource list
- An unfunded mandate



What's in it for US?

- A streamlined processes for determining needs and framing requests for assistance
- A clearer voice for all stakeholders in shaping the system
- A more realistic picture of where we now stand in terms of national preparedness, and where we need to go



**Homeland
Security**

A Closer Look at the Capabilities-Based Planning Tools

Pat Malak

Chief, Policy Analysis Branch, Office of State and Local Government Coordination and Preparedness



**Homeland
Security**

Capabilities-Based Planning Tools

HSPD-8 requires “*actions to strengthen preparedness capabilities of Federal, State and local entities.*”

Three tools have been developed to address this requirement:

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



Capabilities-Based Planning

Scenarios

The National Planning Scenarios highlight the scope, magnitude, and complexity of plausible catastrophic terrorist attacks, major disasters, and other emergencies

Tasks

The Universal Task List (UTL) provides a menu of tasks from all sources that may be performed in major events such as those illustrated by the National Planning Scenarios

Capabilities

The Target Capabilities List (TCL) provides guidance on specific capabilities and levels of capability that Federal, State, local, and tribal entities will be expected to develop and maintain



National Planning Scenarios

The National Planning Scenarios define all-hazard events that exceed the capabilities of any single jurisdiction. The Scenarios help us:

- Answer the question *“How prepared do we need to be?”*
- Define the range and scope of incidents for which we must prepare
- Serve as basis for defining tasks and capabilities

National Planning Scenarios –Development

- Scenarios were developed under the leadership of the Homeland Security Council
- Developed by Federal Working Group
- Reviewed by subject-matter experts
- Designed as a planning tool that defines present-day threats and hazards of national significance with high credibility, consequence and probability
- Define representative incidents, rather than every possible threat



National Planning Scenarios

1. Improvised Nuclear Device
2. Aerosol Anthrax
3. Pandemic Influenza
4. Pneumonic Plague
5. Blister Agent
6. Toxic Industrial Chemicals
7. Nerve Agent
8. Chlorine Tank Explosion
9. Major Earthquake
10. Major Hurricane
11. Radiological Dispersal Device
12. Improvised Explosive Device
13. Food Contamination
14. Foreign Animal Disease
15. Cyber



National Planning Scenarios

Using the Scenarios

- Entities at all levels should use the scenarios as a planning tool to:
 - Evaluate and improve plans and capabilities
 - Design exercises that test a range of tasks and capabilities

Next Steps

- The scenarios will be reviewed periodically to determine if new scenarios need to be added



Universal Task List (UTL)

The UTL identifies “what” tasks need to be performed to prevent, protect against, respond to, and recover from incidents of national significance

- Provides entities flexibility to determine “who” will perform the task and “how”
- Defines tasks related to 4 missions: prevent, protect, respond, recover
- Identifies tasks that need to be performed by all disciplines across all levels of government and the private sector
- Provides a common language and reference system for all users
- Enhances communication between response agencies
- Contains approximately 1,600 unique tasks

No single jurisdiction or agency is expected to perform every task



**Homeland
Security**

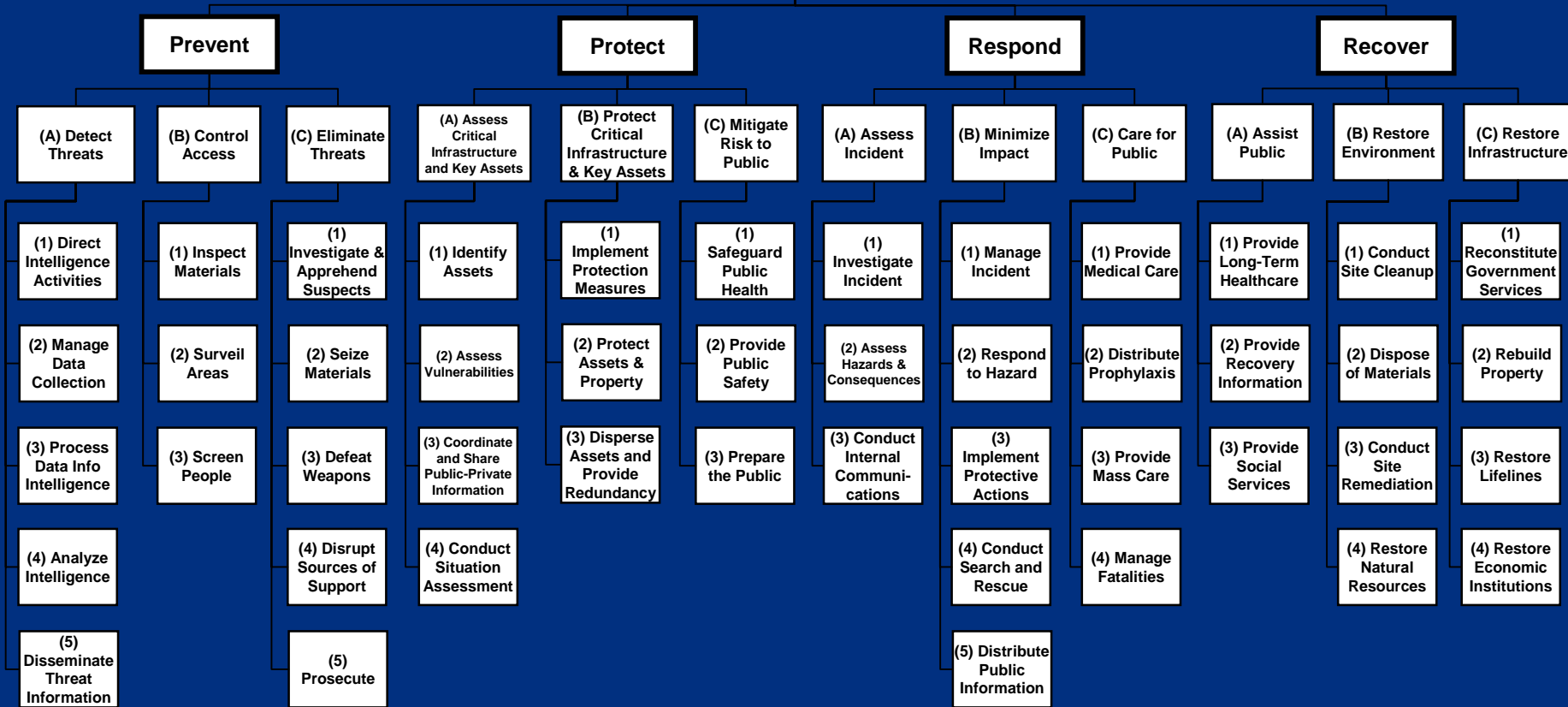
Universal Task List - Development

- Developed with extensive stakeholder involvement
- UTL Workshop in June 2004
- Tasks defined for each scenario
- Consolidated into Universal List – Over 80% of tasks are common across scenarios
- Distributed for broad review and input at several key points
- Regular consultation with State/Local/Tribal Working Group and Federal Working Group
- Consistent with NIMS, NRP, NIPP, HHS Guidelines, etc.



Universal Task List Taxonomy

All-Hazards Taxonomy of National Preparedness Tasks



Common Tasks: (A) Preparedness, (B) Resource Management, (C) Communications & Information Management, (D) Supporting Technology



Homeland Security

Universal Task List

Using the UTL

- Entities at all levels should use the UTL as a planning tool to:
 - Review plans to ensure the comprehensive list of homeland security tasks are addressed
 - Determine training requirements
 - Assess preparedness through evaluation of exercises

Universal Task List

Next steps

- Continue to identify tasks
- Develop definitions, conditions, measures
- Develop user-friendly, web-based database
- Map to training programs – enhance or develop new courses
- Develop exercise evaluation guides
- Establish process and schedule for updating the UTL

Target Capabilities List (TCL)

- The Target Capabilities List defines a National network of capabilities required to prevent, protect against, respond to, and recover from all hazard incidents of national significance
- The TCL will define target levels and assign responsibility for homeland security capabilities
- A capability is the combination of resources that provide the means to achieve a measurable outcome resulting from the performance of one or more critical tasks, under specified conditions and performance standards



Target Capabilities List

- Capabilities were derived from an analysis of *critical tasks* found in the UTL
 - Critical tasks are prevention, protection, response, and recovery tasks that require coordination across levels of government and with the private sector during a major event to minimize the impact on lives, property, and the economy.
- Capabilities are delivered with any combination of properly planned, organized, equipped, trained, and exercised personnel that achieve the expected outcome
- 36 Target Capabilities are defined in Version 1.0 of TCL

No single jurisdiction or agency is expected to have sufficient levels of every capability needed for a major event



Target Capabilities List

Common to all Mission Areas

- Planning
- Interoperable Communications

Prevent Mission Area

- Information Collection and Threat Detection
- Intelligence Fusion and Analysis
- Information Sharing and Collaboration
- Terrorism Investigation and Apprehension
- CBRNE Detection

Protect Mission Area

- Risk Analysis
- Critical Infrastructure Protection
- Food and Agriculture Safety and Defense
- Public Health Epidemiological Investigation and Testing
- Citizen Preparedness and Participation



Target Capabilities List

Response Mission Area

- On-Site Incident Management
- Emergency Operations Center Management
- Critical Resource Logistics and Distribution
- Volunteer Management and Donations
- Worker Health and Safety
- Public Safety and Security Response
- Firefighting Operations/Support
- WMD/Hazardous Incident Response and Decontamination
- Explosive Device Response Operations
- Animal Health Emergency Support
- Environmental Health and Vector Control
- Citizen Protection: Evacuation and/or In-Place Protection



Target Capabilities List

Response Mission Area (cont.)

- Isolation and Quarantine
- Search and Rescue
- Emergency Public Information and Warning
- Triage and Pre-Hospital Treatment
- Medical Surge
- Medical Supplies Management and Distribution
- Mass Prophylaxis
- Mass Care (Sheltering, Feeding, and Related Services)
- Fatality Management

Recover Mission Area

- Structural Damage Assessment and Mitigation
- Restoration of Lifelines
- Economic and Community Recovery



Target Capability Summaries

Each capability summary contains:

- Capability description
- Outcome
- ESF/Annex and UTL reference
- Associated critical tasks
- Capability and performance measures
- Capability elements (personnel, planning, organization and leadership, equipment and systems, training, exercises)
- Linked capabilities
- Event conditions



Target Capabilities List

Using the Target Capabilities List

- Entities at all levels should use the TCL as a planning tool to:
 - Define role in national network of homeland security capabilities
 - Define required capabilities
 - Establish priorities for use of limited resources
 - Develop mutual aid agreements



Target Capabilities List

Next Steps

- Establish target levels for capabilities
- Assign responsibility for building and maintaining the capabilities among federal, state, local, tribal governments, private sector, and non-government organizations
- Tailor capabilities to different tiers of local jurisdictions based on risk factors
- Refine capability and performance measures
- Refine capability elements

Target Capabilities List - Timeline

Early June 2005	Stakeholder Workshop to define requirements and process
June-July	Capability Work Groups to define capability target levels, tiers, measures, and elements
Late July	Stakeholder Workshop to provide recommendations from work groups
August	Broad stakeholder review and input
September 30	Release TCL: Version 2.0

For More Information

- An HSPD-8 information website that includes drafts of the UTL and TCL has been posted at <http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm>
- The UTL and TCL is available on the ODP Secure Portal at <https://odp.esportals.com> and *Lessons Learned Information Sharing* at <http://www.llis.gov>
- Input on UTL and TCL can be sent to: utl@dhs.gov



HSPD-8: Standards for Assessments and Strategies

Tim Beres

Director, Preparedness Programs Division, Office of State and Local Government Coordination and Preparedness



**Homeland
Security**

HSPD-8 Requirements

As stated in HSPD-8...

The National Preparedness Goal will establish “*standards for preparedness assessments and strategies, and a system for assessing the Nation's overall preparedness to respond to major events, especially those involving acts of terrorism.*”

Assessments, Strategies, and HSPD-8

1. Updating Homeland Security Strategies
2. Compliance Assessment
3. Needs Assessment
4. Capability Assessment
5. Performance Assessment



Near-Term: Updating Strategies

- States and Urban Areas will align goals and objectives in homeland security strategies with the seven National Priorities
 - Due date: September 30, 2005
- Element of iterative strategic planning process
- SLGCP will release specific guidance on how to go about updating the strategies
- In meantime, review Goal and Guidance to start drawing links between existing plans and National Priorities



Near-Term: Compliance Assessment

- Show compliance with requirements included in the National Preparedness Guidance
- Checklists consolidate all requirements into simple, easy-to-use list
 - Included as appendix to Guidance
- Checklists will be submitted with FY 2006 grant applications



Near-Term: Needs Assessment

- Evaluation of capabilities and investments will be a requirement for FY 2006 grant applications
- SLGCP will translate existing **capabilities** and **investment** information into new context of target capabilities for states
- Use that data to frame an analysis of the current state of the homeland security program
- States will make the business case for investments needed in FY 2006 to accomplish strategic goals and objectives
- SLGCP will provide additional guidance and detailed instructions



Long-Term: Capability Assessment

- Build a model process that incorporates peer review, onsite evaluation, and assessment of entire homeland security program
- Test process in representative sample of States and Urban Areas during CY 2005
- End product will fold tiers and target levels of capability into validated peer-review assessment process



Long-Term: Performance Assessments

- Homeland Security Exercise and Evaluation Program (HSEEP) will form the foundation of performance assessment process
- DHS updating HSEEP guidelines to integrate the Universal Task List and the Target Capabilities List
- Performance Assessments will be used to help validate achievement of target capability levels



Conclusion

- National Preparedness Goal and National Preparedness Guidance have built the framework
- Much work ahead to build out the national assessment system
- SLGCP will continue to collaborate with State, local, and tribal stakeholders to create a successful system
- Your assistance, feedback, and constructive criticism is crucial





National Incident Management System

Mike Kaminski

NIMS Integration Center



**Homeland
Security**

National Incident Management System

Homeland Security Presidential Directive - 5 :

Management of Domestic Incidents (February, 03)

Homeland Security Presidential Directive – 8 :

National Preparedness (December, 03)

- Complementary Presidential Directives
- Established national initiatives that develop a common approach to preparedness and response
- Each reinforces the other
- Applicable to Federal, State, tribal and local governments



**Homeland
Security**

National Incident Management System

Homeland Security Presidential Directive – 5:

Management of Domestic Incidents (February, 03)

Directed the development of:

- National Incident Management System (NIMS) (March, 04)
- National Response Plan (NRP) (January, 05)

National Incident Management System

NIMS:

- Represents core set of doctrines, concepts, terminologies
- Nationwide standardized approach for Federal, State, tribal and local governments
- Applicable to prevention, preparedness, response, recovery and mitigation
- Used for all domestic incidents regardless of cause, size or complexity

National Incident Management System

Components of NIMS:

- Command & Management
- Preparedness
- Resource Management
- Communications and Information Management
- Supporting Technologies
- Ongoing Management and Maintenance

National Incident Management System

NRP:

- Uses the comprehensive framework of NIMS
- Standardizes Federal incident management actions
- Applicable to all Federal departments and agencies
- All-hazards plan for integrating Federal resources before, during and after an Incident
- Activated for “Incidents of National Significance”

National Incident Management System

The National Preparedness Goal (The Goal) relationship to NIMS and NRP

A national priority established by The Goal:

- Implement the National Incident Management System and the National Response Plan nation – wide

The Goal and Target Capabilities List (TCL)

- Establishes measurable priorities and targets
(eg., On - Site Incident Management)
- Strengthens preparedness capabilities of Federal, State, tribal and local governments

National Incident Management System

NIMS Integration Center (NIC) Initiatives:

- Establishment of the NIC (May, 04)
- NIMS Compliance Guidance (September, 04)
- Resource Typing/National Glossary of Terms and Definitions
- NIMCAST (February, 05)
- NIMS National Standard Curriculum: Training Development Guidance (April, 05)
- Responsible for the NRP (February, 05)

National Incident Management System

The NIMS Integration Center:

- Gil Jamieson, Acting Director
- Web Page: www.fema.gov/nims
- E-Mail: NIMS-Integration-Center@dhs.gov
- NIMS Training: <http://training.fema/emiweb/IS/is700.asp>
- NRP Training: <http://training.fema/emiweb/IS/is800.asp>
- Main Number: 202-646-3850
- Mailing Address: NIMS Integration Center, 500 C Street SW,
Suite 706, Washington, DC 20472

Expanded Regional Collaboration

Tim Beres

Director, Preparedness Programs Division, Office of State and Local Government Coordination and Preparedness



**Homeland
Security**

Why Expanded Regional Collaboration?

Discussion from the Interim Goal

- Extensive regional collaboration required
- Risk-based approach is necessary
- Investment prioritization toward high-risk areas
- Regional approaches increase return on investment

Requirements

Overview

- Requirements apply initially to UASI areas and at least 1 metropolitan area in States with no UASI area
- Planning considerations provided, but no “one size fits all” requirements from DHS
- Organize regionally based on potential effects and needed capabilities

Actions

1. Assess current jurisdictional / geographic makeup of region
2. Consider alternatives
3. Identify a preferred alternative
4. Adjust and update plans, strengthen mutual aid, and begin regional training and exercises



How SLGCP Supports the Regional Priority

Grant Program Requirements & Management

- Priorities align with FY05 HSGP Guidance
- States and sub-grantees use FY05 HSGP funding to address priorities
- Regional collaboration is a key tenet of our grant programs
- Grant programs support planning and mutual aid development

State Assessments and Strategies

- Comprehensive State and Urban Area Homeland Security Assessments and Strategies submitted by all States in 2003
- Strategy addenda required by September 30, 2005 to align goals and objectives with the seven National Priorities outlined in the National Preparedness Goal

How the Expanded Regional Collaboration Priority Ties to the Goal and Target Capabilities

- Expanded Regional Collaboration is an overarching priority
- Essential to success of preparedness initiatives
- Critical for Capabilities-Based Planning Process

Interim National Infrastructure Protection Plan

D'Arcy Morgan

Information Analysis and Infrastructure Protection Division



**Homeland
Security**

Briefing Topics

- National Infrastructure Protection Plan Overview
- Sector Structure
- National Infrastructure Protection Plan Framework
- Interim National Infrastructure Protection Plan
- Sector Coordination
- Relationship to National Preparedness Goal
- Next Steps



NIPP Overview

- The President, under HSPD-7, directed the Department of Homeland Security to lead, integrate and coordinate a comprehensive *national plan* for critical infrastructure and key resources protection
- DHS is working to engage a broad-based of Federal, State, local, tribal and private sector partners on the coordination of the NIPP development
- Critical infrastructure protection is a national effort requiring aggressive outreach, shared planning and responsibility between private sector and government



Sector Structure

Critical Infrastructure Sectors	Agriculture & Food	USDA
	Public Health, Healthcare, Food	HHS
	Drinking Water, Water Treatment	EPA
	Defense Industrial Base	DoD
	Energy	DOE
	Banking and Finance	TREAS
	National Monuments & Icons	DOI
	Transportation Systems	DHS
	Information Technology	DHS
	Telecommunications	DHS
	Chemical	DHS
	Emergency Services	DHS
	Postal and Shipping	DHS
Key Resources	Commercial Facilities	DHS
	Government Facilities	DHS
	Dams	DHS
	Nuclear Facilities	DHS

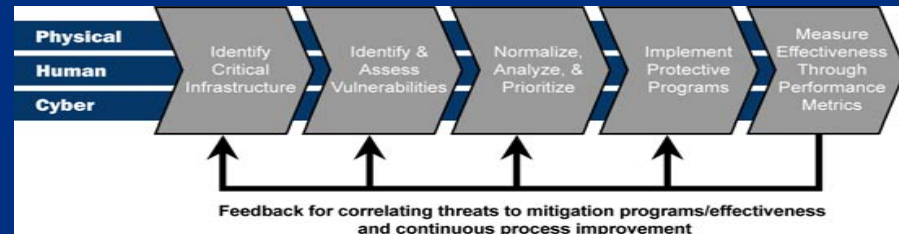
Federal Sector-Specific Agencies

DHS coordinates the overall national effort to enhance protection across sectors

NIPP Framework

The NIPP and supporting Sector-Specific Plans describe the *processes* undertaken in each sector to:

- Identify assets
- Assess risk
- Normalize and prioritize
- Develop protective programs
- Measure progress

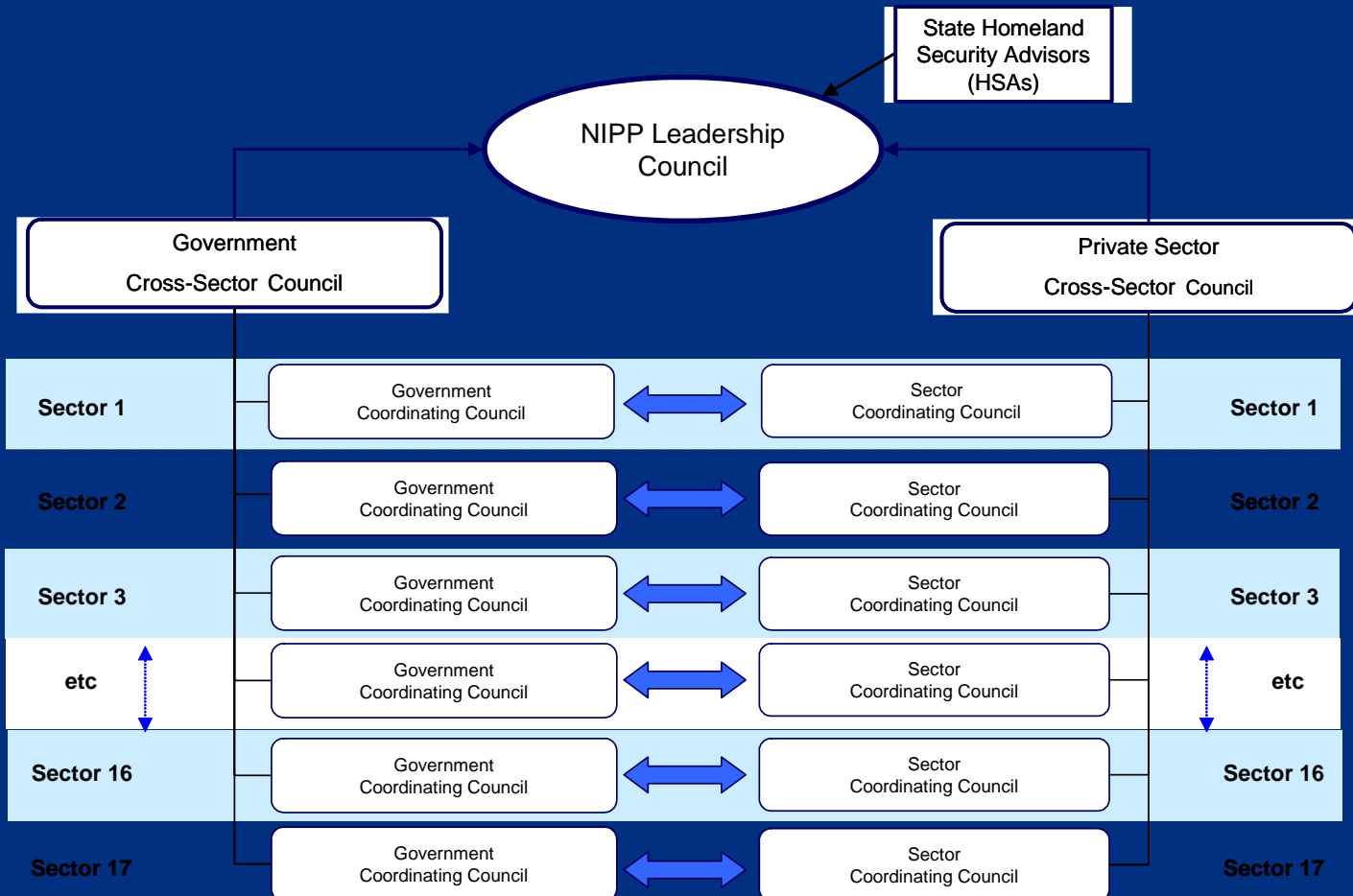


These activities are integrated across sectors and address the physical, human and cyber elements of critical infrastructure

DHS released the Interim NIPP on February 9, 2005 beginning a 270-day interim period to seek additional stakeholder involvement

DHS will continue to work with all stakeholders to further develop the NIPP and Sector-Specific Plans

Sector Coordination



Interim NIPP

The Interim NIPP provides the overall framework for a coordinated national critical infrastructure protection program:

1. National Goals, Framework and Actions – builds on the Homeland Security Act of 2002 and President's National Strategies
2. Vulnerability Reduction Program – describes the use of the risk management framework in the absence of specific threat information
3. Threat-initiated Actions – describes the use of the framework in response to specific threat information
4. Roles and Responsibilities – describes key stakeholder roles and responsibilities for NIPP implementation and identifies information coordination and exchange mechanisms
5. Integration with Other Plans – describes NIPP relationships to the National Response Plan and other Federal plans



Relationship to “The Goal”

- Critical Infrastructure Protection is a key component of the National Preparedness Goal:
 - NIPP implementation is one of the seven “National Priorities”
 - Critical Infrastructure Protection is one of the 36 Critical Capabilities
- Going forward, Critical Infrastructure Protection will be crucial in determining the levels of capability required for achieving the national preparedness goal



Next Steps

- Conduct stakeholder outreach and coordination:
 - To seek broader engagement with private owners and operators, State and local, and Federal agencies of infrastructure on the Interim NIPP
- Further develop and finalize the NIPP and Sector-Specific Plans
- Implement and measure progress and performance efforts

Strengthen Information Sharing and Collaboration Capabilities

Dave Brannegan

Technical Assistance Division, Office of State and Local
Government Coordination and Preparedness



**Homeland
Security**

Capability Overview

Strengthen information sharing and collaboration capabilities to enable effective prevention, protection, response, and recovery activities

- Based on the Information Sharing and Collaboration capability from the Task Capabilities List
- Two year time frame directed by the President and Congress
- Facilitate horizontal and vertical information sharing and collaboration activities

Capability Overview

Required Information

- Identity of the enemy
- Where they operate
- How they are supported
- Intended targets
- Intended attack method

This information will serve as a guide for efforts to:

- Rapidly identify both immediate and long-term as well as emerging threats
- Identify persons involved in terrorism-related activities
- Guide implementation of information-driven and risk-based prevention, response, and continuity planning efforts



Federal Initiatives

- Homeland Security Information Network (HSIN)
- Department of Justice (DOJ) Law Enforcement Information Sharing Program (LEISP)
- National Joint Terrorism Task Force (NJTTF)
- Multi-jurisdictional Prevention and Response Plan (MPRP) Development

Multi-jurisdictional Prevention and Response Plan (MPRP) Development

- FY05 Homeland Security Grant Program (HSGP) requirement for urban/metropolitan areas
- Develop or modify prevention and response plan based on the Homeland Security Council National Planning Scenario for Improvised Explosive Devices (IED)



MPRP Implementation

Guidance

- Stand-alone tool-kit enabling jurisdictions to develop or update individual prevention and response plans
- Identify requirements that materially assist in preventing and responding to incidents involving IEDs

Technical Assistance (TA)

- TA will be available to all interested jurisdictions to assist in guidance implementation

Assessment

- Each jurisdiction will receive a detailed blueprint for increasing prevention and response capabilities
- Assists urban areas in actively tracking progress toward the capability specific priorities, tasks, and capabilities



MPRP Timeline

- MPRP Guidance will be released on May 2, 2005
- Technical assistance will be available on May 2, 2005
- Jurisdictions will have six months from the release of the MPRP Guidance to develop their plan (May 2, 2005 – Nov 2, 2005)

Interoperable Communications

Juan Otero

Deputy Director, OIC and SAFECOM, Science and
Technology Directorate

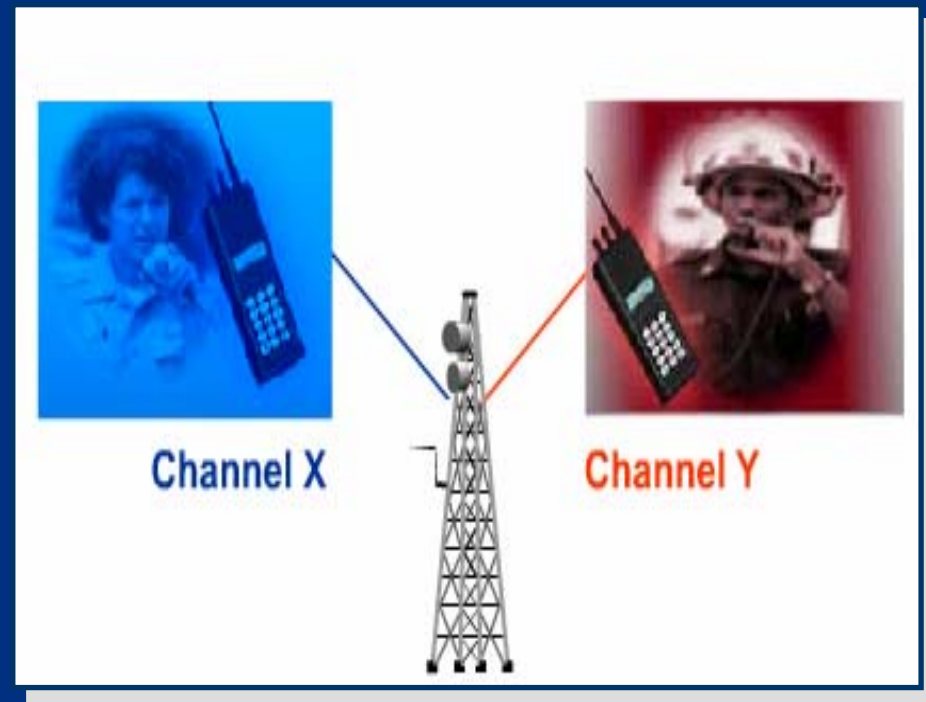


**Homeland
Security**

What is Interoperable Communications?

Wireless interoperability is the ability of public safety service and support providers to talk with each other via voice and data

- on demand
- in real time
- when needed
- when authorized



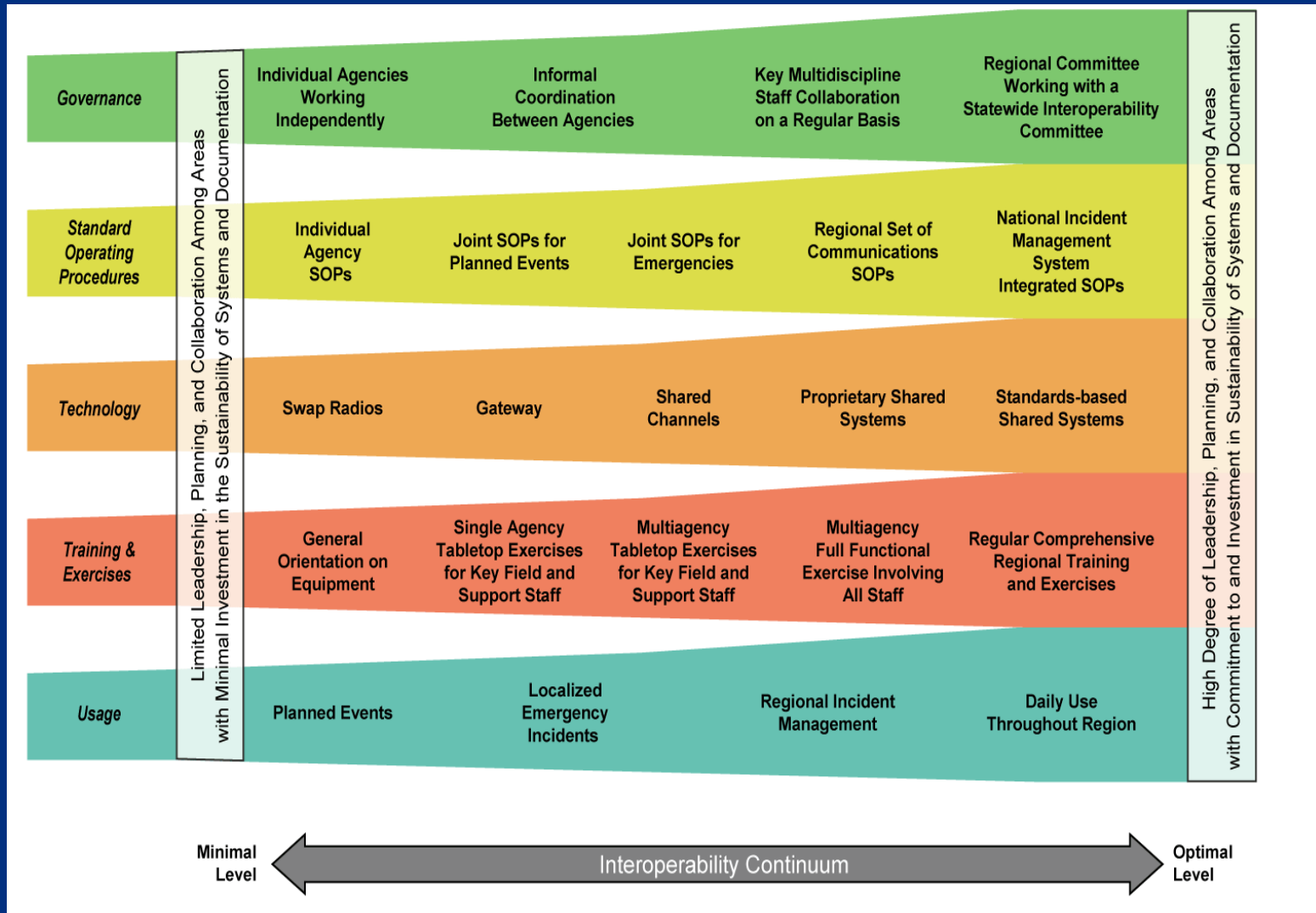
OIC: Supporting the Interoperability Priority

OIC, as a practitioner-driven office, is strengthening public safety's ability to work together to protect lives and property. OIC interim frameworks that support the priority include:

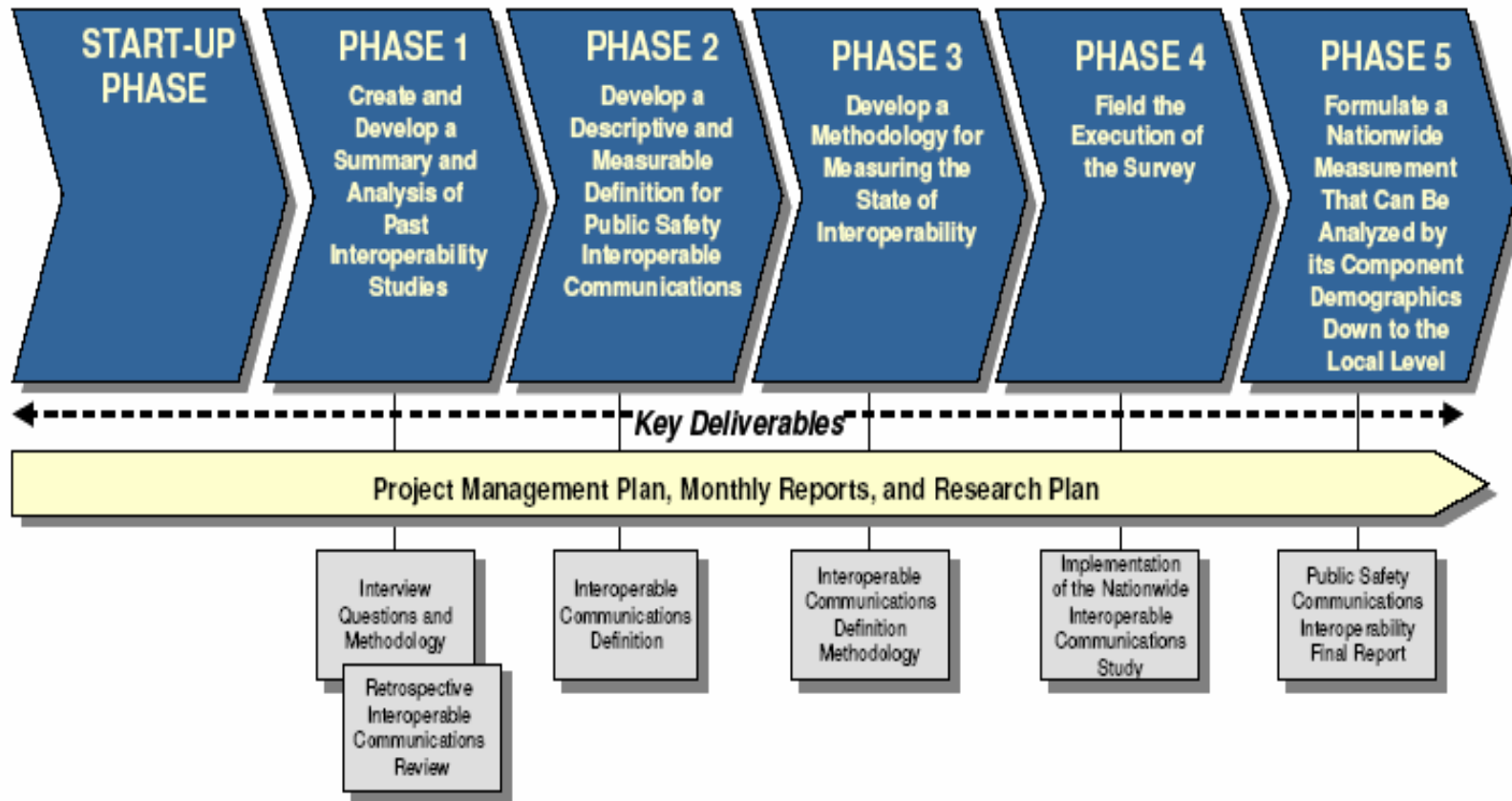
- Interoperability Continuum
- Interoperability Baseline Initiative
- Common Federal Grant Guidance
- Statement of Requirements (SoR)
- Acceleration of Standards Process
- Statewide Communications Interoperability Planning (SCIP) Methodology



Interoperability Continuum

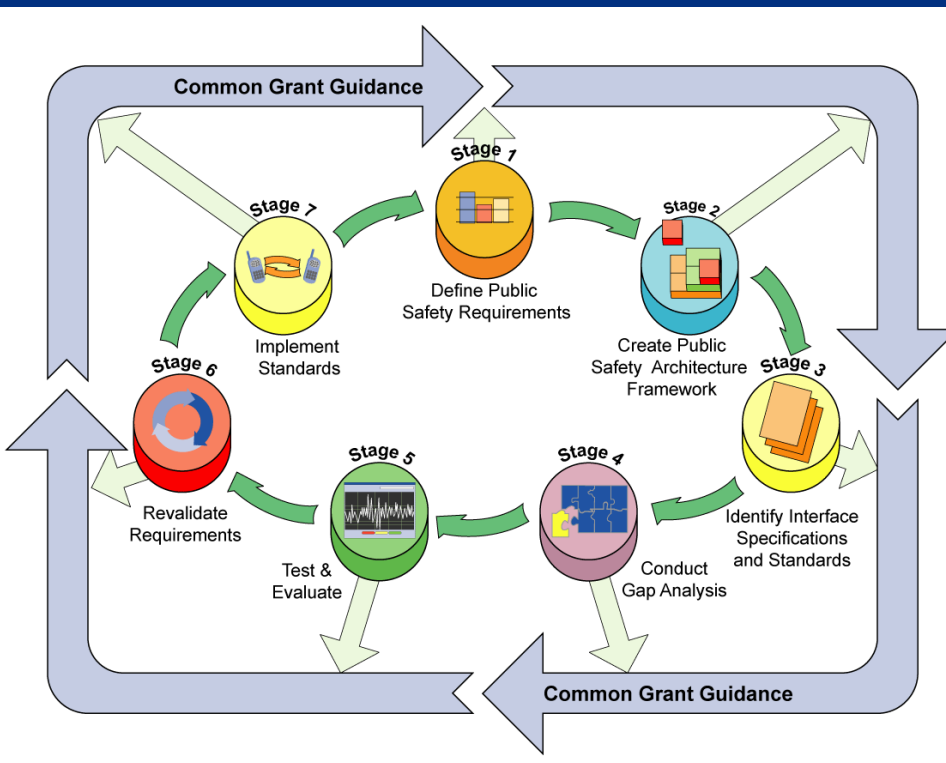


Interoperability Baseline Initiative



Tools for Improving Interoperability

Lifecycle for Standards Development



- **Statement of Requirements (SoR)**
 - Created to identify a basic set of functional and technological interoperable communications requirements for public safety first responders from all disciplines in all jurisdictions to communicate and share information.
- **Statewide Communications Interoperability Planning (SCIP) Methodology**
 - This tool outlines a step-by-step planning process for developing a locally-driven, statewide strategic plan to enhance communications interoperability



Guidance for Interoperability

- Common Federal Grant Guidance
 - SAFECOM has provided common grant guidance to Federal agencies to assist in planning and implementing the community's interoperability solutions
- Office for Domestic Preparedness Tactical Interoperable Communications Plan
 - SAFECOM partnered with ODP to create a guide to assist UASI grantees to create a tactical interoperable communications plan in accordance with the 2005 grant guidance



Strengthen Interoperable Communications Capabilities

Dave Brannegan

Technical Assistance Division, Office of State and
Local Government Coordination and Preparedness



**Homeland
Security**

Objectives

- Tactical Interoperable Communications Plan (TICP) Overview
- Timeframe
 - HSGP requirements for a TICP for UASI locations and States
- Metropolitan Areas
 - Helping these locations assess existing interoperable communications planning they have already undertaken or completed for incorporation into their TICPs
- Interoperable Communications Technical Assistance Program (ICTAP)
 - Advising and supporting the locations, as request, on the interoperable communications aspects required in an exercise scenario for an IED incident



Tactical Interoperable Communications Plan

Defined as the rapid provision of on-scene, incident-based mission critical voice communications among all emergency responder (EMS, fire, and law enforcement) agencies, as appropriate for the incident, and in support of Incident Command and Operations Section personnel as defined in the NIMS model

- Objective is to develop and test a plan to achieve adequate communication between incident commanders within an hour of an incident
- Released in concert with the National Preparedness Guidance on April 1, 2005
- Developed in coordination with the SAFECOM program

Timeframe

Each urban area receiving FY05 UASI funds must develop a plan to achieve tactical interoperable communications across jurisdictions in the urban area and test the plan through the exercise activity required for the IED scenario. Each urban area has:

- Six months to develop tactical interoperable communications plan
- One year following plan submission to test it through multi-jurisdictional exercises
- RapidCom 9/30 participants with previously developed plans need to submit and validate the plan through the exercise requirement



Metropolitan Areas

- If a state does not have a designated urban area, then it must identify a metropolitan area to develop and test the plan
- Metropolitan area should be the same area tasked with developing a Multi-jurisdictional Prevention and Response Plan
- Part of the HSPD-8 Implementation required by the FY05 HSGP guidance



Interoperable Communications Technical Assistance Program (ICTAP)

- Designed to enhance interoperable communications between local, state, and federal emergency responders and public safety officials
- Goal is enable local public safety agencies to communicate as they prevent or respond to a CBRNE terrorist attack
- Leverages other federal, state, and local interoperability efforts whenever possible to enhance state capacity for communication
- All grantees are encouraged to request support through ICTAP



ICTAP Assistance Designated for TICP

- Three one-day regional training workshops on TICP Guidance in conjunction with the Office of Community Oriented Policing Services (COPS) Interoperable Communications Technology Program Workshop Series:
 - Western Region: April 13 in Denver, Colorado
 - Central Region: June 3 in Columbus, Ohio
 - Eastern Region: July 14 in Charlotte, North Carolina
- ICTAP is available on a first-come, first serve basis to provide TA at no cost to States and Urban Areas
- ICTAP staff available to assist in both the development and implementation of the TICP (policy, technical and operational)
- Upon completion of TICP further assistance can be requested through ODP to support validation of the plan



Strengthen CBRNE Detection, Response, & Decontamination Capabilities

Lance Brooks

Chemical/Biological Countermeasures, Science and
Technology Directorate

Mike Carter

Chief Scientist, Domestic Nuclear Detection Office

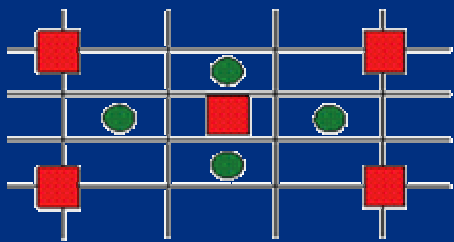


**Homeland
Security**

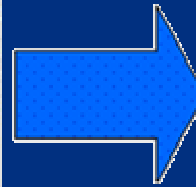
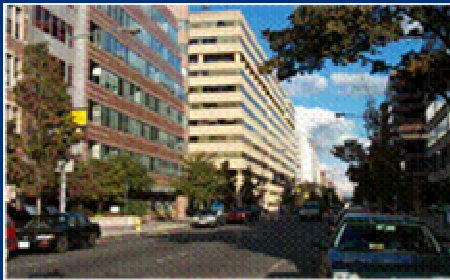
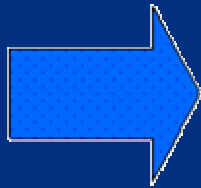
CBRNE Detection

- Detection must deploy systems that are cost-effective, robust, highly sensitive, specific, and integrated into a concept of operations
- ...must include systems for both rapid detection and rapid authentication and verification of the identity and quantity of CBRNE materials.
- ...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

Biological Monitoring Systems



Wide Area



- **Wide area monitoring (detect-to-treat)**

- Phase 1 BioWatch, Phase 2 BioWatch increased sampling, to networked sensors

- **Facility monitoring (detect-to-warn)**

- Simple triggers/low regret responses, to improved detect-to-warn sensors, to improved design of new facilities

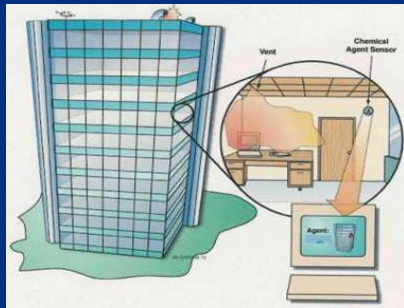
- **Coordination with other national programs**

- With DoD force protection, with USPS Biohazard Detection System, with EPA and DoD building protection programs



**Homeland
Security**

Chemical Detection Systems



- **Facility/Area monitoring**

- PROTECT for Transit/Facilities, Autonomous Rapid Facility Chem Agent Monitor, Deployable Detection System (Special Events)

- **Portable Detection Devices**

- Light-weight Autonomous Chemical ID system, Low volatility Agent Surface Contamination Monitor

- **Development of other systems**

- Chemical Laboratory Response Network, Mobile Lab (PHILIS)



**Homeland
Security**

Homeland Security Advanced Research Projects Agency (HSARPA)

Past solicitations (BAAs):

- Detection systems for bio & chem countermeasures
- Bio-informatics & assay development

Current solicitations (BAAs):

- Instantaneous bioaerosol detector systems (IBADS)
- Food Biological Agent Detection Sensor (FBADS)

Past Small Business Innovative Research solicitations:

- Chem-bio sensors employing novel receptor scaffolds
- Advanced low cost aerosol collectors for surv & ...

For more information see www.hsarpabaa.com



**Homeland
Security**

Nuclear and Radiological Terrorism is one of the greatest threats to the Nation

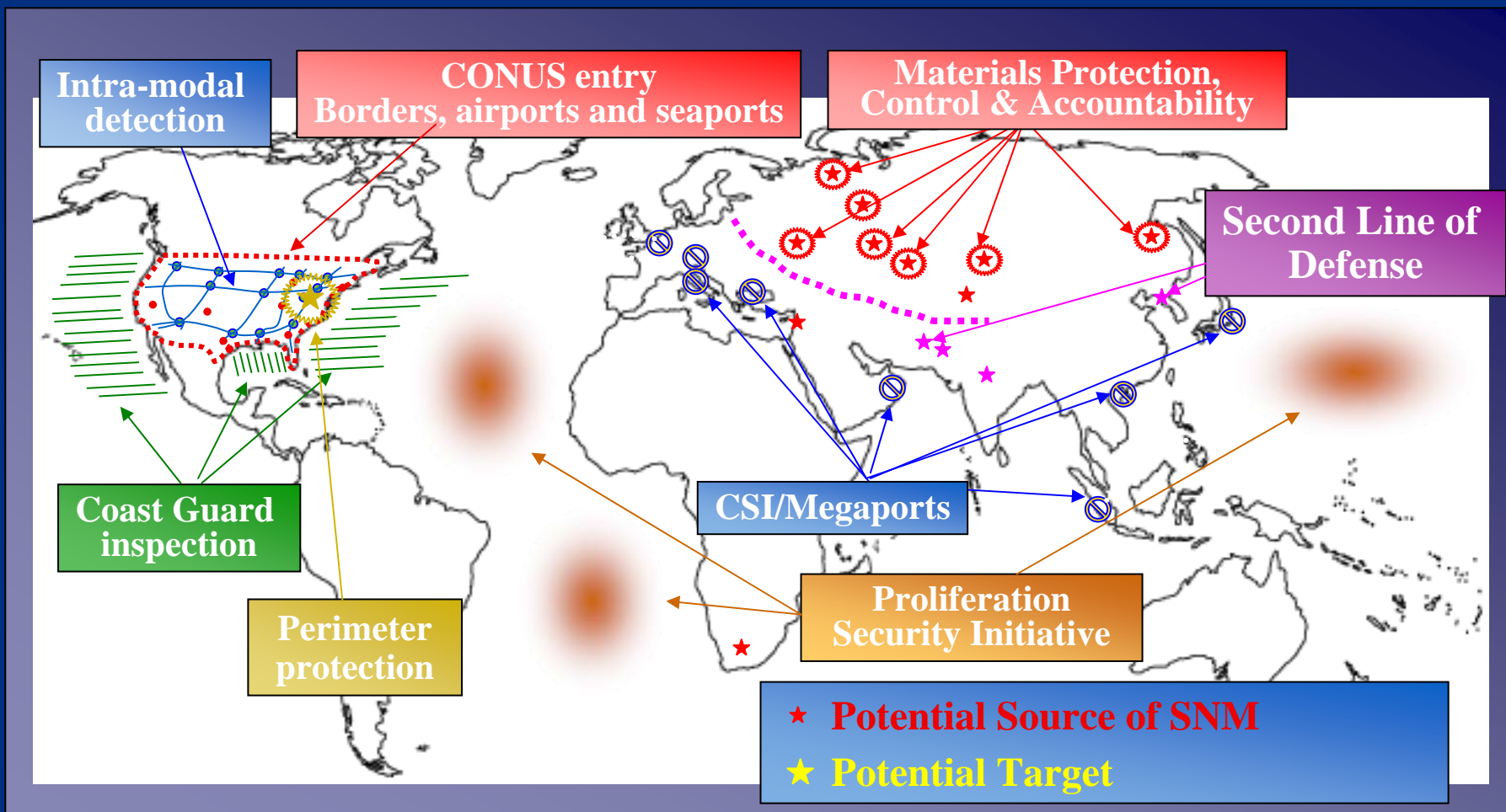
- Emphasis must be placed on prevention
- To defend against this threat, we must develop a robust layered defense
- Each layer must reduce the terrorist ability to use such threats against us
- Layered defense includes:
 - Eliminating excess stocks of nuclear materials and weapons
 - Protecting existing stocks from theft or diversion
 - Detecting illicit movement of nuclear or radiological material overseas
 - Enhancing domestic detection and interdiction efforts

The Domestic Nuclear Detection Office (DNDO) has been established to reduce the risk

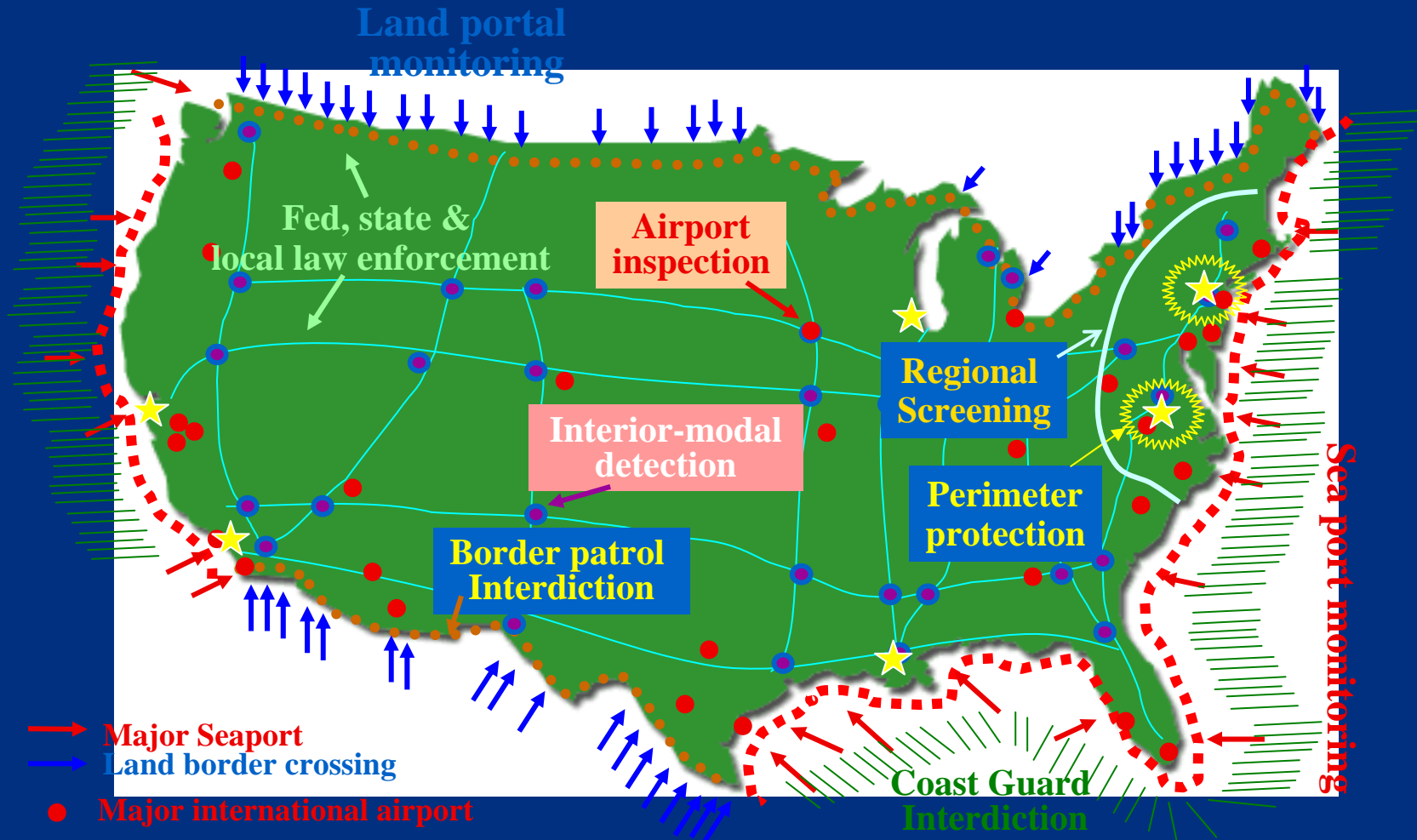
The DNDO will be a *jointly-staffed, national* office established to develop the global nuclear detection architecture, and acquire, and support the deployment of the domestic detection system to detect and report attempts to import or transport a nuclear device or fissile or radiological material intended for illicit use.



Global, multi-layered defense requires integration of overseas and domestic components



Nuclear and radiological countermeasures demands a layered defense at home



Homeland
Security

DNDO Strategic Objectives

- Create a well-integrated detection and reporting system for interdicting nuclear and radiological materials (domestic and international)
- Enhance current detection capabilities to improve probability of detection and interdiction
 - Integrate and deploy current technologies
 - Continuously improve technology through near-term enhancements and transformational research and development
 - Expand detection capabilities at the State and local level
- Develop the global detection architecture and ensure linkages across Federal, State and local agencies
- Establish standards, response protocols and training across the Federal, State, and local levels to ensure that detection leads to timely response actions



DHHS' Support of the Interim National Preparedness Goal

Brad Austin, MPH, CHE

Senior Public Health Analyst

Office of Public Health Emergency Preparedness

Los Angeles, CA

April 27, 2005



Office of Public Health Emergency Preparedness (OPHEP)

Overall Goal of the DHHS Public Health Emergency Preparedness Program

- To ensure sustained public health and medical readiness for our communities and our nation against:
 - Bioterrorism
 - Infectious disease outbreaks
 - Other public health threats and emergencies



CDC's Cooperative Agreement on Public Health Preparedness and Response for Bioterrorism

CDC Cooperative Agreement

- Preparedness Planning/Readiness Assessment
- Surveillance and Epidemiological Capacity
- Biological Laboratory Capacity
- Chemical Laboratory Capacity
- Communications and Information Technology
- Risk Communication
- Education and Training



HRSA's National Bioterrorism Hospital Preparedness Program

HRSA Cooperative Agreement

- Regional Hospital Surge Capacity
 - Beds, Personnel, Equipment
 - Isolation capacity
 - Mental health services
 - Trauma/burn care
- Emergency Medical Services
- Linkages to Public Health
 - Hospital Laboratories
 - Surveillance & Patient Tracking
- Education and Preparedness Training
- Exercises



Public Health and Hospital Preparedness and Response for Bioterrorism Cooperative Agreements

CDC/HRSA Historical Breakdown of Funds

- ▶ Combined Allocations since September 11, 2001
 - FY02 ~ \$1.07 billion
 - FY03 ~ \$1.53 billion
 - FY04 ~ \$1.34 billion
 - FY05 ~ \$1.42 billion
 - FY02-05 Grand-total ~ \$5.36 billion



Capability Specific National Priority in the Interim National Preparedness Goal

Target Capabilities

- Eight target capabilities identify health and medical capabilities
 - ▶ Fatality Management
 - ▶ Isolation and Quarantine
 - ▶ **Mass Prophylaxis**
 - ▶ Medical Supplies Management and Distribution
 - ▶ **Medical Surge**
 - ▶ Public Health Epidemiological Investigation and Laboratory Testing
 - ▶ Triage and Pre-hospital Treatment
 - ▶ Worker Health and Safety
- Sixteen additional target capabilities have public health embedded



Capability Specific National Priority: Strengthen Medical Surge and Mass Prophylaxis Capabilities

Medical Surge and Mass Prophylaxis Target Capabilities

- Medical Surge

Hospitals must be able to collectively handle a mass casualty

- Mass Prophylaxis

Emergency-ready public health departments need to be ready to organize and direct mass campaigns



Resources

- CDC Cooperative Agreement Guidance
<http://www.bt.cdc.gov/planning/continuationguidance/index.asp>
- HRSA Cooperative Agreement Guidance
<http://www.hrsa.gov/bioterrorism/cooperative/index.htm>
- Interim Public Health and Healthcare Supplement to the National Performance Goal
<http://www.hhs.gov/ophep/index.html>



Interim

National Preparedness Goal

Rollout Conference



**Homeland
Security**