DCN 4375

Defense Science Board 2003 Summer Study

on

DoD Roles and Missions in Homeland Security

VOLUME II – A: SUPPORTING REPORTS

May 2004

Office of the Under Secretary of Defense
For Acquisition, Technology, and Logistics
Washington, D.C. 20301-3140

This report is a product of the Defense Science Board (DSB).

The DSB is a Federal Advisory Committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions and recommendations in this report do not necessarily represent the official position of the Department of Defense.

This report is unclassified.

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301-3140

DEFENSE SCIENCE
BOARD

MEMORANDUM FOR THE ACTING UNDER SECRETARY OF DEFENSE
(ACQUISITION, TECHNOLOGY & LOGISTICS)

SUBJECT: Report of the Defense Science Board 2003 Summer Study on DoD Roles and Missions in Homeland Security

I am pleased to forward the final report of the DSB 2003 Summer Study on DoD Roles and Missions in Homeland Security. The report consists of two volumes. Volume I evaluates DoD's role in homeland security and makes recommendations on how best to accomplish this mission. Volume II is a compilation of four sub-panel reports.

The conceptual thinking and the capabilities required to address the homeland security challenge are still immature. The study concludes that maturing the conceptual framework and capabilities related to homeland protection will require a holistic approach. Thus, fostering a holistic approach to protecting the homeland is a guiding theme for this study. The report's recommendations, which fall into the following six areas, reflect this theme.

- Global situation awareness
- Protect DoD mission-critical infrastructure
- Deter and prevent attack
- Emergency preparedness and incident response
- Exporting DoD core competencies
- Empowering U.S. Northern Command

I endorse all of the recommendations of the Task Force and encourage you to review their report.

William Schneider, Jr.
Chairman

This page intentionally left blank

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301-3140

DEFENSE SCIENCE
BOARD

MEMORANDUM FOR THE CHARIMAN, DEFENSE SCIENCE BOARD

SUBJECT: Report of the Defense Science Board 2003 Summer Study on DoD Roles and Missions in Homeland Security

Developing an effective capability to protect the homeland is a top national priority. It is also a complex undertaking filled with many challenges. There are so many assets to protect, so many modes of attack available to adversaries, and so many organizations involved, that, understandably, both the conceptual thinking and the capabilities required are still immature. Maturing the conceptual framework and capabilities related to homeland security, the DSB believes, requires a holistic approach—a guiding theme for this study.

The final report of this study consists of two volumes. Volume I identifies capabilities and initiatives needed by DoD to fulfill its responsibilities to project force when directed and to protect the homeland. It focuses on those capabilities that depend upon DoD working closely with other agencies. In addition, opportunities are identified for DoD to "export" some of its core competencies to help accelerate the maturation of the many agencies involved in homeland security tasks. Volume II is a compilation of four sub-panel reports.

The principal findings and recommendations fall in six key areas:

- Information is vital to homeland security. *Yet improvements are needed in many areas of information sharing, assurance, and collection*. First, incentives are needed to enhance information sharing. Second, tools and capabilities for information assurance need to be developed and implemented. Third, collection capabilities, importantly in the area of human intelligence, must be enhanced. In general, foreign intelligence collection must be more proactive and better integrated with domestically derived intelligence.

- DoD's ability to fulfill its missions—most notably force projection—is dependent on an intricate infrastructure in the

United States. *DoD is not doing enough to address the vulnerabilities of mission critical infrastructure and services, particularly in areas outside its direct control.* A systematic approach—that focuses both "inside and outside the fence"—must be taken to identify and redress vulnerabilities. Moreover, cyber security and cyber-based aspects of critical infrastructure need to be better integrated into DoD mission-critical infrastructure protection efforts.

- *Ocean vessels, cruise missiles, and low-flying aircraft are credible delivery systems available to adversaries. DoD needs to take steps to counter these threats as a complement to ongoing initiatives to defend against ballistic missiles.* First, much more can and should be done to improve maritime security and to integrate maritime-security capabilities across the federal government. Second, because these delivery systems could threaten the continental United States with biological and other weapons of mass destruction, DoD should create a master plan for defense against the low-altitude air threat.

- *Should the U.S. homeland be attacked, DoD could be called on to assist with incident response. Execution of this mission could require capabilities in areas where the Department is deficient*: 1) mitigation and remediation of the effects of attacks from weapons of mass destruction, 2) the ability to surge medical capabilities, 3) communication operability between first responders and federal, state, and local agencies. The report offers detailed recommendations for improving capabilities in each of these areas as well as enhancing Reserve Component capabilities that can support the homeland security mission.

- *DoD can enhance homeland security by "exporting" relevant core competencies that match the needs of other organizations that have homeland security responsibilities.* The study identifies three core competencies in particular: training, experimentation, and operational-level planning and execution. Responsibility to develop, and oversee execution of, plans to export core competencies to other agencies should be assigned to U.S. Northern Command.

- *U.S. Northern Command must be empowered for the nation to achieve its homeland security and homeland defense goals.* The study recommends more than a dozen new tasks for NORTHCOM, with four identified as priorities: develop a roadmap for maritime surveillance; develop a roadmap for defense against the low-altitude air threat; assume operational lead for DoD mission-critical infrastructure protection in CONUS; and assume the lead for exercises, training, experiments, and standards related to homeland defense and military assistance to civil authorities.

The specific recommendations provided in the pages that follow reflect the holistic approach to protecting the homeland that the DSB envisions for the Department of Defense. By taking this approach, and developing the capabilities described in the six areas above, the security of our nation will be improved.

Donald Latham, Co-Chair

ADM Donald Pilling, USN (Ret), Co-Chair

This page intentionally left blank

TABLE OF CONTENTS*

PART 1: EMERGENCY RESPONSE PANEL REPORT

PART 2: TECHNOLOGY AND SYSTEMS PANEL REPORT

PART 3: NATIONAL GUARD ROLES AND MISSIONS

* VOLUME I OF THIS REPORT REPRESENTS THE CONSENSUS VIEW OF THIS TASK FORCE. VOLUME II – A OF THIS REPORT CONTAINS MATERIAL THAT WAS PROVIDED AS INPUTS TO THE TASK FORCE, BUT WHOSE FINDINGS AND RECOMMENDATIONS MAY NOT REPRESENT THE CONSENSUS VIEW OF THIS TASK FORCE

This page intentionally left blank

PART 1: EMERGENCY RESPONSE PANEL REPORT

THIS PAGE INTENTIONALLY LEFT BLANK

In the wake of the events of September 11, 2001, the role of the Department of Defense in domestic emergency preparedness and response is under scrutiny. Ever since President Carter established the Federal Emergency Management Agency (FEMA) in 1978, the Defense Department has considered its domestic emergency response role to be one of providing support or assistance to civil authority. Military planners assume that civil agencies will always lead domestic emergency preparedness and response efforts, with the Department of Defense providing resources only in response to appeals from state and local governments to the President. Local and state governments are expected to use their resources first. While National Guard capabilities may be called into play by the Governor under Title 32 status, military commanders and planners have usually assumed that other Department of Defense assets will be called into play only when local, state, and other federal resources are overwhelmed. Concerns about the Posse Comitatus Act and misunderstandings of its scope have also tended to restrict the deployment of Department of Defense assets where their use might be construed as augmenting state and local law enforcement agencies.

This would appear to describe the current status quo. Considering the potential devastation that could result from a terrorist attack using a weapon of mass destruction (WMD), however, one needs to ask whether the national security environment has changed enough to warrant the Department of Defense taking a more active role in the missions of emergency preparedness and emergency *response.* If the answer to this question were yes, the implications for planning, training, and equipping alone would be significant. An affirmative answer would also have implications for the composition and posture of the new Northern Command (NORTHCOM) with respect to the National Guard, the Department of Homeland Security and other federal agencies, and state and local governments.

This question is not a new one. President Truman wrestled with it at the start of the Cold War. His solution was the creation of the Federal Civil Defense Administration in 1950. This organization was a coordinating body, without policy authority or resources; and it was ineffective in its mission of raising civil defense preparedness across the country. President Eisenhower tried to strengthen the organization by merging it with the Office of Defense Mobilization, but this too had little effect. President Kennedy tried again in 1961, this time moving the civil

defense mission to the Department of Defense, where it remained until the creation of FEMA.

There is a large and complex set of issues associated with any intrusion of the Department of Defense into domestic affairs. On the one hand, most citizens recognize that there is a role for the military in homeland defense. Protection of our airspace and coastline are logical missions for military ships and aircraft. It is less clear what role, if any, the Department should play in preparing for and responding to major terrorist attacks.

The Department of Defense is prepared to respond to calls for assistance with all of the resources at its disposal. This support model can be described as: "you call us when you need us and we'll do all we can." However, there are two very considerable problems with this model. First, a WMD attack may well call for the immediate deployment of equipment or capabilities that no local or state government can afford to maintain. Second, there is a built-in response delay as federal officials respond to local and state government requests for resources: units must be identified, equipment issued, and transportation arranged. The outcome is that the supported officials and the supporting commander meet for the first time at the scene of an emergency. This delay and possible confusion could result in additional damage, additional casualties or the further spread of a chemical or biological agent.

The Emergency Preparedness and Response Panel believes that the national security environment has changed sufficiently to warrant the Department of Defense taking a more active role in domestic emergency preparedness and response. The policies that prescribe the role of the Department of Defense in domestic emergency preparedness and response are simply inadequate for the threat the nation faces today. Developing a model appropriate for today's threats will entail rethinking relationships, policies, and procedures. The Secretary of Defense called the war on terrorism a "transformational event". The Panel agrees, and part of DoD's transformation must be to embrace this emerging mission. A larger role for the Department in domestic preparedness and response seems to fall comfortably within the mandate of the Federal Government as described in the Constitution of the United States. In Article IV, section 4, the Constitution states that

"The United States shall guarantee to every state in this union a Republican Form of Government, and shall protect each of them…against domestic violence."

The Federal Government has already taken major steps in recognition of this new security environment. Within DoD, a new combatant command, Northern Command, was created to:

"…conduct operations to deter, prevent, and defeat threats and aggression aimed at the United States, its territories and interests within assigned areas of responsibility; as directed by the President or Secretary of Defense, provides military assistance to civil authorities, including consequence management operations."

This definition of NORTHCOM's role conspicuously emphasizes DoD's heightened responsibilities in the areas of military assistance to civil authorities (MACA) and consequence management. Additionally, a new office within the Department of Defense was established. The principal duty of the new Assistant Secretary of Defense for Homeland Security (ASD HD) is:

"… The overall supervision of the homeland defense activities of the Department under the authority, direction and control of the Under Secretary of Defense for Policy and, as appropriate, in coordination with the Chairman of the Joint Chiefs of Staff."

Elsewhere in the federal government, both a new White House office and a new cabinet department were created. The role of the Office of Homeland Security is to:

"…develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks."

The new Department of Homeland Security (DHS) is charged to:

"…protect the nation against further terrorist attacks. Component agencies will analyze threats and intelligence, guard our borders and airports, protect our critical infrastructure, and coordinate the response of our nation in future emergencies."

Further, the Department of Homeland Security has a Directorate of Emergency Preparedness and Response whose charter directs it to coordinate all federal response to domestic disasters.

These new structures are just now organizing themselves, and many of their offices are still unfilled and their future roles unclear. Nevertheless, it seems that the role of the Department of Defense in emergency preparedness and response must evolve to keep pace with the evolution of the threat against the country. The Panel also believes that DoD should not wait for all of these organizations and offices to mature before taking a more active role in emergency preparedness and response. While the semantic distinction between homeland defense and homeland security serves some useful purposes in apportioning roles and responsibilities between DoD and DHS, such distinctions can never be absolute. The Department of Defense and the Department of Homeland Security have a common primary mission, which is the protection of the American homeland and people. If the threat of WMD is sufficient to warrant the creation of a Department of Homeland Security, it is sufficient to change the way the Department of Defense will respond to the possibility of their use.

The heaviest burden of preparing for domestic emergencies falls on the emergency medical personnel, firefighters, and police officers of the "first responder" community. Concerns about mass casualties from conventional attacks and the potential use of smallpox and other biological weapons have focused renewed attention on public health and hospital preparedness, which are thought to be woefully lacking. Behind the first responders and healthcare personnel are state emergency management offices, the offices of the state adjutant generals, and finally the many federal agencies with roles to play.

The Panel believes that any role for the Department of Defense in emergency preparedness should start with support for the first responders. The thousands of emergency response organizations throughout the country are each unique. They have separate budgets, different levels of training and expertise, varying levels of interaction with state and federal officials and different threat environments in which they must work. It would be impossible to recommend any set of actions that DoD (or DHS, for that matter) could take to address all of the problems of these disparate organizations. However, there are some common issues and requirements that DoD can help to resolve.

Before discussing recommendations for specific actions, an observation by the Panel about the policy that is emerging from both the Department of Defense and the Department of Homeland Security concerning the cooperation of these two critical organizations should be noted. Many

emergency preparedness and response issues can be resolved if policy enables and encourages communication and collaboration among the responsible officials. Neither DoD nor DHS seems to encourage this interaction. **The Panel recommends that the Secretary of Defense and the Secretary of Homeland Security issue a joint policy statement demanding cooperation between the two departments consistent with current law and regulation, and that the Secretaries proactively lead in that cooperation.**

State National Guard organizations are well positioned to represent DoD to local emergency planners and responders. They are known in their communities and in 25 states; the State Adjutant General is the State Emergency Management Director. The National Guard has both a federal and a state mission. Its federal mission is to provide forces to the Army and Air Force. Its state mission is to: "provide trained and disciplined forces for domestic emergencies or as otherwise required by state laws."

Numerous recent studies on the subject of domestic response to possible terrorist incidents, including the Council on Foreign Relations-sponsored Hart/Rudman report, the Heritage Foundation Working Group on Military Operations, the 2002 Gilmore Commission and several reports of the Defense Science Board all recommended an expanded role for the National Guard in emergency preparedness and response. The Panel fully agrees. To a limited extent, this expanded role could result in the migration of guard units to new structure and missions, but it can be accomplished without substantial change to the current federal mission of the National Guard.

The first step in any expanded role for the Department of Defense is a better understanding of the different vulnerabilities in each state. **The Panel recommends that the Department of Homeland Security, with the cooperation of the state National Guards, Northern Command, and relevant state and federal agencies, undertake state-by-state vulnerability assessments. These assessments should include an evaluation of DoD-critical (non-DoD owned) infrastructure.** The assessments will be provided to the state governors, and can form the basis for allocation of state and local resources. The assessments should also form the basis for a "gap analysis" with recommendations for federal assistance. The Department of Homeland security should take the lead in the establishment of national vulnerability standards, using as a basis the work already done by such agencies as the Army Corps of Engineers and the Defense Threat Reduction Agency.

The Panel recommends that Northern Command analyze the results of these assessments and make recommendations for the allocation of Departmental resources to the Secretary of Defense. Possible recommendations might include:

- Assignment of National Guard units to new collateral or primary duties on a local or regional basis.
- Restructure National Guard units to assume a new mission.
- Assignment of an active duty or reserve organization to a new collateral duty.
- Allocation of DoD equipment to a civil support function.
- Creation of redundant facilities or alternative means of mission assurance

The establishment of national standards and vulnerability baselines will be difficult, and the Panel urges the creation of interagency taskforces to do the job. Success depends on the cooperation and participation of the many federal, state, and local agencies with vital interests in this important work.

To be effective, participation of the National Guard and Northern Command in state emergency preparedness and response requires real-time information sharing and situational awareness. To that end, **the Panel recommends that an experienced Northern Command Liaison Officer be detailed to each state Adjutant General.**

Once National Guard or Title 10 reserve units are allocated against state missions, they need to plan and train with the first responders they will support in the execution of their plans. **The Panel recommends that the National Guard and other DoD units assigned an emergency preparedness mission be resourced to train with local emergency organizations, and that training standards be developed by Northern Command in cooperation with the Department of Homeland Security and the National Guard Bureau**. Policy must be adjusted to facilitate ongoing joint homeland security training opportunities between federal, state, and local responders beyond Congressionally mandated national training exercises like TopOff and TopOff 2.

The joint training described above can only be effective if adequate interoperability exists so that National Guard, Reserve and first response units can communicate with each other. Currently, there are multiple

procurement authorities within each state and no standards for communications interoperability or protection of communication functions. The Department of Defense has experience in the design and implementation of large-scale communication networks. **Therefore, the Panel recommends that the Secretary of Defense direct the Assistant Secretary of Defense for Networks and Information Integration to proactively support the Department of Homeland Security in developing the architecture and setting standards for domestic emergency wireless communications.** The architecture must be fully mobile, self-forming, and self-healing, and the technology utilized should support streaming video and still pictures and be independent of but interoperable with commercial networks. It should be resistant to attack or interference, provide geopositioning capability, and be fully scaleable. Based on this foundation, **the Panel recommends that the Department of Homeland Security and the Department of Defense provide funds to procure adequate interoperable communications equipment for all civilian, National Guard, and Title 10 units with emergency response missions.**

In the event of a domestic emergency, immediate federal response is under the control of the local FBI field office. There is a rather elaborate interagency process that governs federal participation in domestic emergencies, starting with the establishment of an FBI-led Joint Operations Center (JOC). Depending on the size of the emergency, the federal response can quickly grow larger and include the Domestic Emergency Support Team (DEST). The DEST deploys to an emergency site on DoD aircraft, and includes DoD liaison officers. This team can, in turn request additional federal aid from a wide variety of agencies.

The mechanism briefly described above will change with the publication of the National Response Plan in 2005. It is not yet clear whether the new plan will provide a more "user friendly" process. Though the current process eventually brings appropriate resources to bear, it is too slow to be effective in a terrorist incident involving potential weapons of mass destruction or large numbers of casualties. The Panel has chosen not to make recommendations for change to the current process, since changes are already in progress. **The Panel does recommend that the Department of Homeland Security and the Department of Defense jointly review the current statutes relating to DoD assistance to civil authorities, and propose changes where necessary to make the provision of such assistance easier and timelier.**

One of President Bush's recent initiatives is the creation of the USA Freedom Corps. This umbrella organization's mission is to encourage

community involvement across the country. Within the Freedom Corps, the Federal Emergency Management Agency established the Citizen Corps. The Citizen Corps encourages all Americans to participate in some aspect of homeland security through their local first responder organizations.

Every year over 100,000 young men and women leave the armed forces after an initial enlistment. All of them have a four-year inactive obligation in the armed forces reserve. Many of these men and women have skills that would be critical in any large-scale domestic emergency: medical technicians, damage control specialists, and communications technicians to name a few. These are citizens of proven patriotism, who might be willing to trade their reserve obligation for service in a homeland security reserve organization.

The Panel recommends that the Department of Defense, in cooperation with the Department of Homeland security, create a Homeland Security Reserve, using the talents of recently discharged armed forces members. Such an organization could serve as a bridge between first responders and the National Guard. The United States has a history of citizen participation in civil defense, and former members of the armed forces seem to be a solid foundation on which to build.

APPENDIX A

MEMBERSHIP LIST
EMERGENCY PREPAREDNESS AND RESPONSE PANEL

Panel Co-Chairs	
Dr. Richard Hatchett	Department of Health and Human Services
Gen Michael Williams, USMC (Ret.)	Logistics Management Institute
Members	
Dr. Stan Alterman	Alterman Associates, Inc.
MG John Fenimore, USAF (Ret.)	The Fenimore Group LLC
Dr. Joshua Lederberg	The Rockefeller University
Mr. Larry Lynn	Private Consultant
Dr. Thom Mayer	INOVA Fairfax Hospital
Det. Todd Metro	New York City Police Department
Chief Edward Plaugher	Arlington County Fire Department
Dr. Anna Marie Skalka	Fox Chase Cancer Center
Government Advisors	
COL Richard Marchant, USA	Force Transformation Office

This page intentionally left blank

APPENDIX B. GLOSSARY OF ACRONYMS AND ABBREVIATIONS

ASD HD	Assistant Secretary of Defense for Homeland Defense
DEST	Domestic Emergency Support Team
DHS	Department of Homeland Security
DoDs	Department of Defense
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
JOC	Joint Operations Center
MACA	Military Assistance to Civil Authorities
NORTHCOM	Northern Command
TopOff2	Top Officials 2 WMD Terrorism Response Exercise
USA	United States of America
WMD	Weapon of Mass Destruction

This page intentionally left blank

PART 2: TECHNOLOGY AND SYSTEMS PANEL REPORT

This page intentionally left blank

EXECUTIVE SUMMARY

Traditionally, the primary focus of the Defense Department has been on winning the nation's wars and winning them decisively. The approach that has been adopted is to take the fight to the enemy. Consequently, the vast majority of the formal requirements for technology and systems (T&S) to support the Department's mission have been directed at operations outside of the continental U.S. (OCONUS) against nation states in force-on-force situations.

In the aftermath of the September 11 attacks, the Department is beginning to expand its focus to support the global war on terrorism. Initially, the Department has continued its approach of taking the fight to the enemy by aggressively pursuing the terrorist leaders, their organizations, training camps and nations that harbor them as illustrated by operations in Afghanistan and Iraq. However, with the establishment of Northern Command (NORTHCOM), the Department of Defense (DoD) has for the first time created a combatant command that has the continental United States as its area of responsibility (AOR) and homeland defense as its mission.

While much of the capability required by NORTHCOM already exists in DoD as a consequence of the investment for the OCONUS missions, ultimately NORTHCOM will establish its unique T&S requirements. Since the Command is in such an early stage, though, it has not yet completed its first pass at these requirements. For the current study on DoD's role in Homeland Security, the T&S Panel[1] informed its analyses by hearing from a broad range of DoD organizations and individuals listed in Appendix III. We focused our investigations on four areas that we felt were likely to be the source of unique T&S requirements for NORTHCOM, namely:

- Chemical/Biological/Radiological/Nuclear/High Explosive (CBRNE) preparedness for Continental

[1] See Appendix II for complete panel membership.

Unites States (CONUS) bases (including risk assessments)

- Maritime surveillance and security
- Low Altitude Air Threats
- Military Assistance to Civilian Authorities (MACA) Communications/Command and Control (C2) interoperability with Department of Homeland Security (DHS) and state/local leaders and first responders

In addition to these areas, the Panel investigated two other S&T areas – base/defense infrastructure vulnerability assessment and information security – that have a broader impact than just NORTHCOM, but are likely to have a significant impact on DoD's ability to complete its missions successfully, particularly to mobilize its resources to project force anywhere it is needed. The Panel also developed a set of lessons learned from DoD experiences with management of technology, especially with DARPA, that may be useful to DHS as it establishes a similar capability with the Homeland Security Advanced Research Projects Agency (HSARPA).

The primary recommendations for DoD actions that resulted from the Panel deliberations are:

DEFENSE AGAINST CHEMICAL/BIOLOGICAL/RADIOLOGICAL/NUCLEAR/HIGH EXPLOSIVES (CBRNE) ATTACK

- DARPA should initiate a program to reach out to the pharmaceutical and biotechnology industries for broad-based enzymatic decontamination technology.
- The Guardian Program should be extended to include radiological and nuclear threats.
- DoD and DHS should establish a joint program to pursue diagnostic technology to enable pre-symptomatic detection of infection by biological weapon attacks.

- DARPA should conduct a workshop, including the industry and research communities, to explore the possibility of creating a program to develop new approaches for detection of low-vapor pressure chemical threats.
- In concert with other Federal Agencies, DoD should lead the examination of robotics and unattended sensor platforms for installation protection as a means of reducing personnel and increasing effectiveness.
- DoD should develop advanced detectors, intelligent networks, and propagation model-based decision concepts to provide greater standoff, layered defense and integrated decision making.

MARITIME SURVEILLANCE AND SECURITY

- Navy should conduct a design study for a broad area ocean surveillance system that uses low-frequency and broadband acoustics, in concert with fusing data from all-source cooperative vessel tracking systems, to allow for surface vessel location, identification, and tracking and for cueing of sea-launched cruise missile tracking systems.
- Navy should develop a system to effectively integrate existing and planned maritime Identification Safety Range (ISR) data in near-real time, including commercial (global) maritime databases.
- Navy should examine the use of surface robotic vessels and acoustic sensors for affordable underwater port surveillance.

LOW ALTITUDE AIR THREATS

- DARPA should initiate a search for breakthrough solutions that provide highly-reliable, computer-

aided, positive identification of cruise missile and other hostile, low speed, non-cooperative targets.

COMMUNICATIONS/C2 INTEROPERABILITY FOR MILITARY ASSISTANCE TO CIVILIAN AUTHORITIES (MACA) MISSIONS

- National Guard participation in SAFECOM (a DHS program) should explore and evaluate the insertion of appropriate information security technology into the program.
- DoD should ensure that the Joint Tactical Radio System (JTRS) program demonstrates that architecture, waveforms, security, and quality of service can interoperate with future commercial voice and data systems, including Internet technologies.

BASE/INFRASTRUCTURE PROTECTION

- Assign Northern Command and, as required, Pacific Command (NORTHCOM/PACOM) the mission to provide base/critical infrastructure vulnerability assessments
- NORTHCOM/PACOM should explore industry-based risk management techniques and technologies to prioritize investment in CONUS base and critical infrastructure protection

INFORMATION SECURITY

- DoD should use its best capabilities including those at NSA to support, and benefit from, the Presidential-directed, DHS-led national effort to develop solutions that dramatically reduce vulnerability to cyber attack including:

  – Government and industry cooperation relative to analysis, information sharing, incident response and recovery;

– Continuing to introduce available advanced information security products;

– Making available the experience (e.g., technical training materials, procedures, publications) gained from its effort to strengthen its cyber security operations over the last few years;

– Assisting other agencies in understanding potential cyber security threats.

- U.S. Strategic Command (STRATCOM), through the Joint Task Force – Computer Network Operations (JTF-CNO), should ensure that:

  – Defense Information System Agency (DISA) and the next generation Internet protocol (IPv6) network technology deployment is accelerated, includes enhanced security and support for priority quality of service, and is made available to DHS;

  – NSA strengthens the NIAP certification process by:

    - Testing of executable code for known vulnerabilities;
    - Certifying a distribution system for required software patches;
    - Enforcing the reliability of evaluators.

- DARPA should focus its IT research program on fundamentally strengthening the security of the Internet technology base and ensure the transition of this technology to DoD operations and the national cyber security effort.

This report is organized into two major sections. The first six chapters identify the unmet S&T requirements that must be addressed by the Department if it is to be capable to complete the evolving role likely to be assigned to it for homeland defense and in support of homeland security. The second section (Chapter 7) deals

with the technology management problem and makes recommendations for DHS based on DoD's experience.

CHAPTER 1: CBRNE PREPAREDNESS FOR CONUS BASES

DIMENSIONS OF PREPAREDNESS

Overview

This Chapter is organized by focusing initially on overall CBRN issues, followed by addressing each of the sub-categories of Weapons of Mass Destruction (WMD) in sequence: chemical, biological, and radiological / nuclear (combined). The Panel has not addressed defense against high explosives, so for the sake of clarity, the term Chemical/Biological/Radiological/Nuclear (CBRN) will be used in place of CBRNE.

The top-level CBRN defense findings from the Panel and the resultant recommendations, both systems and technology, are highlighted below.

TOP-LEVEL CBRN DEFENSE FINDINGS

The tech base for DoD / non-DoD CBRN defense is very similar; however, the applications may vary dramatically (e. g., MACA versus battlefield platform decontamination).

Base Protection

- Base function requires critical interaction with neighboring civilian community
- All current detection systems are severely limited in range
- Adequate warning and reaction time requires the off-site deployment of detection systems
- Systems will encompass both DoD and civilian authorities

General

- Some DoD requirements may not be applicable to other agencies (large volume of systems; uniform requirements; performance is often more important than cost; system optimized for low false-positives rather than low false-negatives is acceptable; mobility)
- Current DoD validated threat list for CB is too narrow for homeland security scenarios (e. g., toxic industrial chemicals, low vapor pressure threats)

CBRN Preparedness for CONUS Bases

Recommendations

Systems

- Assign NORTHCOM the responsibility to establish unique CBRN needs of CONUS base protection
  - Extend the Guardian program to include radiological dispersal device/improvised/nuclear/device (RDDs/INDs)
- DoD should evaluate the similarities and differences between the applications required for DoD and non-DoD CBRN defense and establish collaborative programs where possible
- Establish a formal mechanism which enables a shared tech base and coordinated investments.

Technology

- DARPA should initiate a program to reach out to the pharmaceutical and biotechnology industries for panenzymatic decontamination technology

- DoD and DHS should establish a joint program to pursue diagnostic technology to enable pre-symptomatic detection of BW attacks, e.g., use of cytokines
- DARPA should conduct a workshop to explore new approaches to detection of low-vapor pressure chemical threats
- In concert with other Federal Agencies, DoD should lead the examination of robotics and unattended sensor platforms for installation protection as a means of reducing personnel and increasing effectiveness
- DoD should develop advanced detectors, intelligent networks, and propagation model-based decision concepts to provide greater standoff, layered defense and integrated decision making

---

Vulnerability Assessment

The Panel recommends a comprehensive approach to preparedness using vulnerability, consequence, and risk analyses. A useful approach would apply consistent methodologies and criteria to address the evolving threats and integrate military and civilian defense capabilities with the goals of preventing attacks, reducing the vulnerability of key assets and infrastructure, minimizing the severity, consequences and duration of an attack, and recovering as quickly as possible from an attack.

The threat matrix is large, given the extensive target set and the multiplicity of attacks available to adversaries. Therefore, initial emphasis should be on threats against high-value targets (e.g., command centers, nuclear facilities, major embarkation facilities) and should include the development of event scenarios and facility monitoring strategies (i.e., cost/benefit analyses). In addition, a balance must be struck between high-consequence/low-probability WMD attacks and attacks that do not require high sophistication (in

terms of operations or technical expertise) in order to cause significant disruption.

Prevention

One central pillar in the DoD Force Projection (FP) strategy is the ability to utilize air and sea ports of debarkation in an uninterrupted manner. A significant finding of the Pope-Bragg Study[2] was that minor application of chemical warfare (CW) agent could inhibit the deployment of a major assets from CONUS to operational theater for days, or longer. The DSB Summer Study Technology and Systems Panel found from AF-XO that OCONUS concept of operations (CONOPS), specifically Kuwaiti theatre of operations, are being modified to permit more efficient base utilization in a post-CW environment. We recommend an extension of this so that post-CW (and biological warfare (BW) and radiological/nuclear warfare (R/NW)) event operations are included in CONOPS for CONUS facilities.

Responsibility for the facilities counter-chemical/biological /radiological/nuclear (C-CBRN) mission currently resides with individual base commanders, each of which reports to their appropriate Service command chain. For CONUS bases, the ability to continue operations in a CBRN contaminated environment is vital to their support of the assigned FP mission. In the role as supporting Commander to DoD's OCONUS warfighting missions, Commander NORTHCOM has the responsibility to insure this FP mission. Thus, the Panel recommends that Commander NORTHCOM be assigned the mission of CBRN CONUS base protection.

We recommend that a "pipeline" connect advances in basic science with technology development, prototyping, commercialization, and deployment. Such a pipeline will provide the advanced systems and technology that will lead to more robust and less costly protection systems. Facility protection systems should be

2 Soldier and Biological Chemical Command (SBCCOM); Karen Quinn-Doggett, author.

vigorously tested and evaluated using both real and "gaming" techniques.

Detection

A key objective of current detectors is to increase the likelihood of preventing attacks by assisting operators in the early detection of suspicious or anomalous activities. Detection of a WMD during transport may thwart an attack, and standoff detection of quantities of explosives may preempt a truck bomb or suicide bomber. Early detection of biological or chemical agents potentially can dramatically reduce casualties. Therefore, we recommend exploration of detection technologies that are autonomous, specific, and rapid, rather than focusing on dramatically increasing detection ranges. The extension of detection distance for most biological radiological nuclear and explosive (BRNE) (chemical detection is an exception) may be possible from the centimeter domain to the meter domain; however, baring the discovery of presently unknown sensing strategies / systems, the extension of this beyond the few tens of meters domain is not technically possible.

Potential CBRN targets include both transportation and fixed facilities. Because of the co-location of many military and civilian sites, existing military and civilian capabilities for monitoring and response should be integrated in selected locations. An integrated approach is also needed to address the requirements associated with National Special Security Events.

We recommend DoD/DHS coordination in the development of detection systems which incorporates the best technology and strives to reduce time and cost, while enhancing mission-specific application and cooperative problem solving.

Remediation and Restoration

Remediation of a facility is the minimum clean-up necessary in order to continue operations. Restoration is completed when the facility is certified to a post-CBRN event state of "clean". In general, decontamination is focused on remediation, while complete

rehabilitation is directed towards restoration. Capabilities needed for use after an attack include those related to decontamination and facility rehabilitation.

Particularly needed are:

- Improved crisis management tools, leveraging of existing HazMat capabilities, and CBRN effects modeling tools.
- Improved understanding of the fate and transport of CBRN agents in order to improve clean up.
- Technologies for CBRN decontamination of personnel and key equipment and rapid restoration of facilities.
- Increased emphasis on maturation and integration of new medical surveillance and response technologies, including stockpiling of vaccines, antibiotics and anti-virals at CONUS bases across the nation.

There is widespread consensus that DoD and DHHS should work closely together on medical countermeasures. The challenge lies in making this happen in the most efficient manner. We believe the DoD-DHHS interface is happening, but with varying degrees of success. For example, in the infectious disease arena, the research interface, while not formally structured, is active and ongoing. Interagency relationships have formed to foster cooperation and synergy and appear to be working fairly well through interagency agreements, memoranda of understanding, etc. Because DoD priorities differ from the priorities of the civil sector based on threats, some R&D efforts will quite rightly remain in DoD channels while others cross over to DHHS. The Panel noted that the research funding mechanisms within DoD and DHHS are quite different, and this does not help in enforcing established national priorities.

The interface between DoD, through DARPA, with DHHS, through National Institutes of Health (NIH), needs to be addressed separately from the larger DoD-DHHS relationship. DARPA staff

talks to NIH staff frequently with active discussion as to how certain promising technological efforts could continue to be funded. The NIH has a formal research review process, but there is no guarantee that projects previously funded by DARPA will continue to be funded by NIH. This is frustrating to DARPA program managers. In addition, DARPA has deviated from its 'traditional' role, because it now funds projects that are quite far along in development.

Attribution

Attribution is the ability to associate CBRN materials (including bulk materials, parts, and trace materials), assemblies, and debris with their origin, diversion pathway, and user. Robust technology and systems are needed to improve our ability to collect in near real-time and interpret technical information from an interdicted sample, assembly, or debris in order to attribute its origin or, at the least, rapidly reduce the number of possible origins. Key activities should include establishing field sample collection and transport protocols, procedures, and tools for a wide range of CBRN objects.

CHEMICAL THREAT

Overview

The chemical threat may be broken into three subsets: toxic industrial materials (TIMs), traditional CW agents, and nontraditional agents (NTAs). While the Panel recognizes that traditional CW agents likely will remain the most likely threat encountered on the OCONUS battlefield, TIMs, or, the subset of TIMs, toxic industrial chemicals (TICs), are envisioned to be the dominant homeland security threat for the foreseeable future[3]. Thus, in addition to retaining the ability to operate to the fullest possible extent in a CW contaminated battlefield environment -- and extending this capability to encompass NTAs -- it is required that DoD add TIM's to the validated threat list. This is important in

3 Finding in agreement with another DSB on CW Defense dated January 2002.

MACA for incident response, as well as potentially playing a role in special operations missions in urban areas.

The Army has a partial list of TICs; however, these are not sensed by most detector systems.[4] Traditional CW agents may be categorized either by their physiological location of action (see Figure 1)[5] or by their historical development period (see Figure 2).[6] For the purposes of this report, NTAs as a group may be considered to encompass both "others" from Figure 1 as well as the compositions, which are post-third generation in development period (see Figure 2).

Figure 1: Classes of Chemical Warfare Agents

Physiological Location of Agent Action					
Blood Agents	AsH3 Arsine	HCl Hydrogen Chloride	CNCl Cyanogen Chloride	HCN Hydrogen Cyanide	
Choking Agents	Cl2 Chlorine	ClC(O)Cl Phosgene	PFIB		
Vesicant "Blister"	S(CH2CH2Cl)2 Mustard	Cl2AsCH=CHCl Lewisite			
Nerve Agents	GA Tabun	GB Sarin	GD Soman	VX	Novichok Series
Others	LSD	Morphine	Cocaine	Ricin	CS

4 https://usachppm.apgea.army.mil/desp/pages/samp_doc/other_guidance/chppm_top27.pdf; Appendix AA

5 DTIC # ADC065552

6 DTIC # ADC065552

Figure 2: Historical Development Period Classification for CW Agents

1st Generation	AsH3 Arsine Cl2 Chlorine S(CH2CH2Cl)2 Mustard	HCl Hydrogen Chloride ClC(O)Cl Phosgene Cl2AsCH=CHCl Lewisite	CNCl Cyanogen Chloride	HCN Hydrogen Cyanide
2nd Generation	GA Tabun	GB Sarin	GD Soman	
3rd Generation VX	**4th Generation** 'Novichok' Series			

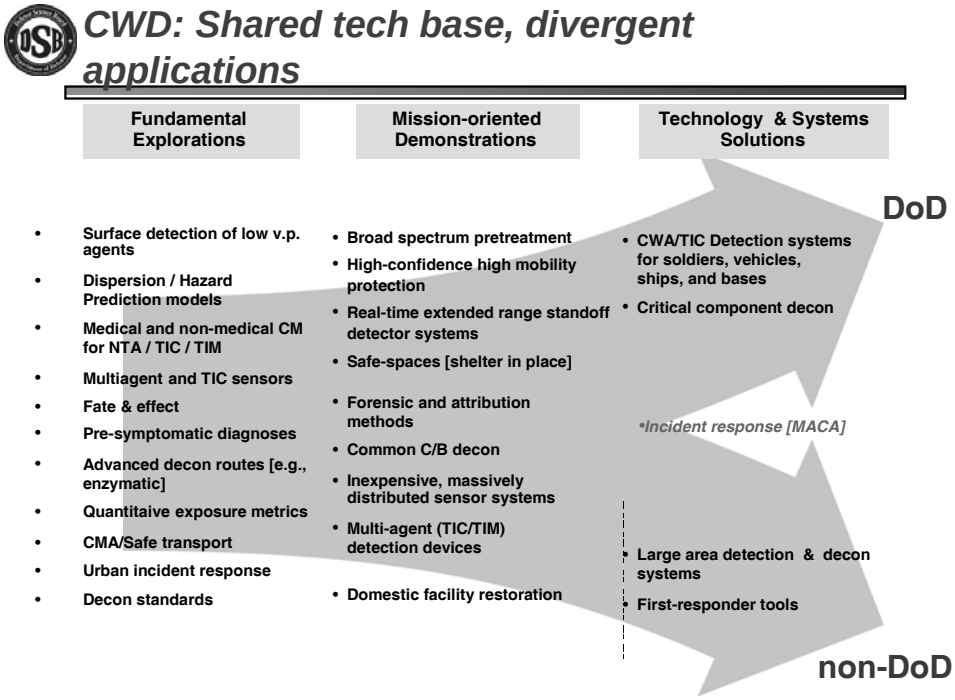
Detection

In the detection arena, the DoD is well-positioned today against traditional CW threats; however, the capability to detect either TICs or NTAs lags behind significantly. Since many of these compounds have lower vapor pressure than traditional CW agents, it is recommended that DoD significantly invest in appropriate detection strategies for these targets.

Decontamination

The chemical warfare defense area where DoD and non-DoD missions diverge most is in decontamination. In some situations, such as FP, DoD must operate quickly in a post-contaminated chemical environment, whereas non-DoD facilities may be able to "wait it out". Conversely, DoD may be able to fence off a heavily contaminated location for indefinite periods, whereas MACA may demand a return to operation more quickly, for example, Critical Infrastructure Protection or CIP. This mission divergence is illustrated in Figure 3.

Figure 3.



It has now become possible, in part because of DARPA investments, either to design rationally or incrementally engineer the kinetic and physicochemical properties of enzymes. To this end, programs should be developed within DoD to generate a suite of enzymes that can be used for the detoxification and decontamination of biological and chemical threats. Initial work at Soldier & Biological Chemical Command (SBCCOM) and elsewhere has demonstrated the feasibility of such approaches, and it is our recommendation to expand their general applicability.

In particular, enzymes can be engineered by generating random libraries and screening -- or selecting -- for desired properties, such as stability in organic solvents or foams, turnover number, or the ability to use novel substrates. In addition, computational methods have advanced to the point where virtually any small molecule substrate can be 'fit' to the active site of an enzyme. Thus, it should be possible to identify classes of enzymes that can be broadly used to break down

a wide variety of relevant organics, including toxic industrial chemicals, phosphonate chemical agents, and more complex biological toxins, such as proteins. During their selection or design, these enzymes could also be accommodated to the systems / solutions in which they would be stored / dispersed. This would improve their shelf-lives and eventually their field efficacies. While the technical means for enzyme improvement are available, these means have not – in the whole -- been integrated into a larger program to generate a particular deliverable in service of an overarching plan for decontamination following a chemical or biological incident.

Summary

An overarching CBRN defense theme is that there are both similarities and differences in the endpoints for DoD and non-DoD applications. These divergent endpoints, however, share a common technology base. As indicated in Figure 3, above, these are illustrated for CW. Figures 4 and 5 illustrate similar observations for BW and R/N defense, respectively. Thus, overall it is incumbent on DoD to continue existing investments in the technology base for each of these areas of counter-WMD, while enhancing selected topics. The top-level findings for CBRN defense are presented in TABLE 1, and the recommendations – both systems and technology – for CBRN defense for CONUS bases are contained in TABLE 2, below. Likewise, the findings for CW defense, together with the recommendations to address them, are contained in TABLE 3, below. Those more specific recommendations to the MACA mission of NORTHCOM, in the area of incident response to a National level chemical event, are contained in TABLE 4, below.

CW DEFENSE FINDINGS AND RECOMMENDATIONS

Findings

Overarching

- Nationally unique infrastructure exists at Edgewood Chemical and Biological Command (ECBC)

- Trained personnel demand exceeds current supply

Specific

- Detection focused on traditional CW agents
- General urban area decon routes lacking

Recommendations

Overarching

- Avoid duplication of investment in unique facilities
- Create significant CWD graduate training program

Specific

- Explore alternate detection modes, directed at TIC/TIM/NTA
- Invest in new, rapid, selective decon approaches (e.g., enzymatic)
- Augment Agent Fate program to encompass forensics & attribution

---

CHEMICAL WARFARE DEFENSE FINDINGS AND RECOMMENDATIONS RELATED TO MACA

Findings

- Personnel protection against CW – as well as BW – threats is becoming a more important small unit warfighter issue, as well as one for incident response
- Development of specialized kits (detection, disarmament, disposition) for use in incident response (DoD & non-DoD) are needed to reduce the threat to incident responders and improve the efficiency of rescue and restoration operations

Recommendations

- Develop broad-spectrum mobile neutralization and remediation technology (e. g., panenzymatic)
- Define requirements for lightweight, multi-agent detection systems for use in incident response, including reach-back to off-site technical expert capability, back-up modeling support, and two-way information access between incident location and Lead Federal Agency (LFA) operations / command center
- Involvement of the Assistant Secretary of Defense (Homeland Defense) (ASD (HD)) is needed early in the development of chemical and biological event incident response technology / systems in order to coordinate DoD and non-DoD tactics, techniques, logistics, etc.

BIOLOGICAL THREAT

Overview

There are currently dozens of biological agents that potentially could be used as bioweapons. The range of potential agents includes disease-causing organisms, as well as toxins, which are the natural products of organisms. Infectious organisms include contagious and non-contagious varieties, and toxins which can act in the long term (e. g., as carcinogens -- such as aflatoxin) or be more rapid acting (like ricin). The two most widely discussed infectious organisms are smallpox and anthrax -- due to the contagion and historical significance of the former and the stability and "shelf life" of the latter. There also are numerous other potential biological agents that are suspected as being assessed for weaponization by terrorists or terrorist-supporting states. Organisms such as Rift Valley Fever, Glanders, Fowl pox and filoviruses are candidates -- as well as genetically modified and novel organisms which are vaccine or antibiotic resistant. The use of lesser known agents or engineered organisms as weapons potentially is attractive to U. S. adversaries,

because they could bypass existing sensors and detection protocols and would likely not be detected until the initial cases -- potentially in the thousands – begin seeking medical care and may not then, if diseases are unfamiliar or widely distributed through early entry points (e.g., food supply). This could result in either incorrect case diagnoses or disconnected causes for correct case diagnoses, or both. Lists of agents which could be used as biological weapons abound. Typical examples of potential biological agents are shown in Table 1.[7]

TABLE 1: Typical Examples of Potential Biological Agents

Possible bio agents	Lethality	Civilian vaccine available
Anthrax (Inhalation)	High	Yes
Brucellosis	<Low if untreated	No
Cholera	Low w/treatment; High without	No
Glanders	>80%	No
Plague (pneumonic)	High unless treated within 12-24 hours	No
Tularemia	Moderate when untreated	Moderate protection
Q Fever	Very low	No
Smallpox	High to moderate	Yes
Viral hemorrhagic fever	High for Zaire strain	No
Botulism	High without respiratory support	No
Staph enterotoxin B	Low	No
Ricin	High	No
Trichothecene Mycotoxins	Moderate if untreated	No

A major focus for DoD contributions to CBRN homeland security will be in the area of improving CONUS base protection and ensuring force projection capabilities. This goal requires coordination and cooperation between civilian and military agencies – in effect a combined defense network that successfully integrates civilian and

7 Block, S.M. The Growing Threat of Biological Weapons. American Scientist 89: 2-11 (2001).

military capabilities. Current technology should be tested at DoD installations as components of an integrated system and, thus aid in the identification of technology gaps.

Detection

There is no current standoff biological agent detection capability for development in either battlefield (OCONUS) or Homeland Defense/Homeland Security (HLD/HLS) applications. A detection system to identify a generic aerosol at ranges of 5 to 30 km, or a specific aerosol at ranges of 5 to 100 km, with any degree of reliability does not exist. Bioaerosol point detection is slightly more mature; however, both selectivity and sensitivity are not at a level commensurate with the early and accurate detection necessary to warn of a biological attack. Both real time sensors and multi-agent detection are inadequate, as presently constructed. Additionally, there are only a small number of adequately trained responders to a major CONUS BW event, and the capability for mobilization and rapid deployment of likely DoD assets is, at best, marginal.

The DHHS investment is largely focused on general sensor technology development, without a firm appreciation of the particular military or emergency situations that may be encountered. For many cases, there is little or no incorporated knowledge on what chemical correlates may be associated with a given pathogen or disease state (for example, dipicolinic acid as an indicator of B. anthracis, or NO as an indicator of infection). This lack of knowledge can be ameliorated by investing in DoD research programs directed at better understanding how biothreat agents are likely to be weaponized (without actually attempting weaponization itself; for example, the identification of biomarkers associated with fermentation of common Bacilli), and at identifying biomarkers associated with alterations in human physiology. While there are some efforts in place to categorize and better understand such biomarkers, they are largely not coordinated and have not been emphasized. Such coordination and emphasis would be a unique DoD role in technology development. Based on the results of the recommended programs, DoD investments could

be better directed towards the development of particular sensor technologies demanded for detect to warn of BW attacks on CONUS bases relied upon for Force Projection (e. g., Air Ports of Debarkation (APODS) and Sea Ports of Debarkation (SPODS)).

The BIOWATCH Program probably is the most complete sensing system for this task at this time. BIOWATCH is built on the Biological Aerosol Sentry and Information System (BASIS) and consists of a network of air sampling units capable of detecting airborne organisms through the capture of organisms on a filter, and the subsequent laboratory analysis of deoxyribon nucleic acid (DNA), following sample transportation from the collection location to the remote analysis location. There are numerous technical and systems shortcomings with BASIS (e. g., it is labor intensive, has both low selectivity and low specificity, detects after an agent has been used in an attack and currently can only be used with Centers for Disease Control (CDC)-validated assays that are not state of the art). Furthermore, the high ongoing operational cost per city, the limited deployment across the Nation, and the optimized ability to detect only post-release and outdoor release (versus indoor) contribute to the systems and technical limitations of the systems.

A biological agent can be used against a water supply, in large office buildings, event venues, or in the ventilation system of transport vehicles (ships and aircraft). There are currently only limited techniques to determine if an attack has taken place in any of these scenarios and, most probably, the first notification would be the sickening -- or dying -- of exposed individuals. In the case of CONUS base personnel, local public health services and facilities are likely to become the detection "system" – while simultaneously with being tasked to respond to the attack. This highlights the significant technical and systems differences between "detect-to-warn" and "detect-to-treat" concepts. This Panel recommends a re-focusing of the DoD detection efforts from "detect-to-treat" (status quo) to 'detect to warn' (desired target within 5 – 10 years).

A DoD detect-to-warn research and development (R&D) program should include (but are not be limited to) the following elements:

- Identification of chemical correlates for pathogens or disease states, in either bioweapons or infected individuals.
- Prioritization of these chemical correlates in terms of ease-of-detection (e.g., vapor pressure, optical properties).
- Down-selection of technologies most relevant to a given chemical correlate and its ease-of-detection.
- Development of novel technologies for particular chemical correlates or relevant detection modalities.

While the identification of chemical correlates or biomarkers, and the development of sensor technologies for detecting these biomarkers could be construed as conventional "detect-to-react" scenarios, in fact in many instances, bioweapons or infected individuals will not be identified in real-time. Rather, the trace evidence of bioterrorist or biological warfare activities will remain in place and will provide keys to establishing an alert posture after an attack. As value added, this data will also aid in reducing the time required for attack attribution.

A variety of affordable, selective, and sensitive sensors for a large number of future DoD applications are required, including CONUS base protection. Investment in basic R&D is required for advancement to the needed levels of detection capability. Desired system technology objectives include:

- Response times on the order of seconds,
- Ability to quantify multiple analytes at nanomolar levels in the presence of the complex backgrounds found in urban environments,
- Ruggedness and long life,
- Cost-effective producibility in demanded quantities.

Additionally, it is critical that microbial backgrounds be characterized to understand what is "normal", so an "abnormal" concentration of something not usually present can be identified.

Overall detector technology must dramatically reduce false positives, have better resolution, and increase sensitivity, discrimination and range.

One desired outcome is presymptomatic detection. This could be based on cytokines, which fall within a category of cellular signaling molecules that turn on the immune system. Messenger ribonucleic acid (RNA) patterns are another area of promising research and, early neurotransmitters (such as nitric oxide) which show up in the breath, should be examined for applicability to the challenge of presymptomatic detection. Integrating the application of these rather new technologies with current, visual or infrared (fever) 'threat recognition' technologies would be extremely valuable. Defining what to monitor is premature at this stage; rather, investment should be directed at discovery of the chemical correlates/biomarkers both specific to a given pathogen and indicative of a broad family of potentially mutatable organisms. Specifically, a program to determine "marker" emanations (e. g., from breath and skin, particular patterns of blood flow, detailed thermal imaging, etc.) is required as the initial point for the detect-to-warn approach.

The advantages of presymptomatic detection are not limited to BW agent defense. For example, flu epidemics and other "common" naturally-occuring health events would be detected very early in the spread cycle, thereby decreasing sick personnel and increasing available deployable forces for force protection for CONUS bases. Additionally, such detection abilities would permit the deployment of "certified clean" personnel, following a BW attack on APODs and SPODs. In this case, the suspect personnel never depart CONUS and quarantined to limit further spread of diseases.

Basic research and technology development is needed – in fact a technological breakthrough is required. Techniques of biomolecular receptor-based narrow-band sensors, as well as broadband array biosensors, capable of classifying, quantifying and gradient-tracking small amounts of target agents in complex urban backgrounds are needed. Targets for agent detection can include divalent metal ions, organics, proteins and viruses. Detectors must be modular with optical or electrochemical output, and should operate by detection

using combinatorial or evolutionary biological/chemical means. The high-throughput generation of receptor molecules should be encouraged in both academia and industry, including the facile generation of antibodies, other protein and peptide receptors, and nucleic acid aptamers. The DoD is in a position to provide test beds for new technology and accelerate its development and deployment.

DoD should continue investment in the R&D required to develop wide area surveillance and – eventually -- stand off detection capabilities based on currently unknown systems. Medical surveillance capability development should be accelerated and integrated with detection systems that focus on environmental monitoring. The approximately 600,000 MDs and 2.2 million nurses in the U.S. public health system form the backbone of this biodetector array. They are educated in syndromic surveillance from a systemic viewpoint and could become inputs for lowering the signal-to-noise ratio of such an approach. Coupled with monitoring of over the counter sales, self-reporting to health care providers, and other public domain data. Medical monitoring, such as syndromic surveillance, is a critical part of detection system integration. CONUS base installations are well positioned to test and deploy syndromic surveillance systems. This is a near ideal situation for the development of presymptomatic detection strategies, since the DoD workforce culturally is accustomed to daily monitoring.

Medical Countermeasures

Table 1 above demonstrates the need for more vaccines and therapeutics to protect military as well as civilian personnel from biological attack. The vast number of potential biological organisms which could be weaponized, or those which could be employed by an unsophisticated terrorist, dictates an emphasis on therapeutics.

The current civilian systems for approving new vaccines and therapeutics are very slow and cumbersome. New and safer vaccines against the most dangerous and contagious organisms must be accelerated, along with streamlined procedures for vaccine development and licensing.

Continued development of DNA vaccines is recommended. This is a technique in which the direct injection of a DNA template leads to cellular production of the antigen and to the stimulation of an immune response. The great advantage is that one does not have to go through the difficulties inherent in making recombinant proteins or attenuated viruses/strains. Also, the DNA is not replicable and one can choose essentially any gene or epitope wanted (or even sets of genes or epitopes, in cocktails). Because of this, DNA vaccines are the method of choice for fast response in the case of a novel biowarfare attack (e. g., an under-appreciated virus or engineered strain). The basic research in this area is largely taken care of by NIH; however, this is a case in which human testing and introduction of the technology need to be streamlined.

In addition, the investigation of novel but simple techniques for vaccination should be encouraged. In particular, probiotic approaches in which lactic acid bacteria present antigens in the gastrointestinal tract may be useful for the stimulation of the human immune system. Similar approaches using other foodstuffs have also been attempted. In this way, personnel could be immunized simply by altering the composition of their diet.

The stockpiling of antibiotics, vaccines, and therapeutics at select DoD locations across the Nation should be undertaken. If an attack occurs, it is critical that these drugs be housed in quantities sufficient for the needs of the area and be quickly accessible. Additionally, the pipeline that connects advances in basic biological science with technology development, prototyping, and deployment must be streamlined. The DoD can support accelerated development, testing, and use of new vaccines and therapeutics based on the needs for force protection -- especially those applicable to environs where natural health threats include biological agents which an adversary could weaponize.

Decontamination

The continuity of full military operations -- after a biological attack -- must be improved, especially at DoD CONUS installations. Thus decontamination techniques are demanded for force projection

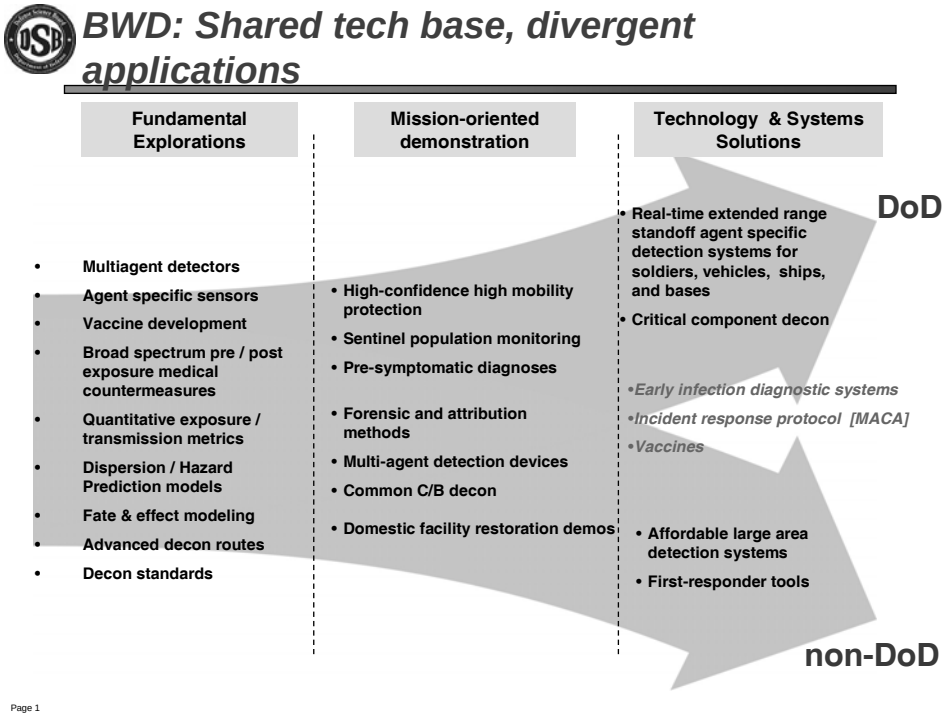
and may be drawn upon for MACA in a supporting role for incident response. These technologies and systems must also be transferred to the local first responder community quickly, together with training programs to ensure long-term viability.

As was demonstrated in the anthrax letter attacks after 9/11, more efficient and effective remediation techniques and clean up technologies must be developed, as well as standards for declaring facilities "safe" after an attack. A major contributor to the disruption and havoc after the anthrax letters was uncertainty about how to determine when a facility was "clean." Part of this uncertainty was a fundamental lack of understanding of what the ambient norms were for B. anthracis (i. e., how much is present in the natural environment).

DoD should establish standards for restoration of its installations and deploy/stockpile the resources needed both to clean up after an attack and maintain continuity of operations. The DoD must significantly invest in panenzymatic decontamination systems, if this is to become a tractable issue.

Figure 4 summarizes the current DoD and non-DoD applications, along with the shared technology base required to counter the biological threat.

Figure 4.



RADIOLOGICAL/NUCLEAR (R/N) THREAT

Overview

For several years, the Defense Threat Reduction Agency (DTRA) and the National Nuclear Security Administration (NNSA) have been working together on countering the threat from nuclear weapons, improvised nuclear devices (INDs), or radiological dispersal devices (RDDs) delivered by unconventional methods (i.e., by means other than missile or military aircraft). In July 2001, the Defense Science Board Task Force Report on Unconventional Nuclear Warfare Defense (UNWD) elaborated on this threat and recommended that DTRA develop a program to deploy, test, and demonstrate a nuclear

protection system. As of April 2003, four base systems were installed and demoed and currently all four are operating . Data continues to be collected, however the systems have been able to detect all medical, industrial and special nuclear material test items. The systems regularly alarm for persons who have received medical isotope therapy and industrial sources contained in equipment such as soil density meters. They also regularly detect radioactivity in coal, gravel and in natural gas. A Red Team effort directed against these four systems is currently underway, as well as a report on the best detectors and procedures that is being prepared for September 2003 release.

In the future, DoD should examine the practicality of providing a technical "package" for base protection, similar to the UNWD program. This package could include detectors, operational procedures, and CONOPS. The system should permit the incorporation of improved R/N sensors and other technologies as they become available as well as chemical and biological sensors. There is a need for continued development to include base-specific surveys, and installation and testing of specialized technical components, and actual system demonstrations. This package should also address issues of incident response.

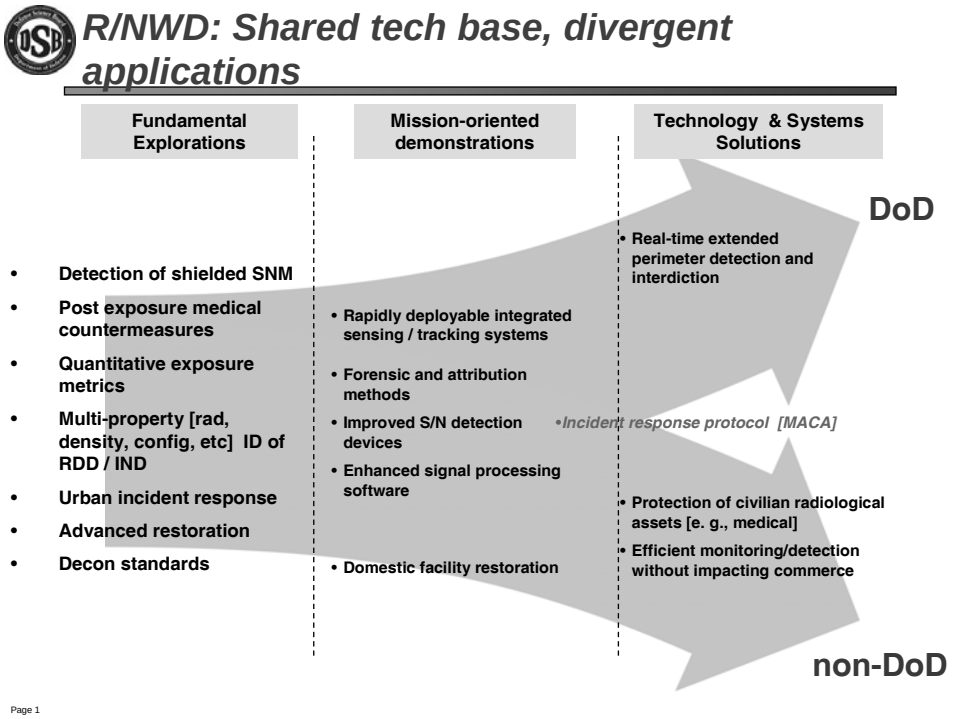
Interdepartmental Partnerships

The Department of Energy (DoE) is recognized as a leader for responding to nuclear emergencies, working with the DoD for the first response to nuclear weapon accidents and incidents. Other federal, state, local governments and tribal nations are included in the response efforts as needed. Clearly, the nation's nuclear response capability relies on a strong partnership between DoE and DoD.

In the event of a nuclear crisis, DoD can provide trained personnel, equipment, and logistical support. Since 11 September 2001, the Nation has exercised increased vigilance to ensure proper response to potential or real terrorist R/N activities, at home and abroad, while maintaining the capability to respond to other types of radiological accidents. If DoD is to fulfill future MACA commitments, development of new equipment and techniques (e.g.,

aerial monitoring, search, diagnostics, training, mitigation) may be required, as well as cooperative exercises to better define requirements. A variety of capabilities needed for radiological and nuclear emergency response include, for example, capabilities for emergency responders to obtain additional technical expertise. This requires properly configured on-site diagnostics and appropriate communication links to the home base technical experts.

Figure 5.



Attribution

Attribution is essential for the United States to appropriately respond to a domestic nuclear event (DNE). The requirement for attribution capability as a part of deterrence was reaffirmed in a recent National Security Presidential Directive (NSPD). Attribution

capability development (per the NSPD) is a joint responsibility of the "military, intelligence, technical, and law enforcement communities."

Several attribution issues are present (e.g., coordinating DoD's R/N materials knowledge-base activities with those supported by the DHS, DoE Nuclear Non-proliferation and Security Administration and intelligence community; establishing support relationships with operational agencies (FBI, DHS) to deploy debris collection teams in the crisis environment, and extended field support.).

Although DTRA's effort to modernize and "operationalize" a national rapid-attribution capability has already made significant progress, more work is required to achieve a more rapid and accurate attribution capability by the FY06 initial operating capability. Threat weapons systems and device modeling must be completed. This task will have the greatest impact on reducing the time required to attribute an event. Instead of waiting until a DNE occurs before analyzing possible weapon systems that may have been used, Domestic Nuclear Event Assessment (DNEA) is developing an event characterization database that will contain information on several likely candidate weapons systems and devices. Weapons design codes are being modified and run to provide information on weapons debris beyond that point where analysis was previously stopped in the design of nuclear weapons. This pre-event analysis will quicken the attribution time significantly. Development of efficient and rapid ground and air sampling capabilities must be completed. Unlike the collection of low-level radioactive materials from other incidents, a DNE will result in very high levels of radioactivity. Access to debris from such an event requires unique collection devices and methods. DNEA will complete the development of two robotic ground collection systems being investigated and the use of unmanned aerial vehicles. Remote collection of debris is essential due to the extremely high radioactivity levels that will be encountered. DNEA is also exploiting available debris from downwind locations, which may present human risk problems, and can also be tackled with remote devices. DNEA is developing, improving and leveraging various databases to characterize and track nuclear materials that have been diverted, stolen, or secretly manufactured to aid in identifying or eliminating possible material sources, to include radiological

dispersal device cases. The bottom line is that DNEA is the most comprehensive, coordinated, and organized approach ever undertaken by the U.S. Government to identify the perpetrators of an event using a nuclear or radiological dispersal device. It is on schedule for mid-FY06 IOC.

CHAPTER 2. MARITIME SURVEILLANCE AND SECURITY

SECURING THE MARITIME PERIMETER

NORTHCOM's AOR extends seaward to 500 miles from the continental United States. In its mission of homeland defense, therefore, the new combatant command must provide security assurance across a vast ocean area that has until now received relatively limited attention. Accomplishing this mission will require close coordination between DoD and other Federal agencies, primarily the U.S. Coast Guard (USCG), which is the Lead Federal Agency (LFA) for Maritime homeland security (MHLS) and has legal authority out to 12 miles from the continental United States. Beyond this 12 mile limit, however, the USCG has some responsibilities for search and rescue and fisheries enforcement out to the 200 mile limit of the Exclusive Economic Zone. Success will demand the development and implementation of new technologies and systems that will provide situation awareness over an ocean region of approximately 3 million square miles.

Addressing the maritime threat within the NORTHCOM area of responsibility (AOR) requires an understanding of the global Marine Transportation System (MTS), chiefly because of the possible use of a commercial vessel as a conduit for the delivery of terrorists and weapons into the United States, or as a weapon in itself, as has already occurred in the attacks on the USS Cole and the French freighter Lindberg. From a Force Projection standpoint, the domestic MTS plays a dominant role: in large-scale military deployments, more than 95% of military equipment and supplies pass through 17 domestic ports that have been identified by DoD and DoT as "strategic". It is worth noting that 13 of these 17 ports are commercial seaports.

The U.S. domestic MTS includes 361 sea and river ports, approximately 5,000 cargo and passenger terminals, and more than 1,000 harbor channels. The MTS is responsible for approximately 97% of all U.S. overseas trade. A recent Brookings Institute study

postulates that a major terrorist incident in a U.S. port would cost the U.S. economy on the order of a trillion dollars. In 2001, approximately 5,400 commercial ships made more than 60,000 U.S. port calls. The vast majority of these vessels are foreign-flag, as evidenced by the fact that less than 3% of U.S. overseas trade is carried on U.S.-flag vessels. Recent attention to the security issues associated with this complex, global transportation network have focused on marine containers, and with good reason – the vast majority of ocean-borne cargo is transported via container; more than 6 million marine containers enter U.S. ports each year, of which only approximately 2% are opened and inspected. The worldwide inventory of marine containers is estimated as 12 million.

UNITED STATES COAST GUARD

As the Lead Federal Agency for MHLS, the Coast Guard's mission is the protection of the U.S. maritime domain and the U.S. MTS. The Coast Guard MHLS Strategy, termed "Maritime Domain Awareness", has the following strategic objectives[8]:

1. Prevent terrorist attacks within and terrorist exploitation of the U.S. Maritime Domain.
2. Reduce America's vulnerability to terrorism within the U.S. Maritime Domain.
3. Protect U.S. population centers, critical infrastructure, maritime borders, ports, coastal approaches, and boundaries and "seams" among them.
4. Protect the U.S. MTS while preserving the freedom of the maritime domain for legitimate pursuits.
5. Minimize the damage and recover from attacks that may occur within the U.S. Maritime Domain as either the Lead Federal Agency or a supporting agency.

The Marine Transportation Security Act (MTSA) of 2002[9] extended the territorial waters of the United States, and Coast Guard

8 USDOT, Coast Guard, 2003.
9 S. 1214/P.L. 107-295

legal authority out to the 12-mile limit established by presidential proclamation in 1988. The MTSA of 2002 also designates Coast Guard officials as local-area Federal Maritime Security Coordinators and requires the Coast Guard to prepare National and Regional Area Maritime Transportation Security Plans. Port security is facilitated at the Federal level through the Coast Guard, Customs and Border Protection (formerly the Customs Service), U.S. Maritime Administration, and the Transportation Security Agency (TSA). FEMA is involved via response planning on both national and regional levels.

Non-Federal (State and local government and private industry) involvement in port security has increased significantly in recent years as a result of TSA port security grants and/or actions made mandatory by the MTSA of 2002 and various International Maritime Organization (IMO) agreements. However, implementation strategies and level of investment vary greatly among domestic ports because of significant differences in authority and responsibility among the more than 100 public Port Authorities in the United States.

Currently, the USCG is conducting a recapitalization program, Project Deepwater, that will provide additional platforms and capabilities beyond their current baseline. Deepwater assets to be acquired will include ISR capabilities far above their previous capabilities. The USCG acquisition plan, however, will not provide the number of ISR assets necessary to address the scope of the Maritime Domain Awareness challenge (i.e., 200 mile maritime boundary).

Maritime Domain Awareness

MDA is a critical element of both our National Security for Homeland Security Strategy and our National Security Strategy. Based on its large perimeter, porous borders (especially maritime) and societal emphasis on freedom of travel, the United States remains vulnerable to asymmetric attack from our waterways and open seas. MDA needs to be regarded as an "enterprise transformational challenge". Regrettably we have not committed the resources and organizational emphasis to reduce America's vulnerability to

maritime-generated threats. Nor have we provided the capability to project maritime forces overseas responsively in a terrorist threat environment. There is no accepted vision/definition of MDA. Any definition implies that MDA involves diverse user interests, a global knowledge base, a multi-sensor solution and the means to respond decisively to any threat. An acceptable definition must assume there is both a need and conops for global and focused maritime surveillance capability. There are many organizations with a stake in MDA. Accordingly, there is much room for conflict between different agencies and departments. DoD and DHS must resolve their different understanding of overlapping MDA requirements and responsibilities.

The DHS definition of Maritime Domain Awareness is an initiative to effectively push the nation's maritime border outward, via a combination of agreements and actions at overseas ports (via Bureau of Customs and Border Protection), the development of international maritime agreements (e.g., via the International Maritime Organization), and maritime ISR, such as through the use of Automatic Identification Systems (AIS). It is our opinion that the DHS MDA initiative does not effectively address the threat associated with **uncooperative** (large and small) vessels, small (less than 65 feet in overall length) vessels, subsurface threats, and sea-based weapons. **The Panel's definition for MDA** is the timely knowledge of position, identity, intent and history of every element, in any area of interest, operating in or influencing the maritime environment, in a way that insures that actionable information pertaining to any threat (or requiring a response) is disseminated to decision makers for an appropriate response.

CURRENT STATUS OF MARITIME SECURITY S&T

Technology development and systems integration in support of MHLS has been conducted with support from DHS, primarily via TSA and the Coast Guard, with the participation of Customs and Border Protection as well as individual Port Authorities, State and local agencies, and the maritime industry. DoD activity in this area has been focused primarily on Force Protection-related S&T, some of

which has already found its way into broader use. Examples of recent MHLS S&T developments include the following.

- Automatic Identification System (AIS) - mandated under Coast Guard and IMO rules. AIS equipment includes a position-indicating transponder and a situation display that can include, among other information: ship call sign and name, length, beam and draft, type of ship, speed over ground, heading, cargo type, destination, and route plan. Commercial vessels will be required to be fitted with an AIS transponder. Implementation deadlines are yet to be finalized, although both the IMO rules and U.S. MTSA regulations mandate a 31 December, 2004 final AIS deadline. At the present time, the range of the AIS is line-of-sight. Efforts are ongoing to enhance the value of AIS for long-range vessel identification and tracking by enabling satellite-based interrogation of AIS systems via the Global Maritime Distress and Safety System (GMDSS).
- Vessel Traffic Service (VTS) systems - radar-based ship tracking systems funded by the Coast Guard, and designed to allow for the identification and tracking of vessels NOT in possession of an AIS system.
- "Smart and Secure Tradelanes" (SST) - borrows technology from DoD Total Asset Visibility Network. Wireless cargo tracking system. Employs radio-frequency identification (RFID) technology. Other vendors are also proposing RFID-based tracking systems under the TSA Operation Safe Commerce initiative, which addresses the issue of marine container security through demonstration projects at the nation's three largest container ports- Los Angeles/Long Beach, New York/New Jersey, and Seattle/Tacoma.

- Automated Commercial Environment (ACE) - will provide Customs Officers with detailed cargo information to enable decisions before a shipment reaches the U.S. border. ACE will integrate international law enforcement and commercial intelligence with data mining tools to identify high-risk cargo.
- Automated Targeting System (ATS) – operated by the Bureau of Customs and Border Protection (BCBP), this system is designed to identify high-risk cargo.
- Advanced Passenger Information System (APIS) - this Customs system is integrated with the Coast Guard to process crew information 96 hours in advance of vessel arrival.
- International Trade Data System (ITDS) - will provide a single interface for trading partners. The benefits will include single-window filing for trade information, improved enforcement of, and compliance with trade requirements, and an improved multi-agency database for security assessments.
- Customs has implemented Non-Intrusive Technology (NII) at numerous seaports and plans to deploy additional NII systems in the immediate future. NII systems include a Mobile X-Ray System for containers, and other mobile and fixed NII systems.
- An ongoing Advanced Concept Technology Demonstration (ACTD) sponsored by SOUTHCOM (lead service – USN, with Coast Guard support) to examine the use of high frequency surface wave radar to provide continuous detection & tracking of small boats to 70nmi, low-flying aircraft and helicopters to 125 nmi, un-cooperative targets to 24 nmi, and large vessels to 200nmi. The project is

being conducted by Raytheon Co., with the demonstration phase scheduled for FY04-06.

In addition to the activities noted above, DoD involvement in MHLS-related technology development and testing includes the Joint Harbor Operations Centers (JHOCs) located at the ports of San Diego and Norfolk. Each JHOC is staffed with Navy, Coast Guard and local law enforcement personnel, and provides surveillance and command and control capabilities for protecting critical harbor infrastructure and vessels. Each JHOC is organized to facilitate the integration of different sensors – and different agencies - to provide local maritime domain awareness.

At the San Diego JHOC, the existing sensors include:

- Border Patrol Thermal/Closed Circuit Television (CCTV) cameras,
- Coast Guard (short-range) thermal imaging system (TIS) and scientific data management system (SDMS) (SM-10) cameras,
- Port of San Diego video systems,
- Navy Waterside Security Systems and Pier Cameras.

Proposed systems for future installation at San Diego (with possible funding from a TSA Port Security grant) include a long-range (75 mile) radar, a long-range TIS, and ship-based swimmer detection sonar systems for use in the carrier basin.

Another active area of DoD/DHS partnership in the area of maritime security is the establishment of various combined organizations for the collection, fusion, analysis and dissemination of maritime information. The Coast Guard operates two Maritime Intelligence Fusion Centers (MIFCs), one located on the west coast in Alameda, Ca. and the other located on the east coast at Dam Neck, Va. The Dam Neck facility is co-located with the Navy's Ship Coordination Center, which enables the Navy to track "white" shipping. The Navy and Coast Guard jointly participate in the National Maritime Intelligence Center (NMIC), located in Suitland,

Md., which is co-located with the Coast Guard Intelligence Coordination Center. In theory, information is passed from MIFC to NMIC to NORTHCOM.

Clearly, there are several multi-department efforts underway to ensure the security of cargo and passengers within the domestic and global MTS. However, several threats are not addressed with currently deployed and planned systems. With regards to OCONUS and CONUS military seaports as well as domestic ports, attacks from small vessels (e.g., the USS Cole attack) and underwater vessels/swimmers/mines remain a major concern. Within NORTHCOM's 500-mile AOR (and beyond), the threat posed by uncooperative vessels (e.g., those not complying with the AIS requirement) is not adequately addressed by the ISR capabilities of either the Coast Guard or Navy. The satellite-based interrogation of AIS systems via the Global Maritime Distress and Safety System (GMDSS) offers promise of identifying cooperative vessels at great distance from shore. Technologies and systems must be developed and implemented to detect and identify all other vessel traffic, whether friendly or not. When combined with additional information, such as that supplied by the NMIC, this combined system can provide an effective filter that identifies vessels of interest. Once these vessels are identified, further investigation and/or interdiction can be pursued. Although traditionally, surface ship detection has been pursued using high-frequency radar, such systems are severely limited in range. It is the panel's opinion that the most promising technology for enabling long-range vessel detection and identification system is a low-frequency and broadband underwater acoustics system. Such a system could be configured to detect the presence of a surface vessel at great distance offshore. Given the fact that vessels having different hull and propeller characteristics produce different acoustic signatures, an acoustic system could be used to indicate the type of vessel and possibly even the identity of the vessel.

Maritime Databases

Current maritime databases are not compatible. For example, the IMO rules regarding AIS implementation involve passenger ships,

tankers, and all ships over 300 tons. However, these rules are only enforceable when individual nations adopt their own national legislation. The U.S. MTSA of 2002 mandates AIS implementation for all self-propelled commercial vessels of at least 65 feet in length overall, towing vessels of more than 26 feet in length overall and 600 horsepower, ships carrying a certain number of passengers for hire specified by the Secretary of Transportation, and all other vessels specified by the Secretary. The recently-initiated database, Maritime Information System for Law Enforcement (MISL), is shared by the Navy and Coast Guard, and essentially combines the MIS and SEER. Other sources such as the Seawatch database are potentially over-classified. Still other databases with potential MDA utility are: Ship Arrival and Notification System (SANS), VTS, various BCBP systems, National Oceanic and Atmospheric Agency (NOAA) weather, WRANGLER, MISNA, United States Defense Attaché Office (USDAO) information, Lloyd's, Purple Finder, and Automatic Direction Finder (ADF). Secret Internet protocol router network (SIPRNET) is currently U.S. only. Veterans from OIF and OEF have emphatically stated, "Wars are fought on the SIPRNET". It would aid Canadian efforts to make SIPRNET an Australia-Canada-UK-US alliance (AUSCANUKUS) system. The Joint Fires Network (JFN) is used for different purposes by each of the services. Currently it is used for Time Critical Targeting, intelligence surveillance and reconnaissance (ISR) control, imagery intelligence (IMINT) analysis and email and chat room capabilities. JFN performs varying levels of fusion. It is a system built around a multi-int core. JFN can support MDA by serving as the vehicle for units to receive and display national level data.

Dissemination of this information is also a major problem. Stovepipes, caveats and releasability issues make dissemination a key bottleneck. Challenge Athena is on a limited number of ships. Cargo Data Logger and Battle Group Passive Horizon Extension System are not on Coast Guard assets. In addition, maritime dissemination requirements for MDA are not baselined in the Transformational Communications Architecture. C4I support plans for various airborne systems are still incomplete. The inter-departmental, Maritime Security Working Group shows promise of

addressing these concerns, particularly via increased cooperation between the Coast Guard and the Navy.

FINDINGS, NEEDS, AND RECOMMENDATIONS RELATED TO MARITIME DEFENSE

Findings

- The primary responsibility for domestic maritime security lies with the USCG, with DoD in a supporting role as required. However, the current USCG recapitalization program (Project Deepwater) will not provide sufficient ISR platforms capable of meeting the Maritime Domain Awareness requirements within the immediate coastal areas under USCG responsibility. In order to resolve this deficiency, either USCG must increase the number of ISR platforms to be procured under Deepwater; or, the Navy must be resourced to address this ISR deficiency.
- The NORTHCOM mission of homeland defense requires situation awareness over approximately 3 million square miles of ocean, out to 500 miles offshore of the continental United States. Although this requirement overlaps with the new Coast Guard initiative - Maritime Domain Awareness- in terms of its AOR, it must be recognized that the Coast Guard initiative is focused almost exclusively on the security assurance of commercial vessels and cargo/passengers. As such, it is incumbent on DoD to acquire capabilities that enable situation awareness across the NORTHCOM maritime AOR and that allow for the detection of threats originating from vessels, including threats posed by vessel-borne weapons (e.g., cruise missiles and shoulder-launched SAMs) and the vessels themselves.
- There are several competing programs vying for maritime global ISR dollars. They include space

capabilities(space based radar, GMDSS, commercial space imagery, INMARSAT, and classified systems), airborne (Global Hawk, Eagle Eye, unmanned combat air vehicle, broad area maritime surveillance(BAMS)/multi-mission aircraft(MMA)/joint automated COMSEC system (JACS) Tethered Aerostats, terrestrial jindalee operational radar network, and AIS Quiet Interlude Processing System (QuIPS), and sea-based (Deepwater, Littoral Combat Ship). The Coast Guard has reported that their solution for broad area ocean coverage is the Global Hawk UAV System. Unfortunately, due to budget constraints this system will not be procured until 2016 as part of the Deepwater Program. Even if procurement were accelerated, the Coast Guard's proposed force structure is inadequate to the task of timely surveillance of over 3 million square miles of ocean. However, with suitable cueing from the recommended integrated maritime ISR, this force structure may be adequate for target identification and tracking.

- Current maritime databases – essential to the successful implementation of the Maritime Domain Awareness initiative as defined here – exist in many different forms (paper, analog, digital), and are not compatible. This information, and other ISR-generated information, is not adequately disseminated to support MDA.

Needs

- The naval component of NORTHCOM must provide assistance to the Coast Guard for uncooperative surface ship surveillance and tracking. NORTHCOM must take the lead in providing broad area ocean surveillance for its AOR. This capability should provide for timely, long-range interdiction of vessels of interest, as well as the detection of cruise missile launches.
- The Coast Guard must lead an international effort to increase the capability and adoption of robust cooperative vessel identification, location and tracking. This effort should ideally lead to SATCOM-based global reporting. DoD should extend the existing NMIC capabilities to fuse ocean surveillance data with cooperative vessel tracking to highlight potential vessels of interest.
- Mine clearance and sub-surface surveillance and tracking are also near-term needs for the Coast Guard.
- An effort is needed to effectively retrieve, process, and integrate the information generated by NMIC, MIFC and the BCBP, using advanced data mining, formatting, and fusion tools. In addition, dissemination to users with various communication and security systems could create bottlenecks and unacceptable latency.

Recommendations for S&T

- Navy should conduct a design study for a broad area ocean surveillance system that uses low-frequency and broadband acoustics, in concert with fusing data from all-source cooperative vessel tracking systems, to allow for surface vessel location, identification, and tracking and for cueing of sea-launched cruise missile tracking systems.
- Vessel information should be interfaced to NMIC
  - Missile launch cueing data to NORTHCOM air defense system
- The Navy should develop a system to effectively integrate existing and planned maritime ISR data in near-real time, including commercial (global) maritime databases.
- The Navy should examine the use of surface robotic vessels and acoustic sensors for affordable underwater port surveillance.
  - This problem is critical to Navy OCONUS and CONUS Force Protection, as well as being applicable to domestic port security
  - The domestic application of this technology should be interfaced to Coast Guard Port Security Units (PSUs)

CHAPTER 3. LOW ALTITUDE AIR THREATS

In assessing the roles and missions for the DoD in homeland security, the defense of the continental United States against potential low altitude air threats is, clearly, a DoD mission. As such, it is, also, clearly the responsibility of the newly created NORTHCOM, as well as that of NORAD.

Low altitude air threats are loosely defined and include drones, small "kit "planes, with autopilot capability guided by GPS position measurements, and using readily available commercial equipment. The attack size is presumed to consist of a single or few weapons, launched without significant coordination in time. Emphasis is on using existing assets in an architecture that maximizes the integrated value of the assets against the land attack cruise missile (LACM) threat.

The Panel's work on this topic was enabled by the existence of an excellent report prepared by the MIT/Lincoln Laboratory. The study was chaired by L.O. Upton and was published on 23 April, 2001. It is titled "National Cruise Missile Defense Study" and much, if not all of the material in this section come from this report.

After reviewing the Lincoln study and other studies, including two previous DSB reports, this panel concluded that the low technology LACM is well within the capability of rogue nations to acquire and that the number of such nations able to procure this technology will probably increase as the technology is exported on a world-wide basis

There has been considerable work on defense against attacks that come from over Canada and there is now a growing awareness of attacks that might originate in Mexico. Indeed, our border patrol activities already include balloon-borne radars that can look many tens of miles into Mexico.

Because of this, the Panel concentrated on the problem of a LACM launched from a maritime platform targeted against a point target by a rogue nation. The reason for this is the very large number of merchant ships that crowd the civil maritime environment (> 100,000) and the very limited, current, capability to surveil these areas.

Specifically, the near term threat was considered to be a short range (<500nmi) ship launched cruise missile with a radar cross section (RCS) of between -10 and +5 dbsm at X- band, a speed of about Mach .7, with about 100 kg high explosive or WMD warhead, GPS guidance and the ability to cruise at about 300 m altitude with a 100 m terminal phase.

For the far term, the range was doubled, all at 100 m altitude, speed was increased to high subsonic, inertial guidance was assumed in addition to GPS and the RCS was considered to be of low observable quality.

The combination of the missile ranges and the stated NORTHCOM marine AOR of 500 nmi from the coastal United States results in the fact that that the available launch area from which such attacks can emanate comprise about three million square nautical miles of ocean.

An examination of existing sensors, weapon system capabilities and engagement analyses lead to the conclusion that no viable defense capability exists in NORTHCOM's AOR. There was some limited attribution and point defense capability for certain attack geometries. The Lincoln study also concluded that defense against wind dispersed chemical and biological weapons required intercepts at about 100km out at sea.

A result of this is the need for enhanced I&W capability and for a single integrated air and surface picture. In addition, it was concluded that the use of unmanned combat air vehicles for intercept could significantly lower system costs.

The very large marine area to be surveilled, the large number of possible launch platforms in this area and the need for a very tight time line led the panel to conclude that:

1. Very close coordination with the DHS/USCG activities on maritime domain awareness which focuses on cooperative vessel detection, localization and tracking and fusion of this data with the DoD maritime surveillance efforts is absolutely essential for cruise missile defense.
2. The use of low frequency and broadband acoustics in concert with fusion of data from all cooperative vessel tracking systems can provide 24/7 affordable, all weather ocean surveillance for uncooperative vessel and may also provide essential cues as to location and times of possible cruise missile launches from surface vessels, eliminating the need for radars to perform uncued search of the very large potential launch areas.
3. Once cued, current radar and unmanned platform technologies can provide the required detection and tracking of the cruise missile.
4. However, the present engagement doctrine that requires visual identification of an intruder prior to intercept cannot support the timeline engagement requirements for cruise missiles.
5. Accordingly, a key technology requiring a significant investment for risk reduction is automatic, positive hostile target recognition. This will probably require improvements in cooperative air target ID technologies and systems

Recommendations

- NORTHCOM should develop its CONOPS and requirements for cruise missile defense capability and the necessary battle management command, control, communications, and computers (BMC4I) architecture.
- To increase I&W use low frequency broadband acoustic and space-based systems to provide cueing of cruise missile launch position and time, to

significantly reduce the risk involved in searching the large ocean areas.

- DoD should continue to explore long endurance platforms such as the current high altitude airship Advanced Concept Technology Demonstration (ACTD) to enable the radar detection, tracking of the targets. Emphasis should be on cued integrated surveillance, detection, and tracking.
- DARPA should initiate a search for breakthrough solutions that provide highly reliable, positive identification of hostile cruise missiles and other low speed, non-cooperative targets.

In summary, the threat is real and is quite serious and will probably get more serious in the future. In addition, there is a major shortfall in achieving the timeline required to intercept cruise missiles that may be carrying WMD with present doctrine that requires visual ID prior to intercept.

CHAPTER 4. COMMUNICATIONS AND C2 INTEROPERABILITY

MACA COMMUNICATIONS/C2 INTEROPERABILITY REQUIREMENTS

Communications for Military Assistance to Civilian Authorities (MACA) presents a unique challenge and opportunity for DoD. Civilian authorities include the civilian parts of the Federal government, the State and Local governments and Tribal authorities, and a diversity of private sector organizations including individual people. There is a pervasive communications infrastructure for broadcast communications of radio and television, cellular telephones, wired telephones, a wide range of two-way radios that are both analog and digital, and the Internet. The Internet is becoming increasingly interfaced with other communications systems and in some cases is replacing them. The Internet includes both wired and wireless access to an increasing range of end user devices and advanced services. While the communications systems are increasingly pervasive, they are generally not interoperable or suitable for use in critical situations to protect life and property. The same kind of communications systems are needed to deal with both natural and unnatural events within the civilian population except to the extent that there may be national security information involved.

The near term challenge is to achieve effective communications for critical applications to enable interoperable command and control within the civilian sector with the ability to effectively interoperate with DoD when Military Assistance is needed. Assistance throughout the life cycle of an event from increased readiness in the case of warning, through an actual event, and beyond to the aftermath and eventual recovery needs to be provided as appropriate. DoD/NORTHCOM and the National Guard have a major role to play in providing leadership in establishing effective standards and in supporting the deployment of critical assets in cooperation with DHS. In addition, there is an opportunity for the private sector commercial products to provide enhancements to the information

infrastructure and end user devices. Early involvement of the commercial sector will enable the accelerated development of cost effective and highly functional products that can gracefully transition from pervasive applications to critical applications when needed. The communications systems include the Internet and those deployed using the Internet technology base. The Internet and other systems using Internet technology need to be enhanced as described in Chapter 6 Information Security.

Since the DoD and, for that matter, the rest of the Federal government are unlikely to be able to dictate communications systems standards to state and local governments, the DoD in its MACA role will likely be forced to interoperate with a broad range of different commercial systems. Through the Homeland Security/Homeland Defense ACTD[10], DoD is seeking to demonstrate technologies that support assured communications, interoperability with civil agencies, and command and control coordination. This ACTD has demonstrated the value of the Naval Research Laboratory's InfraLynx vehicle in exercises in Chesapeake, VA and Holden, LA (April 2002) and at 20 sites across the country from New York to Hawaii (December 2003). InfraLynx supports 24 different civilian radio protocols and can cross-connect as many as 10 at a time or patch them into landlines by satellite links.

At the radio level, DoD's Joint Tactical Radio System (JTRS) uses a software-defined radio architecture to provide interoperability with the large number of different waveforms and protocols currently deployed within the different Services. To provide the interoperability required for DoD to communicate seamlessly with the various civilian agencies in its MACA role, the JTRS program should be tasked to demonstrate that it can interoperate with future voice and data systems, including Internet technologies.

PROJECT SAFECOM

SAFECOM is a DHS program to provide a near term capability for enabling the effective interoperation of existing wireless

10 Ref X—Riley article on Information Sharing, September 2003

communications devices and systems including their interface to the wired command and control system. Such a system has the potential to improve overall situation awareness among the first responders and the ability to provide decisive information to them to save time essential for saving life and property in a crisis. However, SAFECOM has limitations because it does not address critical communications security issues and has the potential to become a natural target for an adversary who recognizes the role of communications in critical situations.

An open standards process combined with experimental pilot projects in realistic settings is essential for accelerating the development of SAFECOM in the near term. For the longer term, the SAFECOM capability should be extended to interoperate with the pervasive public communications systems to enable designated first responders with the critical capabilities they need through future enhanced commercially available commercial communications and end user devices. The future systems will provide significantly enhanced performance and functionality while also saving time. Rapid deployment of emergency wireless capability will enable increased readiness in preparation for an expected event, response to an actual event, and the recovery process.

Recommendations

As a result of these findings the panel recommends that:

- National Guard participation in SAFECOM should explore and evaluate the insertion of appropriate information security technology into the program.
- DoD should ensure that JTRS program demonstrates that architecture, waveforms, security, quality of service, *et cetera* can interoperate with future commercial voice and data systems, including Internet technologies. The DoD should review progress in this area on a semi-annual basis.

CHAPTER 5. BASE/INFRASTRUCTURE VULNERABILITY ASSESSMENT

BASE/INFRASTRUCTURE VULNERABILITY ASSESSMENT

Our national security is critically dependent upon the readiness and health of our forces and assets located at both CONUS and OCONUS bases. CONUS bases must be ready to supply personnel and equipment on a variety of time scales. In some cases, our air defenses will be called upon for strike timelines measured in only minutes whereas in other cases, deployment timelines of weeks and months apply. To respond to these needs, our base commanders must be able to ensure real time continuity of operations and readiness of assets. This in turn requires availability and support from the National Defense Infrastructure (NDI) as well as some parts of the civilian infrastructure. The latter requirement derives from the reliance of our CONUS bases upon the civilian sector both in terms of support personnel as well as infrastructure.

There are three essential aspects to the operational requirements from a base commander perspective that must be considered as one looks at the terrorist threat.

- There must be free movement of personnel and materiel within a base, from base to base within CONUS, from bases through neutral third party countries, and from CONUS bases directly to foreign objectives or staging areas.
- All deployable troops must be ready and healthy (infection free).
- There must be sufficient support from the civilian-based infrastructure, on-base and off-base, to avoid any disruption of normal operations (power, communication, supply and operational services).

Possible threat scenarios presented by a terrorist attack include the involvement of chemical agents (toxic industrial chemicals, highly toxic chemical warfare agents, etc.), biological agents (either lethal or non-lethal), radiological dispersal devices, nuclear weapons or conventional high explosives. The range of scenarios affecting base operation all start with the point of deployment by the terrorist which can be of one of three categories: on base, at the base perimeter, or within a finite zone extending out from the base perimeter, which often includes an urban area. The following table describes some of the possible deployment and delivery methods.

Figure 6.

Point of Deployment	Delivery Method
On Base	-Foreign intruder -Trusted insider -Surreptitious attachment of threats to trusted vehicles/people -Low slow fliers
Base Perimeter	-Vehicle -Human -Aerial -Nearby rail -Boat or underwater
Surrounding community and infrastructure facilities	-Aerial -Public transit modes -Private transit vehicles -Rail/port -Surreptitious entry -IT

Operational consequences immediately following a terrorist attack range from obvious destruction of either people or materiel, to temporary immobilization from chemical attack, to disruption of service through infrastructure attack, to delayed consequences from invisible biological contamination and infection. Attack through sophisticated information technologies can give rise to either immediate consequences or to longer term degradation in capabilities more difficult to isolate, such as slowing or denial of services.

DoD NEEDS, INVESTMENTS AND RELATIONSHIPS

Investments to support needs for homeland defense associated with CONUS bases must come from both the Department of Defense and the Department of Homeland Security. Within the DoD, a critical infrastructure protection (CIP) directorate exists within the Office of the Assistant Secretary of Defense/Networks and Information Integration (OASD/NII). An annual report for FY2002 describing this CIP directorate has been published. Within the Department of Homeland Security, an Undersecretary for Information Analysis and Infrastructure Protection has the lead responsibility for identification and assurance of the non-DoD critical infrastructure. Coordination of the DoD with the DHS CIP programs is needed in order to meet requirements for asset and force projection assurance by base commanders.

To ensure that an appropriate operational focus is provided, NORTHCOM should be assigned responsibility for ensuring that regular vulnerability assessments are conducted for all CONUS bases. Because much of the capability to conduct these assessments resides at the Joint Program Office-Special Technology Countermeasures (JPO-STC) and because budget support for this organization within the Navy has been inconsistent, the Panel recommends that JPO-STC be assigned to NORTHCOM[11].

RISK BASED APPROACHES TO EVALUATING BASE VULNERABILITIES

When the vulnerabilities have been identified, invariably there will be insufficient resources to address all of them. Many industries are developing new "results-oriented" risk management techniques that the DoD should consider to prioritize base vulnerabilities to potential terrorist attacks based on the likelihood of occurrence. The

11 Since this report was authored, JPO-STC has been renamed Defense Program Office for Mission Assurance (DPO-MA) and has been assigned to the ASD (HD) with responsibilities over the DoD Critical Infrastructure Protection Program.

insurance industry, the electric power industry, and many others use these techniques. While these industries have extensive experience in analyzing vulnerabilities with respect to natural disasters, accidents in the workplace, and other analogous threats for which there are no historical actuarial databases to provide accurate probabilities of occurrence there is relatively little experience to date in these industries in analyzing terrorist threats. However, recent events and customer demands, along with national legislation have led to some new developments with which NORTHCOM and other DoD HLS-related operations should be familiar.

The DoD employs some risk management approaches to evaluate vulnerabilities, but deficiencies have been seen in recent outside reviews. A recent GAO report[12], states (and DoD concurs) that the "critical elements of a results-oriented management framework are not being used by the services to guide their antiterrorism efforts. In results-based management, program effectiveness is measured in terms of outcomes or impact rather than outputs (i.e., activities and processes)." In this context, the "results-oriented framework" refers to the "Government Performance and Results Act" of 1993.

In an effort to help property/casualty carriers working to offer terrorism coverage at viable prices after the passage of the Terrorism Risk Insurance Act[13], several corporations have begun developing terrorism insurance models. Examples include: Applied Insurance Research (AIR) (www.air-boston.com), EQECAT (www.eqecat.com), and Risk Management Solutions (www.rms.com). These terrorism loss models are intended to provide a pricing framework for insurance companies, state insurance regulators, and industry groups to develop rational insurance premiums. Because of the lack of historical terrorism data with which statistical analyses can be performed, modelers have had to use other information sources,

12 COMBATING TERRORISM -- Actions Needed to Guide Services' Antiterrorism Efforts at Installations," Nov 2002

13 On November 26, 2002, President Bush signed into law the Terrorism Risk Insurance Act. This Act applies to all lines of commercial property and causality insurance and has three main elements: Insurance Availability, Disclosure, and Federal Participation in Terrorism Losses.

including subjective judgments from experts. With different data sources and different methodology, various models may generate substantially different results, yet still be valid for differing situations. These models have been used to analyze the impacts of such threats as bomb blasts, aircraft impact, and chemical, biological, nuclear, and radiological weapons.

For example, the AIR Terrorism Loss Estimation Model was recently used to support Silent Vector, a terrorism preparedness exercise held at Andrews Air Force Base in October 2002. This model consists of three major components: probabilistic loss analysis, exposure concentration analysis, and deterministic loss analysis. The AIR model was used to provide detailed exposure data for possible terrorist targets used in the exercise.

Some of the insurance companies have extensive databases of what are termed to be critical locations, including areas surrounding many DoD bases. For example, the AIR model accounts for "the likelihood of attack on more than 300,000 potential targets[14]". The EQECAT model features "hundreds of thousands of high probability terrorism 'target' sites[15]". Finally, "from a list of more than 200,000 potential sites for terrorist attack, RMS has identified 2,400 that could be considered as priority targets[16]".

In addition to the insurance industry, the electric power industry is also developing risk assessment techniques and technology to address potential terrorist threats. The North American Electric Reliability Council (NERC) (www.nerc.com) is an industry consortium originally organized to create standards and technology to reduce the risks of massive blackouts. The electric power utilities have considerable experience in responding to the impacts of equipment failures, severe weather, and other phenomena that disrupt power. However, these risk assessments and operations must be modified to respond to the terrorist threat. Currently, NERC and DHS are presenting methodologies at a series of meetings for power

14AIR press release, Nov. 2002
15 EQECAT press release, Sept. 2002
16 RMS press release, Jan. 2003

companies throughout the United States. These methodologies include risk assessment methodologies for such critical infrastructure facilities as generating plants, dams for hydroelectric power, transmission lines, etc. This work includes both physical and cyber threats, and it anticipates the possibilities of coordinated attacks. In part, these methodologies include techniques developed at the Sandia National Laboratory (i.e., Risk Assessment Methodology – Dams (RAM-D)). NERC's Critical Infrastructure Protection Advisory Group has developed a model for developing organization-specific physical threat alert level response plans, entitled, "Threat Alert System and Physical Response Guidelines for the Electricity Sector.[17]"

Other industries such as telecommunications, energy (oil and natural gas), and finance are developing similar risk assessment and response plans. There has been communications between these industry groups and the Critical Infrastructure Protection Joint Program Office at Dahlgren, VA, but we believe that this communication should be focused into more specific action by the DoD, and notably by NORTHCOM.

Recommendations

Responsibility for coordination of CIP assessment and assurance programs must be clear. Within DoD, we recommend that this occur under NORTHCOM. Responsibility begins with ensuring the existence and support of an enduring vulnerability assessment function that encompasses both the NDI, as well as the non-DoD supporting CIP relevant to base operation. We also recommend that various approaches to assessment and management of risks should explored, including an examination of what has been done in the industry by the infrastructure sector (e.g. telecommunications, energy, finance, etc.) and the insurance industry (insurers themselves, as well and insurers of insurers). These two recommendations are summarized as follows:

17 This and many other publications are available at http://www.esisac.com/library.htm.

- Assign NORTHCOM/PACOM the mission to provide base/critical infrastructure vulnerability assessments
  - Includes, as required, neighboring infrastructure (non-DoD) assets necessary to base operation.
  - Assign JPO-STC to NORTHCOM (see footnote 13)
  - Coordinate with DHS Under Secretary for IA/IP
- NORTHCOM/PACOM should explore industry-based risk management techniques and technologies to prioritize investment in CONUS bases and CIP

CHAPTER 6. CYBER SECURITY

OVERVIEW

Industry and government, including those organizations involved in U.S. homeland security, are increasingly dependent on information systems and networks. These networks include the Internet, the public switched network, and the networks controlling the U.S. critical infrastructure (e.g., the U.S. power grid, the public switched telephone network (PSTN), the Internet and Internet-based systems, etc.). This increasing dependence is shown by the strong growth of e-business and e-government initiatives, as well as DoD's use of commercial communications services. For example, during 2002, global IT spending and telecommunications revenues each exceeded $1 trillion with strong growth indicated for the future. The Internet now has significantly more than 500 million users and mobile Internet users have now exceeded 150 million. Growth has created many significant targets for terrorist activities, and consequently, protecting these networks is a high priority for DoD's HLS activities.

Despite increased security investment and awareness in the past few years, information systems and networks are increasingly vulnerable to cyber attacks. There have been significant recent Internet attacks, and security incidents on the PSTN, the U.S. power grid, the Internet, DoD networks, and many others. Known vulnerabilities include not only information systems (e.g., databases and servers) but also computer systems used to control the critical infrastructure. Data from the CERT/Coordination Center at Carnegie Mellon shows that the number of computer system vulnerabilities is now several thousand with the list doubling annually in the past few years. Furthermore, the number of reported security incidents is growing at similar rates. Much can be done today about these incidents since more than 95 percent of these security incidents on the Internet are caused by exploiting vulnerabilities for which there are known solutions. However, we are also seeing new attack strategies, and an increasing percentage of

incidents on networks like the DoD unclassified system, NIPRNET, is caused by these new attacks (14 percent in 2002).

Trends in the industry to converge networks (integrating voice, data, and video) and the introduction of broadband mobile wireless technology will continue to increase the value of services offered over these networks leading to much economic growth and improved government and industry operations. However, this trend will also provide many more high-value targets, background cover, and incentives for cyber attacks.

TRENDS IN CYBER ATTACKS

Cyber attacks include unauthorized access to information (e.g., identity theft), denial of service (e.g., Internet worms), and alteration of information and software (e.g., viruses). Recent events have shown much more sophistication, speed, and reach for cyber attacks on a variety of networks than was apparent a few years ago. For example, the SQL Slammer worm released on the Internet in January 2003 affected many thousands of systems including Internet web sites, banking ATM machines, and others within just a few hours of release. These new cyber attack strategies include random variations in their structure that reduce the effectiveness of current defensive tools.

These recent attacks also indicate a move from attacks primarily by individual hackers to higher levels of "professionalism" showing coordination and multiple strategies. These events indicate continued coordinated attacks on network infrastructure and/or network security systems. For example, the October 2002 attack on the Internet Domain Name Servers illustrates the potential for these widespread coordinated attacks.

Many recent vulnerability and threat assessments have noted weaknesses in critical infrastructure networks. Important classes of these systems are the Supervisory Control and Data Acquisition (SCADA) systems that are widely used for industrial process control, notably in the energy, power, and transportation industries. For example, in the Electric Power Risk Assessment report the National

Security Telecommunications Advisory Committee found that only 25 percent of electric power utilities operate network intrusion detection systems and less than 17 percent of these utilities would report an intrusion incident. Other studies by the FBI, the NERC, and the Institute of Electrical and Electronics Engineers conclude that SCADA systems are vulnerable to electronic attack.

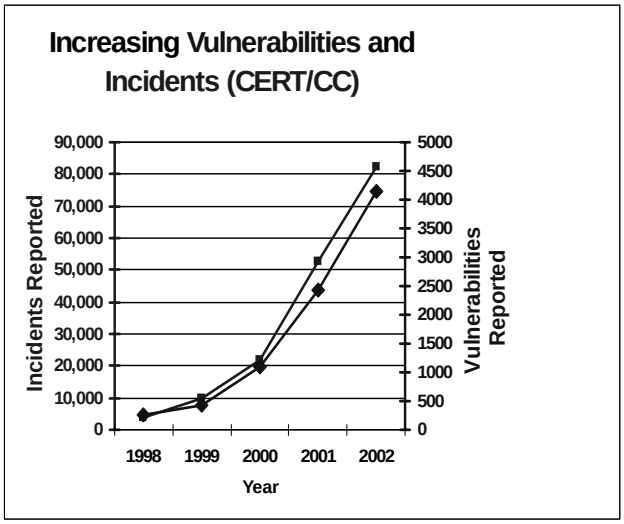
Finally, it is also clear that the major events that have occurred to date (e.g. Code Red, NIMDA, domain name sever (DNS), structured query language (SQL) Slammer, etc.) could have been far worse with relatively minor design changes in these malicious computer code. It should also be noted that while the majority of these widespread publicly visible attacks have been directed toward the Internet, the rapidly growing connectivity between the Internet and other networks creates the potential for a range of coordinated and linked attacks on U.S. critical infrastructure. For example, in a widely publicized incident in 2001, hackers penetrated a subnet on the California power grid undetected for more than two weeks. Additionally, many of the critical infrastructure networks are now providing wireless access capabilities to improve their costs and performance. However, these wireless networks are new with relatively immature security capabilities and configurations. These new capabilities create many additional cyber vulnerabilities.

Technical Capabilities Needed To Satisfy DoD HLS Requirements

The following technical capabilities would greatly improve the information security capabilities for DoD and other homeland security-related organizations.

- **Improved Simplified Systems for Network and System Configuration on Management, and Updates –** The large majority of security incidents are caused by improper system configuration and software that has not been updated to eliminate known security vulnerabilities. The number of these vulnerabilities continues to grow (see Figure below), and the capacity to address all of these

vulnerabilities is beyond the capabilities of typical network operations staffs. Accordingly, a significant improvement in automating vulnerability assessments and updates to system and network configurations and that binds authorized software to hardware to protect against unauthorized changes would do much to eliminate 95% or more of security incidents. Because many DoD systems are based on commercial products, DoD should work closely with industry to realize these improvements.



- **A Robust Key Management System –** DoD HLS roles require a robust national scales (possibly federated among state and local governments and the private sector) interoperable authentication system deployed throughout all HLS-related organizations (e.g., DoD and other national security, civil federal, state/local, first responders, private critical infrastructure organizations, etc.). NSA and DISA have built a public-key-infrastructure (PKI) system for DoD. A national PKI system is required that allows for strong authentication in cyberspace for HLS. Such a system would authenticate each user (e.g., first responders, state government officials, military personnel, etc) and enable them access and upload required information according to their individual permissions. It would also control access to critical

infrastructure systems (e.g., SCADA) and enable digital signatures and non-repudiation of signed information. The credibility of this system requires that it be built using U.S. technology.

- **Predictive Warning of Impending Attacks –** There appears to be little likelihood of reliable long-term indication and warnings for cyber attacks. However, real-time sharing of network and system data among trusted network administrators would do much to provide short-term predictive warnings. Many recent security incidents have been caused by exploitation of vulnerabilities that have been known (to at least some) for a period of days to months. Accordingly, the likelihood of predicting attacks against certain classes of targets given certain types of vulnerabilities appears somewhat feasible assuming relevant information dissemination can occur quickly and appropriate actions taken.
- **Improved Defensive Tools and Other Measures to Blunt Cyber Attacks –** Current tools (e.g. virus software, intrusion detection systems, etc.) are not sufficiently robust to stop attacks intended to penetrate networks, to deny service to legitimate users, or to corrupt data or software. These tools rely on recognizing specific attack signatures, catalogued by software providers. These systems can often be defeated by minor variations in this malicious code. Accordingly, adaptive, scalable, intelligent security architectures are needed to stop attacks with random elements. Furthermore, network and system fallback configurations would help in the event of partial system failures. Many current systems essential to HLS do not have adequate "defense in depth" implemented in their systems and networks.
- **Attribution Tools To Identify The Source Of Attack –** Capabilities to identify attack sources in real-time, providing geolocation information and

other associated metadata would be a significant advance, enabling the integration of information about cyber attacks to information in other intelligence and HLS databases. In general, developments in methods for geolocating the sources of Internet (and other network) attacks have achieved only limited success to date. However, research in this area could likely lead to further improvements.

- Network and Systems Capable of Efficient and Secure Processing of Multi-Level Security Information With Dynamic Network Membership – DoD has many requirements for the rapid creation and management of ad hoc networks (e.g., multi-national military coalitions), consisting of members coming together for a specific purpose during a limited period of time. The members must be enabled to access and provide certain types of information and be prevented from accessing other types of information. For U.S. HLS, DoD and other national security organizations must provide a variety of information to organizations with uncleared personnel, (e.g, state/local). Current technology does not permit efficient creation of these ad hoc networks, nor does it provide the ability to protect sensitive information and to extract relevant aspects of this information that could be provided at lower security levels. The technology aspects of this information sharing should be a high priority for DoD.

Recommended Specific Actions for DoD

DoD should use its best capabilities including those at NSA to support, and benefit from, the Presidentially-directed, DHS-led national effort to develop solutions that dramatically reduce vulnerability to cyber attack.

This is a critical element of the U.S. national plan for cyber security. The development of this national system will require significant cooperation among government and industry, and DoD has critical roles in this area. DoD has achieved significant improvements in its cyber security operations during the past few years. That large-scale experience should be made available through the distribution of training materials, procedures, publications, etc. to these other organizations. DoD and the private sector have experience in developing systems that can protect against an increasing range of cyber attacks if the technologies were deployed. DoD can lead with an acquisition policy that mandates certified products and continues to introduce products with new security capabilities.

STRATCOM, through the JTF-CNO, should ensure that two key operational improvements are made in cyber security

The first of these improvements are in network infrastructure, implemented by DISA. The next generation of Internet Protocol (IPv6) includes many security and quality of service (QoS) improvements. In addition to expanded addressing, simplified headers, and mobile IP features, IPv6 mandates the implementation of the secure Internet protocols (IPSec) that integrate enhanced authentication, confidentiality, compression, and key management. DISA has begun DoD's implementation of IPv6, but it should ensure that this is done with these advanced security features implemented fully. DISA should also ensure that the IPv6 capabilities for QoS are also implemented. These are particularly important for low-latency traffic such as voice and video.

The second of these improvements is in the area of certification of software to eliminate known vulnerabilities. NSA should strengthen

the current National Information Assurance Partnership (NIAP) certification by including the testing of executable code, not only design specifications. The NIAP was created to implement the "National Policy Regarding The Evaluation Of Commercial IA Products." This policy was established by the National Security Telecommunications and Information Systems Security Committee, and current policy mandates NIAP Common Criteria certification for products to be acquired by the executive branch for use on national security systems. NSA should also enable a significant increase in the automation of the testing for known vulnerabilities in order to increase the speed and reduce the costs of the NIAP certification. These improvements will speed the introduction of new and innovative products into DoD and HLS-related organizations.

DARPA should focus its IT research program on fundamentally strengthening the security of the Internet technology base and ensure the transition of this technology to DoD operations and the national cyber security effort.

Because of the critical importance of the Internet to the United States and, in particular, to DoD's roles in HLS described in this report, DARPA should focus its relevant research toward a fundamental strengthening of the security of the Internet. The following areas are those in which there is significant potential for unique national contributions by the DoD. These areas are not likely to be pursued significantly by commercial product organizations or by U.S. civil agencies. These include the following:

- Cyber attack attribution technology
- Predictive warning technology
- Interoperable key management
- Cyber warfare modeling and simulation
- Systems for cyber risk assessment and management for critical DoD systems
- Technology for remediation of security issues in infrastructure systems, notably SCADA systems

- Dynamic coalition networks with multi-level security capabilities.

CHAPTER 7. DOD TECHNOLOGY MANAGEMENT EXPERIENCE AND ITS RELEVANCE TO DHS

DARPA LESSONS LEARNED

The DoD, through its Defense Advanced Projects Agency (DARPA), has a well-deserved reputation for innovation and invention in science, technology, and transition processes for overcoming challenges at the frontier of science. While there have been many attempts to replicate DARPA in other organizations (both inside and outside the U.S. Government), they have generally been unsuccessful for a variety of reasons. Because the new Department of Homeland Security has been directed by its enabling legislation to establish a Homeland Security Advanced Research Projects Agency (HSARPA), the panel has summarized its views on the critical factors responsible for DARPA's success as lessons learned that might be useful to DHS as it stands up HSARPA. Figure 8 provides an overview of these critical success factors.

Figure 8. DARPA Critical Success Factors

Critical DARPA Success Factors

- High-level Department commitment and support
- Focused customer with definable requirements
- DARPA is about 25% of the total DoD S&T budget portfolio, is opportunity-driven, and is managed separately and differently from the requirements-driven part of the portfolio. *DHS/HSARPA needs to incorporate these dual processes (opportunity-driven and requirements-driven) in their implementation*
- DARPA program management characteristics:
  - PMs conceives ideas and sell programs based on projected outcomes
  - PM has significant autonomy and accountability
  - PM has critical mass of funding and willingness to take risks
  - PMs stay for only short periods
- DARPA mission-oriented approach is incompatible with the peer-reviewed decision making process and it requires linkage to the acquisition process

Page 31

One of DARPA's key advantages is that it only manages about 25 percent of DoD's total science and technology portfolio. Consequently, it has the luxury of being able to pursue an opportunity-driven, high-risk/high-reward research agenda. Other elements of the DoD, including the Service laboratories, are responsible for responding to specific user requirements. Equally important is the fact that DARPA has benefited from consistent, high-level support within the DoD for this positioning of its research strategy. This support has protected DARPA from the inevitable attempts to shorten its time horizon or to focus its resources on specific user requirements.

To complement this strategic positioning, DARPA has evolved a program management philosophy that is unique to the organization and is judged by the panel to be one of the key reasons for its success.

This starts with a well-promulgated willingness to take risks, which is continually reinforced by the management through an informal test of all proposed programs to ensure that they are addressing "DARPA-hard" problems. Individual program managers (PMs) are afforded considerable autonomy to make decisions and allocate resources within their program areas. Special efforts are used to attract the brightest technical people possible as PMs.

These PMs are expected to review technical developments in their field along with developing an awareness of the most difficult challenges confronting the DoD. They are challenged to conceive ideas that offer the potential for breakthroughs that provide dramatic performance improvements beyond existing capabilities. Incremental advances and reducing known solutions to practice are discouraged. The PMs operate under the leadership of their Office Directors to sell their ideas to the DARPA Director in competition with all their colleagues so that only the most promising ideas survive. To be successful in the process, a DARPA PM not only must have a great idea, but also have the passion and commitment to convince the Office Director and DARPA Director that the PM will find a way to make it happen. This approach contrasts significantly with other research strategies that rely heavily on peer reviews and consensus before a program is approved. It is the panel's judgment that peer reviews tend to result in more conservative programs that make incremental advances on prior work rather than pursuing dramatic breakthroughs.

After the program is approved, the PM, under the guidance of the Office Director, is afforded considerable latitude and autonomy in managing the program to achieve its objective. Typical programs are at least three years long and are provided a critical mass of resources. The PM has great freedom in selecting the contractor and university researchers to work on the program and to redirect them, including terminating or adding new players if necessary, as the program proceeds and new information is developed indicating that different approaches may be required to reach the desired objectives. Program managers are held accountable for making steady progress and demonstrating success at intermediate milestones. However, if a program gets into difficulty and needs to be cancelled because it is

unlikely to succeed, there is no stigma. The PM is encouraged to move on to a new area and start the process all over again.

The final element of the DARPA program management philosophy is a personnel policy that is designed to ensure that new blood, and hopefully new ideas, are continually brought into the organization. DARPA PMs expect to stay with the agency only a short period of time. The typical initial assignment is only four years. Very few stay for more than a total of four years. Consequently, each program area (called an "Office") is constantly seeking new PMs. One of the primary roles of DARPA office directors is to search constantly for individuals with the passion and technical talent to conceive of and achieve the next technical breakthrough, and provide guidance in formulating and managing programs.

Based on a review of the initial DHS legislation and budgets as well as our discussions with senior DHS officials, the panel understands the scope of HSARPA's responsibilities, and for that matter the entire DHS Science and Technology Directorate, to be much more directed toward acquisition and systems operation than the DoD S&T budget. This difference is even more pronounced when comparing HSAPRA with DARPA. The panel recommends the initial DHS leadership make specific decisions about its approach to S&T portfolio management.

It will be important for the HSARPA in particular to be very clear on its goals and objectives. With a broader charter than DARPA, HSARPA is not likely to have the luxury of allocating all its resources to high-risk/high-reward projects. However, with the similarity of organization names, Congress and others are likely to look to HSARPA for DARPA-like results unless expectations are clearly and explicitly set. If HSARPA decides to allocate a portion of its budget to long-term, high-risk research, the panel recommends that the DARPA approach should be adopted for that portion of its portfolio.

SCIENCE AND TECHNOLOGY INFORMATION EXCHANGE

As has been discussed extensively early in this report, there is a significant overlap in the technology, and to a lesser extent the

systems, that DoD and DHS require to fulfill their assigned missions. While the panel does not believe that it would be productive to require a formal coordination/integration of the S&T budgets for the two departments, we do recommend that structured mechanisms be established to exchange regularly information on activities.

These information exchanges should occur at all appropriate levels in the two departments at the assistant/under secretary levels. Because of the broad range of potential common interests, the panel recommends the DoD's ASD(HD), DDR&E and ASD(NCB) each meet periodically with the DHS Under Secretary for Science and Technology, particularly in the early formative stages of the new department to discuss problems of common interest and to share priorities and strategies. Over time, these interchanges will likely become more structured on the DHS side as its organization matures. However, the panel strongly recommends that a regular high-level interaction between the two departments on S&T issues be institutionalized.

Similarly, a regular series of information exchange meetings should established at lower levels of the departments where common interests and problems are likely to occur. Specifically, the panel recommends at least the following interactions:

- DARPA and HSARPA
- USAMRIID and DHS bio-defense program manager
- ECBC and DHS chemical-defense program manager
- DTRA and DHS nuclear-defense program manager.

Further, DoD should invite DHS to attend the relevant Technology Area Review and Assessments (TARAs) conducted by DDR&E to review the DoD laboratory research program. By inviting DHS to this existing program, DoD can facilitate information exchange and technology transfer for the good of the Nation without burdening its program with any addition bureaucracy.

During these information exchanges, DoD and DHS should look for opportunities to cooperate on problems of mutual interest. For

example, one such action might be to identify technical areas where the country has significant skill shortages – such as bio-defense, CW and radiation medical treatment, and systems analysis – to address the needs of the new world environment. Both departments would benefit from a coordinated national strategy to address these needs.

APPENDIX I. TERMS OF REFERENCE

THIS PAGE INTENTIONALLY LEFT BLANK

THE UNDER SECRETARY OF DEFENSE

3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

ACQUISITION,
TECHNOLOGY
AND LOGISTICS

06 JAN 2003

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference - Defense Science Board 2003 Summer Study on the DoD Roles and Missions in Homeland Security

You are requested to form a Defense Science Board (DSB) Task Force addressing the Department of Defense (DoD) roles and missions in homeland security.

DoD's historic missions of homeland defense and civil support are under review in light of grave terrorist and other threats to US territory and citizenry. The DoD has access to many of the systems engineering, technical capabilities, relevant technologies, logistics expertise, and modeling and simulation capabilities needed for effective homeland security. Defense forces are also critically dependent upon various infrastructures operated by DoD or provided by commercial sources and civil utilities to support its force projection war-fighting mission and also provide force protection to forces stationed within the homeland.

The development of an effective homeland security capability will involve not only the Department of Defense but the direct participation of many other existing federal, state and local agencies as described in the "National Strategy for Homeland Security," Office of Homeland Security, July 2002.

Some of the key questions related to homeland security, which will be addressed by this DSB 2003 Summer Study, are:

a. What is "homeland defense" and what specific roles and missions will the Department of Defense (DoD) be responsible to accomplish? What are the derivative unique operational responsibilities of US Northern Command?

b. What are the prioritized goals for DoD support to civil authorities in a national security emergency? What are the derivative unique operational responsibilities of US Northern Command?

c. What is the role of the National Guard and Reserve in homeland security? What are the implications for their warfighting mission?

d. What are the inter-agency processes that need to be put in place to support an integrated security strategy, planning function and operational capabilities? What are the processes for interacting with State and local governments?

e. What are the specific information sharing/fusion requirements with DoD and other governmental and non-governmental agencies? Define the processes and evaluate potential technologies to accomplish this requirement. Determine the optimal communications/hardware architectures.

f. What refinement is needed of theater security cooperation methods with Canada and Mexico? What are the short term and long term optimal goals with respect to homeland defense and military assistance to civil authorities for U.S. cooperation with these countries? Suggest a strategy to achieve these goals that addresses treaties, trade relations, and impacts.

g. There are known and many unknown vulnerabilities regarding DoD force projection. How will projection issues and responsibilities be addressed in the larger context of homeland security?

h. What are the classes of technologies and systems that DoD should have the lead in developing and fielding which have applications for homeland security as well?

Other areas to be addressed by the 2003 Summer Study include: emergency preparedness and response, defending against catastrophic threats, and consequence management in dealing with weapons of mass destruction (chemical, biological and nuclear).

This study will be co-sponsored by me as the Under Secretary of Defense (AT&L), Assistant to the Secretary of Defense (Nuclear, Chemical, and Biological Defense Programs), Under Secretary of Defense (Policy), and Northern Command (NORTHCOM). The study will be co-chaired by Mr. Donald Latham and Admiral Donald Pilling, USN (Ret). Mr. Paul Bergeron, DATSD Chemical/Biological/Defense, Colonel Neal Anderson, NORTHCOM, and Lieutenant Colonel Craig Costello, Homeland Security Task Force, will serve as Executive Secretaries. Lieutenant Colonel Scott Dolgoff, USA, will serve as the Defense Science Board Secretariat Representative.

The Task Force will operate in accordance with the provisions of P.L. 92-463, the "Federal Advisory Committee Act," and DoD Directive 5105.4, the "DoD Federal Advisory Committee Management Program." It is not anticipated that this Task Force will need to go into any "particular matters" within the meaning of section 208 of Title 18, U.S. Code, nor will it cause any member to be placed in the position of acting as procurement official.

E. C. Aldridge, Jr.

APPENDIX II. TASK FORCE MEMBERSHIP

CO-CHAIRMEN

Dr. Frank Fernandez	Private Consultant
Mr. James Shields	Charles Stark Draper Laboratory

TASK FORCE MEMBERS

Dr. Jane Alexander	Department of Homeland Security
Dr. Bob Brammer	Northrop Grumman TASC
Dr. Michael Bruno	Davidson Laboratory
Mr. John Cittadino	JCC Technology Associates
Dr. Lisa Costa	MITRE
Dr. Andrew Ellington	University of Texas at Austin
Mr. Ev Greinke	GMD Solutions
Dr. Mark Harper	US Naval Academy
MajGen Kenneth Israel (Ret.)	Lockheed Martin
Dr. William Rees	Georgia Institute of Technology
Dr. Stephen L. Squires	Hewlett-Packard Company
Dr. Rick Stulen	Sandia National Laboratory
Dr. Jill Trewhella	Los Alamos National Laboratory
Dr. Harry Vantine	Lawrence Livermore National Laboratory

DSB REPRESENTATIVE

CDR David Waugh, USN

GOVERNMENT ADVISORS

Mr. Paul Bergeron	OSD
Mr. Michael Evenson	DTRA
Mr. Ben Riley	ODUSD(AS&C)

STAFF

Mr. Kevin Gates	SAI

APPENDIX III: BRIEFINGS TO THE TECHNOLOGY AND SYSTEMS PANEL

February 18, 2003

DARPA DSO	Dr. John Carney
DARPA IAO	ADM John Poindexter, USN (Ret)
DARPA SPO	Dr. Amy Alving
MESHNET	Eric Alterman
DARPA IXO	Dr. Bob Tenney

February 20, 2003

ACTDs	Mr. Ben Riley

March 21, 2003

DARPA/IXO	Dr. Robert Tenney
DTRA	Mike Evenson
MESHNET	Eric Alterman
Cruise Missile Defense	Dr. Amy Alving

April 8, 2003

Overview of Homeland Security Programs at Sandia and LLNL	Dr. Harry Vantine /Dr. Rick Stulen
Overview of Homeland Security Programs at Los Alamos	Dr. Jill Trewhella

May 29, 2003

Systems Analysis at DoE	Dr. Richard Stulen

May 30, 2003

R&D at DHS	Dr. Parney Albright
Army Bioterrorism Programs	COL Gerry Parker
TSWG	Jeffrey David
Overview of Coast Guard R&D	Captain Jim Evans
DDR&E Perspectives on HLS Programs	Dr. Robert Foster

June 25, 2003

TTL Technologies	Dr. Tim Grayson, DARPA/TTO

June 26, 2003

DDR&E Perspectives on HLS Programs	Dr. Robert Foster,
Biodefense Programs at Edgewood	Mr. Jim Zarzycki
DISA Cybersecurity Efforts	MGen J. David Bryan, DISA

July 18, 2003

Cybersecurity	COL Tim Gibson
Cybersecurity	Rich Pethia
Coast Guard Operational Requirements for HLS	ADM Hathaway
MANPADS	Mr. Jay Kistler

APPENDIX IV. REFERENCES

Carafano, "Congress Must Act to Link Navy and Coast Guard Future Needs", The Heritage Foundation, June 13, 2003.

Fritelli, "Port and Maritime Security: Background and Issues for Congress", Congressional Research Service, RL31733, May, 2003.

O'Rourke, "Homeland Security: Coast Guard Operations - Background and Issues for Congress", Congressional Research Service, RS21125, March, 2003.

O'Rourke, "Homeland Security: Navy Operations - Background and Issues for Congress", Congressional Research Service, RS21230, June, 2003.

USDOT, Coast Guard, "United States Coast Guard FY2003 Report, Fiscal Year 2002 Performance Report and Fiscal Year 2004 Budget in Brief". Washington, 2003.

U.S. General Accounting Office. " Combating Terrorism, Actions Needed to Improve Force Protection for DoD Deployments through Domestic Seaports", GAO-03-15, Washington, October, 2002.

LINKS TO THESE AND OTHER REFERENCES:

http://www.globalsecurity.org/security/library/report/gao/d02993t.pdf

http://www.globalsecurity.org/security/library/report/gao/d03297t.pdf

http://weller.house.gov/UploadedFiles/HS%20-%20Homeland%20Security%20Coast%20Guard%20Operations%20-%20Background%20and%20Issues%20for%20Congress.pdf

http://www.maritimesecurity.com/

http://www.gao.gov/new.items/d0315.pdf

http://www.gao.gov/new.items/d03594t.pdf

http://www.house.gov/israel/issues/crs_home_port_052003.pdf

This page intentionally left blank

APPENDIX V GLOSSARY OF DEFINITIONS, ACRONYMS, AND ABBREVIATIONS

ACRONYMS AND ABBREVIATIONS

ACE	Automated Commercial Environment
ACTD	Advanced Concept Technology Demonstration
ADF	Automatic Direction Finder
AIS	Automatic Identification System
AOR	Area of Responsibility
APIS	Advanced Passenger Information System
APODs	Air Ports of Debarkation
ASD	Assistant Secretary of Defense
ATS	Automated Targeting System
AUSCANUKUS	Australia-Canada-UK-US alliance
BAMS	Broad Area Maritime Surveillance
BASIS	Biological Aerosol Sentry and Information System
BCBP	Bureau of Customs and Border Protection
BGPHES	Battle Group Passive Horizon Extension System
BMC4I	Battle Management Command, Control, Communications, Computers and Intelligence
BRNE	Biological, Radiological, Nuclear and Explosive
BW	Biological Warfare
CBRNE	Chemical/Biological/Radiological/Nuclear/Explosive
CCTV	Closed Circuit Television
CDC	Centers for Disease Control
CDL	Cargo Data Logger
CIP	Critical Infrastructure Protection
CNO	Computer Network Operations
CONUS	Continental United States
CW	Chemical Warfare
DARPA	Defense Advanced Project Agency
DDR&E	Director of Defense Research & Engineering
DHHA	Department of Health and Human Services
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DNE	Domestic Nuclear Event
DNEA	Domestic Nuclear Event Assessment

DNS	Domain Name Server
DoD	Department of Defense
DoE	Department of Energy
DTRA	Defense Threat Reduction Agency
ECBC	Edgewood Chemical and Biological Command
FBI	Federal Bureau of Investigation
FP	Force Protection
GMDSS	Global Maritime Distress and Safety System
GMSS	Is it suppose to be GMDSS
GPS	Global Positioning System
HD	Homeland Defense
HLS	Homeland Security
HSARPA	Homeland Security Advanced Research Projects Agency
I&W	Indications & Warning
IMINT	Imagery Intelligence
IMO	International Maritime Organization
IND	Improvised Nuclear Devices
INMARSATC	International Marine/Maritime Satellite
IOC	Initial Operational Capability
IPSec	Secure Internet Protocol
IPv6	The Next Generation of Protocol
ISR	Intelligence, Surveillance and Reconnaissance
ITDS	International Trade Data System
JACS	Joint Automated COMSEC System
JFN	Joint Fires Network
JHOC	Joint Harbor Operations Centers
JORN	Jindalee Operational Radar Network
JPO-STC	Joint Program Office-Special Technology Countermeasures
JTF	Joint Task Force
JTRS	Joint Tactical Radio System
KTO	Kuwaiti Theater of Operations
LAMP	Land Attack Cruise Missile
LFA	Lead Federal Agency
LO	Low Observable

MACA	Military Assistance to Civilian Authorities
MDA	Maritime Domain Awareness
MHLS	Maritime Homeland Security
MIFC	Maritime Intelligence Fusion Centers
MISL	Maritime Information System for Law Enforcement
MMA	Multi-Mission Aircraft
MTS	Marine Transportation System
MTSA	Marine Transportation Security Act
NCB	Nuclear, Chemical and Biological
NDI	National Defense Infrastructure
NERC	North American Electric Reliability Council
NIAP	National Information Assurance Partnership
NIH	National Institutes of Health
NII	Networks and Information Integration
NMIC	National Maritime Intelligence Center
NNSA	National Nuclear Security Administration
NOAA	Non-Operating Aircraft Organization
NORAD	North American Air Defense Command
NORTHCOM	Northern Command
NSA	National Security Agency
NSPD	National Security Presidential Directive
NSTISSC	National Security Telecommunications and Information Systems Security Committee
NTA	Nontraditional Agents
OASD/NII	Office of Assistant Secretary of Defense/Networks and Information Integration
OCONUS	Outside of the Continental United States
OEF	Operation Enduring Freedom
OIF	Operation Iraqi Freedom
PKI	Public Key Infrastructure
PM	Program Managers
QOS	Quality of Service
R&D	Research and Development
R/NW	Radiological/Nuclear Warfare
RAM-D	Risk Assessment Methodology – Dams
RCS	Radar Cross Section

RDD/IND	Radiological Dispersal Device/Improvised Nuclear Device
RFID	Radio Frequency Identification
RNA	Ribonucleic Acid
SANS	Ship Arrival and Notification System
SBCCOM	Soldier & Biological Chemical Command
SBR	Space Based Radar
SCADA	Supervisory Control & Data Acquisition
SCC	Ship Coordination Center
SDMS	Scientific Data Management System
SIPRNET	Secret Internet Protocol Router Network
SOUTHCOM	Southern Command
SPODs	Sea Ports of Debarkation
SQL	Structured Query Language
SST	Smart and Secure Trade lanes
STRATCOM	U.S. Strategic Command
T&S	Technology and Systems
TARA	Technology Area Review and Assessments
TIC	Toxic Industrial Chemicals
TIM	Toxic Industrial Materials
TIS	Thermal Imaging System
TSA	Transportation Security Administration
UAV	Unmanned Aerial Vehicle
UCAV-N	Unmanned Combat Air Vehicle – Navy
UNWD	Unconventional Nuclear Warfare Defense
USAMRIID	United States Army Medical Research Institute of Infectious Diseases
USCG	United States Coast Guard
USDAO	United States Defense Attache Office
VTS	Vessel Traffic Service
WMD	Weapons of Mass Destruction

PART 3: NATIONAL GUARD ROLES AND MISSIONS

This page intentionally left blank

The Terms of Reference for the Defense Science Board (DSB) 2003 Summer Study on the DoD Roles and Missions in Homeland Security specifically directs the Task Force to address "the Roles of the National Guard and Reserve in Homeland Security, and what are the implications on their war-fighting mission." The DSB was also asked to "determine the optimal communications/hardware architecture."

Section A of this chapter addresses the roles of the National Guard and specific initiatives that will assist the National Guard in support of Department of Defense (DoD) and Northern Command (NORTHCOM) missions. Since the National Guard currently has an IT architecture that can be leveraged to a much broader advantage, Section A proposes a "way ahead" in developing the IT architecture in support of DoD and NORTHCOM. Section B addresses the roles of the Army Reserve, Naval Reserve, Air Force Reserve, Marine Reserve and Coast Guard Reserve. Implications for the war fighting missions of the Guard and Reserve components will also be addressed.

SECTION A: NATIONAL GUARD ROLES AND MISSIONS

The National Guard is a unique multi-status military component with roles and responsibilities defined by federal and state law. Understanding the flexible and multi-faceted role of the Guard therefore requires an understanding of the Militia and War Powers clauses of the U.S. Constitution, the provisions of Title 32 and Title 10 of the United States Code and the Constitutions and statutes of the several states, territories and the District of Columbia (hereafter referred to collectively as the "states" or "the several states"). State constitutions and state law define the role and status of the National Guard when performing state active duty under state control for state purposes and at state expense. The federal constitution and federal laws define the role and status of the National Guard when performing federal duty under either state or federal control for federal purposes and at federal expense.

Article 1, Section 8 of the U.S. Constitution expressly authorizes the Army and Air National Guard, under the continuing control of the several states, to be used for federal purposes and at federal expense to execute the laws of the union, suppress insurrections and repel invasions. Sections 3062(c) and 8062(d) of Title 10 United States Code (USC) underscore this Constitutional authorization by recognizing that when the National Guard is used for federal purposes and at federal expense (what the United States Code refers to as the National Guard "while *in the service of* the United States") it is part of the Army or Air Force even though Guard forces remain under continuing state command and control (state C2). Various provisions of Title 32 USC elaborate on use of the National Guard "while *in the service of* the United States," thereby giving rise to the short-hand reference to this status as "Title 32 duty".

When used in Title 32 duty status, the National Guard is not subject to the *Posse Comitatus Act* and can be used to enforce all federal, state and local laws. President Bush requested use of the National Guard "*in the service of* the United States" (under continuing state control in Title 32 duty status for a federal purpose and at federal expense) to secure the nation's airports following the attacks of September 11, 2001. Title 32 duty is also the status in which the Guard has long performed counter-drug operations and homeland security/military assistance to civil authorities (HLS-MACA) missions such as Weapons of Mass Destruction Civil Support Team (CST) operations. DoD determines which missions can be undertaken in Title 32 duty status and prescribes the tasks, standards and conditions by which the Guard performs such missions, thereby assuring prescribed federal objectives are achieved, albeit by Guard forces acting "*in the service of* the United States".

The National Guard can also be used under Title 10 federal duty status (see 10 USC Sections 3062(c) and 8062(d)) for a federal purpose, at federal expense and under federal command and control. The Guard must be in Title 10 duty status for all OCONUS missions since the Militia Clause of the U.S. Constitution (which authorizes the Guard to be used *in the service of* the United States to execute the laws of the union, suppress insurrections and repel invasions) applies only in a CONUS context. When used in Title 10 status, the National

Guard becomes part of the Army or Air Force as the National Guard "*of* the United States." When used in Title 10 status for domestic missions, the Guard is therefore subject to the restrictions and prohibitions of the *Posse Comitatus Act* and all other operational restrictions attendant to the domestic employment of federal military forces.

These varied and distinct Guard duty status options provide highly desirable fiscal and operational flexibility and should be preserved. The Guard has been the first military responder in domestic emergencies in this country for more than 300 years. As a result of its unique Constitutional status, the Guard is fully integrated into state and local emergency response protocols and is the military force of choice in responding to domestic emergencies in which state and local interests are paramount. Regardless of the ultimate consequences, all domestic emergencies, including domestic terrorist attacks, are local emergencies and all consequence management responses are local. Equally important, emergency response professionals, elected officials and community leaders *trust* the Guard and enjoy a stable and mature working relationship with the Guard.

In the current global threat environment, terrorist incidents, although immediately and directly impacting the paramount interests of the state(s) involved, also affect the strategic interests of the federal government. In such circumstances, including but not limited to asymmetric attacks involving more than one CONUS incident site, the paramount interests of a given state overlap with the strategic interests of the federal government. By using the Guard in Title 32 status to the maximum extent possible in such situations, as well as all other circumstances in which the Guard is used domestically for federal purposes, DoD can quickly and efficiently leverage the Guard's situational awareness and integration with supported civilian authorities. At the same time, by authorizing use of the Guard in Title 32 status, DoD can take advantage of existing state command and control (C2) structure and establish and enforce the standards by which HLS/MACA missions are executed. This avoids the costly and time-consuming stand up of special-purpose federal command structure that is required when the Guard is federalized under Title 10. Title 32 also allows much greater

flexibility in how Guard forces can be utilized. As noted above, when the Guard is in Title 32 status it can be used to directly or indirectly enforce all local, state and federal laws. Use of the National Guard in Title 32 status also insures full operational synchronization with the National Incident Management System (NIMS), which is mandated by HSPD-5 and used by the lead federal and state civilian agencies (it should be noted that the lead state agency is also often under the statutory control of the Adjutant General).

The Guard is also America's most forward deployed domestic military force. Unlike active duty components that are confined to a limited number of CONUS installations in a limited number of states, the Guard has an organized presence in nearly every population center (3,300 locations and in more than 2700 communities) in every state, territory and the District of Columbia. As a true community-based force, the Guard is the first military responder in virtually all domestic emergencies and can respond to most disasters without external logistical support. This forward deployed posture has given rise to suggestions that the Guard be fundamentally redirected to HLS/MACA missions. Although the Task Force believes the Guard should play an important and even principal role in such missions, the Guard's essential strength in responding to domestic emergencies is derived from its OCONUS combat, combat support and combat service support experience. Moreover, the Guard's role as the nation's primary reserve combat force is vital to our national security. The Guard provided combatant commanders 2,015,270 duty days of combat, combat support and combat service support in eighty-nine (89) countries in FY01 and expanded the level of support to 9,624,919 duty days from 1 Oct 02 through 31 Mar 03. The Army and Air Guard provide nearly half of the combat capacity of the U.S. Army and Air Force for approximately 4.3% of the FY03 DoD budget. This tooth-to-tail ratio generates a powerful cost and combat power advantage. The Guard's traditional OCONUS combat roles and missions are therefore essential to our national security and to our ability to project global reach and global power within the relatively small percentage of gross domestic product (GDP) the United States expends for national security.

Homeland security and MACA responsibilities must therefore be recognized as *an* important mission but not *the* sole or primary mission of the National Guard. Although there may be a need for selected units (e.g., WMD-CSTs and Counter Drug detachments) to be specially missioned or resourced for domestic security purposes, homeland security can be most effectively and efficiently accomplished as a *dual mission* that compliments, enhances and draws its essential strength from the National Guard's continued combat force structure, training and experience.

Having recommended the continued dual-missioning of the Guard, the Task Force is also mindful that without additional personnel and training dollars the Guard could become overextended as it takes on new HLD-HLS/MACA missions. As DoD establishes HLD-HLS/MACA requirements for the Guard, it must properly resource the Guard to execute its new missions. Properly resourcing the Guard for these planning, training, exercising and employment of force functions is the most fiscally and operationally efficient way to export the DoD training culture to other federal, state and local government agencies.

EMPLOYMENT CONCEPTS AND FORCE STRUCTURE PROPOSALS

Organizational Proposals

State Joint Forces Headquarters

The National Guard Bureau reorganized as a Joint Bureau effective 1 July 2003 and separate Army National Guard and Air National Guard headquarters in each state are being replaced by a single, streamlined Joint Forces Headquarters in each state no later than 1 October 2003. Each state Joint Forces Headquarters also has billets for Title 10 active and reserve component personnel from the Army, Air Force, Navy and Marines and Title 14 personnel from the Coast Guard. *The Task Force applauds and supports this transformational Guard reorganization. It recommends the SecDef support validation of the NGB/state Joint Table of Distributions (JTDs) by the CJCS, with National*

Guard inclusion in the AC Joint Duty Assignment List (JDAL), establishment of the RC Joint Duty Assignment Reserve (JDAR), and further provide robust access to Joint Professional Military Education (JPME) for National Guard personnel.

EPLOs, REPLOs, JRADs and DCOs

The Task Force also strongly recommends that the Title 10 and Title 14 drill status reserve component Emergency Preparedness Liaison Officers (EPLOS) each of the military services have assigned to the states' former ARNG State Area Command (STARC) Headquarters be reorganized as a single, horizontally-integrated unit within each of the newly formed state Joint Forces Headquarters. The EPLOs should work together as an integrated joint unit, should continue to support the Adjutant General and Joint Forces Headquarters commander in preparing for and responding to domestic emergencies, and should report to and operate under the overall direction of NORTHCOM. Drill status reserve component Regional Emergency Preparedness Liaison Officers (REPLOs) currently assigned by each of the military services to FEMA region headquarters should also be reorganized as a single, horizontally-integrated unit in each FEMA region and should also report to and operate under the overall direction of NORTHCOM.

In addition, NORTHCOM, ASD(HD) and OSD should support the National Guard in its initiative to create a Joint Reserve Augmentation Detachment (JRAD) at each state Joint Forces Headquarters. The JRADs should be a traditional mix of full-time and part-time personnel. JRAD members should conduct their drill status duty at the state Joint Forces Headquarters and their annual training at NORTHCOM, thereby assuring each command echelon a cadre of experienced personnel that can be employed at either or both of the command echelons during contingency operations.

The Task Force further recommends that the full-time Title 10 Senior Army Advisor - Guard (SRAAG) in each state be trained and dual-hatted as the Defense Coordinating Officer (DCO) for that state, reporting to and operating under the direction of NORTHCOM. Designating the SRAAG as the DCO would give NORTHCOM a

senior full-time Title 10 officer in each state who already routinely and habitually works with and supports the Adjutant General. In his dual role as Senior Army Advisor, the SRAAG would continue to report to the Commander, Continental U.S. Army (CONUSA) on traditional combat-readiness issues unrelated to the NORTHCOM mission.

NORTHCOM planners, with the assistance of the newly reorganized and reconstituted EPLOs, REPLOs, JRADs and DCOs, should develop a complete data base of CONUS reserve components and facilities. The data should include unit and facility capabilities and availability for HLS/MACA taskings. The data bases should be kept up-to-date and should be shared with the Adjutants General and Joint Forces Headquarters in each of the several states.

WMD Civil Support Teams

The joint Army-Air Guard Weapons of Mass Destruction Civil Support Teams (WMD-CSTs) are a critical, special purpose HLS/MACA resource that should be enhanced and expanded. Each team consists of twenty-two (22) full-time Title 32 duty status members capable of conducting on-site sampling and evaluation of hundreds of potentially lethal CBRNE threat agents and providing technical information and guidance to incident commanders and other emergency responders. Each team has a nuclear science medical officer and at least ten (10) members, including all of the survey team members, possess a Duty Military Occupational Specialty Qualification (DMOSQ) in NBC Warfare. The teams are self-contained and self-deployable on a 24/7/365 basis. They have an advanced mobile communications suite capable of interacting with other emergency responders and reaching back to subject matter experts throughout the CONUS. Each CST is also capable of providing medical care and decontamination for its own team members. There are presently thirty-three (33) certified mission-ready teams in 32 states (California has two teams). The 107th Congress authorized, but did not fund, a total of fifty-five (55) teams, including a team for each of the twenty-three (23) states that do not presently have a CST. *The DSB believes the remaining 23 teams should be funded and activated as quickly as possible and that when fifty-five (55)*

teams have been certified as mission-ready the current laws restricting CSTs to CONUS operations should be amended to authorize support for OCONUS combatant commanders on a temporary, as-needed basis.

The Task Force also encourages the Secretary of Defense to task the Chief, National Guard Bureau to report to him on the feasibility of expanding ten (10) of the CSTs so that each of the ten specially-designated Title 32 units has a full, single-unit capability equivalent to that of the Marine Corps' Title 10 Chemical, Biological Incident Response Force (CBIRF). This would result in the strategic positioning of ten (10) additional CBIRF-equivalents throughout the CONUS, while leveraging the Guard's C2 and operational integration with civilian emergency responders and assuring CST coverage for the states and geographic regions in which the CBIRF-equivalent Title 32 Guard units are located. In addition, the Guard should explore the feasibility of enhancing existing Army and Air National Guard engineering, medical and security police units with additional equipment, training and other resources to assure their ability to perform core urban search and rescue, mass medical decontamination, and tactical site security functions, respectively. The enhancement of these existing drill-status Guard units, in combination with the mission capabilities of the full-time 22-member CST, would assure each state has a collective CBIRF-like response capability – albeit, not in a single unit.

Although each CST is capable of deploying with its own wheeled vehicles, there are also circumstances in which a CST must be deployed by airlift. Recognizing that military airlift might be unavailable due to restricted resources and competing priorities, *the Task Force recommends that OSD explore the feasibility of renegotiating the Civil Reserve Air Fleet (CRAF) agreement to meet the emergency airlift requirements of CSTs and other critical HLD-HLS/MACA assets.*

Transformational State HLS Plans

The National Guard has operated a successful Title 32 Counter-Drug program in each of the several states for more than thirteen (13) years. Under this program, each state determines its own unique needs and priorities for military support to civilian law enforcement

authorities and develops an annual Governor's Plan for Guard assistance in the state's war on drugs. The Chief, National Guard Bureau is the DoD action agent for reviewing and approving each Governor's Plan and for enforcing prescribed DoD program requirements.

The connection between international drug operations and international terrorism is becoming increasingly well documented. The DSB therefore believes there is an obvious overlap between National Guard counter-drug operations and potential Guard counter-terrorism operations. Guard intelligence analysts, for example, could be a valuable force multiplier for FBI Joint Terrorism Task Forces (JTTFs), newly formed state and federal intelligence fusion centers, and similar operations which fall within the core military competencies and DMOSQ functions of the assigned Guard personnel. Such integration could also be a valuable situational awareness tool for NORTHCOM. *DoD and NGB should explore the feasibility of transforming the current National Guard Counter-Drug program into a single, integrated Guard Counter-Drug/Counter-Terrorism program*.

National Guard Bureau (NGB) Statutory Reformation

As noted above, the National Guard Bureau has fundamentally transformed into a Joint Bureau effective 1 July 2003. To complete this Guard-initiated transformation, DoD should support legislative action to align the statutory authority of the National Guard Bureau with the transformational reorganization of the Office of the Secretary of Defense and the Joint Staff. The Bureau is an essential and highly efficient channel of communications between the several states and the Departments of the Army and Air Force (Title 10 USC 10501(b)); in light of the reorganization of the Office of the Secretary of Defense and the Joint Staff, however, the Bureau's statutory role should be clarified to also recognize NGB as a military channel of communications on homeland security and MACA matters between the states and the new DoD MACA executive agent (the Assistant Secretary of Defense for Homeland Defense; ASD(HD)) and the new DoD MACA agent (the Joint Staff DOMS, J-DOMS). With this legislative clarification, NGB will be able to enhance mission

coordination and information sharing capabilities, facilitate evolution of state-federal operational concepts, and support the operational needs of ASD(HD), the Joint Staff, JFCOM, NORTHCOM, and other key stakeholders. This will also enhance flexibility and the ability to quickly and efficiently leverage National Guard resources locally, regionally, and/or nationally, as appropriate to each situation.

Title 10 USC 10501-10503 and DoD Directives 3025.1 (Military Support to Civil Authorities) and 3025.15 (Military Assistance to Civil Authorities) should also be amended to reflect these new relationships and operational concepts. These amendments will facilitate transition to effective command relationships, operational processes and supportive infrastructure capabilities.

INFORMATION OPERATIONS PROPOSALS

Joint CONUS Communications Support Element (JCCSE)

The HLS/MACA mission mandates capabilities to share information in order to provide situational awareness and facilitate planning and execution of HLS/MACA mission requirements within both a joint and inter-agency framework. Additionally, the trusted information environment and supporting infrastructure design must support vertical and horizontal information exchange, anytime/anywhere information access, and joint/inter-agency collaboration capabilities that extend from the national level to the state level and, ultimately, to the incident command site.

Because of its community-based presence, the National Guard will be a critical and early contributor to the trusted information sharing environment and will also have a need for timely access to information and collaboration tools in order to effectively carry out the Guard's HLS/MACA responsibilities. The Army and Air National Guard also have IT capabilities that can be leveraged to extend the trusted information environment from the DoD enterprise level to the state level and down to the incident scene.

As illustrated in Figure 1, a Joint CONUS Communications Support Element (JCCSE) should be established to support these requirements. ASD(HD) should request a Joint

Staff Action tasking NORTHCOM to create a JCCSE and further tasking the National Guard Bureau to develop and operate the JCCSE as a national mission in support of OSD and NORTHCOM. Capabilities managed by the JCCSE will support military HLS/MACA requirements, but can also be leveraged to provide information sharing capabilities to the Department of Homeland Security (DHS) and other lead federal agencies (LFA) in support of the National Response Plan (NRP) and National Incident Management System (NIMS).

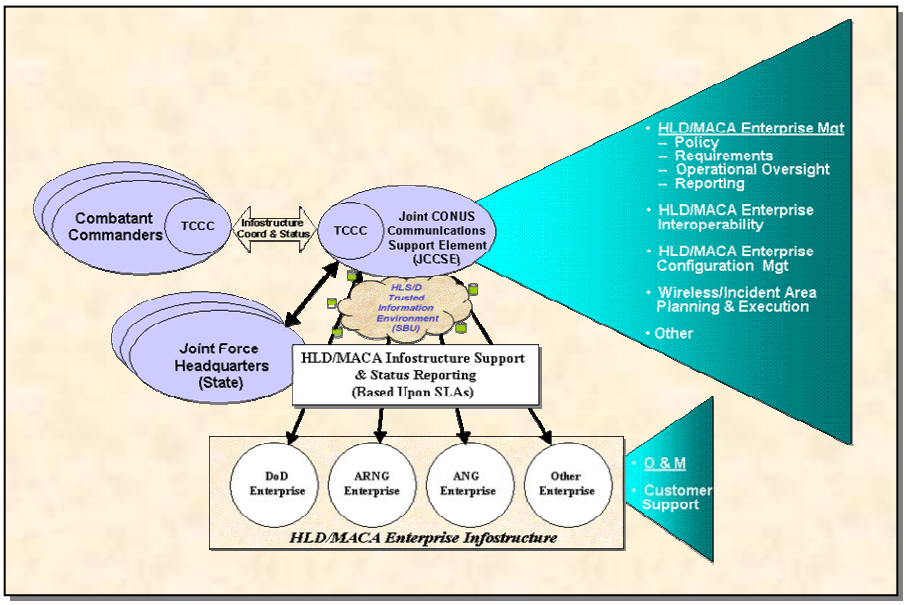


Figure 1. Notional JCCSE Construct

The JCCSE staff should not only include the ANG and ARNG, but also other reserve component and active personnel as appropriate.

The JCCSE should have as its foundation the National Guard IT networks (both Army and Air) as well as other available network capabilities. It should support NORTHCOM by providing a single focal point for enterprise management of those HLS/MACA-related infostructure capabilities (networks, applications, and services) that

extend the trusted information exchange environment from the DoD enterprise level to the state level and down to the incident site. Additionally, the JCCSE should be responsible for planning and executing employment of deployable tactical communications that provide forward information exchange capabilities at the incident site as well as reach-back to the state and national levels.The JCCSE mission and command relationships should be synchronized to current and emerging NORTHCOM mission requirements (e.g., support of the National Capital Region Joint Task Force) and should have a direct coordination and reporting relationship with NORTHCOM in order to provide comprehensive enterprise-level management and oversight of the HLS/MACA infostructure. Additionally, command relationships and operational processes established for the JCCSE must be adaptable throughout the entire spectrum of operations to ensure effective enterprise management tailored to the current operational needs at all times. Finally, command relationships must be established between the JCCSE and the Joint Force Headquarters in each of the several states.

To summarize: OSD should direct a Joint Staff Action tasking NORTHCOM to (1) create a Joint CONUS Communications Support Element (JCCSE) and (2) task the National Guard to develop and operate the JCCSE to fulfill the mission. Upon receipt of the tasking, NGB should collaborate with NORTHCOM to develop a detailed concept of operations and undertake all required missioning actions necessary to stand up a JCCSE.

The JCCSE must address the backbone network requirements as well as local area net issues. The Global Information Grid-Bandwidth Expansion (GIG-BE) program, sponsored by the Assistant Secretary of Defense for Networks & Information Integration (ASD-NII), addresses the backbone network requirements and the DHS-sponsored SAFECOM program is addressing the local area net requirements.

Global Information Grid-Bandwidth Expansion (GIG-BE)

In describing his vision for Defense Transformation, The Secretary of Defense stated:

"The two truly transforming things, conceivably, might be in

- information technology and information operations and
- networking and connecting things in ways that they function totally differently than they had previously.

And if that's possible, what I said, that possibly the single-most transforming thing in our force will not be a weapon system, but a set of interconnections and a substantially enhanced capability because of that awareness."

Secretary Rumsfeld – August 9, 2001

A major initiative in support of this vision is the Global Information Grid-Bandwidth Expansion (GIG-BE) program. Fully supportive of net-centric operations, the GIG-BE will be a ubiquitous, secure, robust, optical, IP terrestrial network providing increased bandwidth and physical diversity to DoD users worldwide. This capability will be essential to the success of the JCCSE initiative. The current program for expanding the GIG-BE was based on requirements developed prior to the attacks of September 11, 2001 and thus did not consider the new and emerging requirement for HLD/HLS or the correlative National Guard requirements.

The Task Force recommends that ASD(NII) immediately consider expansion of the current program to encompass these new missions on an accelerated timeline. An analysis of the current GIG-BE expansion program shows fourteen (14) state Joint Forces Headquarters (JFHQ) that are within reasonable proximity to the GIG-BE backbone. Expanding the current program to provide an optical connection to these fourteen (14) JFHQ locations would begin to address this shortfall in supporting the new requirements of HLD/HLS. The objective solution should be an optical connection to the GIG-BE for the JFHQ of each state in order to maximize information exchange capability.

SAFECOM

The President's Management Council has established wireless interoperability for public safety as a domestic security priority. The Department of Homeland Security is therefore pursuing an e-Government Initiative for Wireless Public SAFEty Interoperable COMmunications (SAFECOM) in coordination with other government agencies. SAFECOM is addressing communications interoperability at the incident site, examining ways to create a standard for interoperable wireless transmissions and looking at current and future systems to address the issue. The Adjutants General have also recognized the need to extend existing National Guard communications architecture down to the incident command site and the National Guard Bureau is examining current DoD systems, to include the Land Mobile Radio (LMR) system, the Force XXI Battle Command, Brigade and Battalion (FBCB2) system, and the future Joint Tactical Radio System (JTRS) as possible answers to the incident site interoperability issue. *The Task Force concurs with these Guard initiatives and objectives, commends the Chief, NGB for providing military representatives on the SAFECOM Committee and recommends that NGB be designated as the lead DoD representative for the SAFECOM project.*

EMPLOYMENT OF FORCES PROPOSALS

The creation of a Joint Forces Headquarters in each state gives the Governor and the Adjutant General a more streamlined force deployment capability and provides NORTHCOM a meaningful forward deployed command structure in each of the several states. Governors have extraordinary constitutional and statutory emergency powers and they exercise those powers principally through the Adjutants General for both civil and military exigencies. The Guard is the first military force to respond to domestic emergencies, nearly always in state active duty status. When state and federal interests converge or overlap in a domestic emergency situation, however, and whenever national command authorities determine it is in the national interest to utilize the Guard for federal

domestic purposes, the Guard should be used in Title 32 status to the maximum extent possible.

There are numerous fiscal and operational advantages in using the Guard in Title 32 status, as opposed to federalized Title 10 status. As previously noted, the Guard can be employed in Title 32 status using existing state command structure and without the need for a time consuming and costly stand-up of a special federal command structure. Use of the Guard in Title 32 status also allows most domestic missions to be accomplished jointly, through Army and Air Guard volunteers, without having to involuntarily mobilize Guard units. As an example, post-9/11 airport security missions were accomplished principally through the mobilization of individual Army *and* Air Guard volunteers, thereby diffusing the impact throughout the *entire* Guard force rather than a singe service element (by contrast, the subsequent federalization of the Army Guard for border security assistance impacted only the Army Guard and had a disproportionate negative impact on the readiness of Army Guard units to perform their OCONUS war-trace missions). Staffing a mission with volunteers from the entire Guard force also avoids impacting members for whom mobilization would be a personal or employer hardship as well as those for whom a domestic mobilization would conflict with their primary employment as civilian emergency responders.

Adjutants General can also manage an activated Title 32 force in such a way that individual soldier and airman training and unit training requirements continue to be met (i.e. soldiers and airmen are scheduled so that days off coincide with scheduled individual soldier training and unit training assemblies in which the Title 32 soldiers and airmen are required to participate) while simultaneously meeting the federal Title 32 mission objectives.

The continued state management of the activated Title 32 force assures that combat readiness is not degraded in the units from which the volunteers have been drawn. If and when other combatant commanders require Title 10 forces, Adjutants General can order personnel from Title 32 status to Title 10 status (backfilling with other personnel on voluntary or involuntary Title 32 orders for the

domestic mission) to deploy OCONUS with their combat units, thereby meeting the needs of both NORTHCOM and OCONUS combatant commanders. The Task Force notes that OSD has traditionally used Title 32 duty primarily for training purposes, since military training obviously satisfies federal as well as state objectives. *The Task Force believes the better course is to use the Guard to the maximum extent possible in Title 32 status for all federal-purpose domestic operations*, as was done in executing the airport security mission in the immediate aftermath of the September 11 terrorist attacks. *OSD should request and support legislation that enhances the flexibility of employing the Guard in Title 32 status for domestic operational purposes, to include training and exercising with civilian emergency responders and deploying in support of lead civilian agencies*.

The National Response Plan (NRP) prescribes the process by which DoD and Title 10 forces can be tasked to support a lead federal agency which is itself supporting the lead state agency in charge of a given state's emergency management operations. In many instances, the supported lead state agency will be under the statutory control of the Adjutant General. Even when that is not the case, the Adjutant General will have a close working relationship with the head of the supported lead state agency. Since all disasters and all emergencies are local, Guard forces will already have been deployed pursuant to the Governor's emergency orders and will have been fully integrated into the mature and ongoing state and local emergency response. *The Task Force* therefore *believes that maximum unity of effort can be achieved by having the later arriving Title 10 forces operate under the "supervisory authority" of the Adjutant General or his subordinate Joint Forces Headquarters commander or Joint Forces Task Force commander.* "Supervisory authority" is a well-established joint doctrine that results in Title 10 forces taking their operational direction from a designated entity outside their chain of command. Full command and control (COCON, TACON, OPCON and ADCON) remains with the Title 10 authorities and is not relinquished to the Adjutant General or anyone else in state active duty status or Title 32 duty status; the deployed Title 10 forces are merely directed to operate under the "supervisory authority" of the state's senior military commander, the Adjutant General. This force employment policy would insure the priorities and operational objectives established by

the Governor's emergency proclamations are accomplished by a true unity of effort under the operational oversight of the Governor's senior military commander. This force employment recommendation is consistent with existing doctrine and does not require any statutory, regulatory or doctrinal change.

Recognizing that these force status issues are poorly understood by many military officials, including commanders at senior levels, *NORTHCOM, in collaboration with each of the 54 Adjutants General, should develop a "Guide to Legal Authority and Rules of Engagement in the States and Territories."*

PROGRAMMATIC SUPPORT PROPOSALS

National Guard HLS/MACA requirements should be included in NORTHCOM and PACOM Integrated Priority Lists. DoD should also provide policy and resource support for upgrades to National Guard administrative and operational communications and IT capabilities, including enhanced capability for information sharing and mission coordination extending from the national and regional levels down to the state level and local incident site. Although the National Guard has significant capabilities that can be leveraged for HLS/MACA missions, existing capabilities must be enhanced to fully support the scope of envisioned homeland defense and homeland security mission support for NORTHCOM and OSD. Additionally, since Military Assistance to Civil Authorities has historically been based on a "leverage what you have" construct, dedicated funding has been exceptionally limited. The HLS/MACA mission could likely involve regional or national scenarios that demand more robust levels of preparedness similar to traditional OCONUS theaters of operation. *Validation of National Guard requirements through the JROC/IPL processes, with formal NGB membership and participation in the processes, is needed since the Guard will be a principal support force for the NORTHCOM combatant commander.*

DoD should authorize, fund and equip the National Guard to train and exercise with civil authorities in accordance with DoD-approved HLS/MACA plans. Training is a vitally important element in developing and sustaining preparedness and expertise for

HLS/MACA operations. Traditionally, funding for military training and exercising with civilian authorities has been confined to preparation for suppressing riots and other civil disturbances. The potential for regional or national-level terrorism attacks expands the range of potential military support to civil authorities, thereby necessitating more robust civil-military training and exercising. Although the National Guard has been funded to participate in JCS exercises in support of "theater warfare" scenarios, no funding has been provided for the Guard to participate in HLS-related joint exercises such as JFCOM's "Determined Promise." *Guard training for HLS/MACA mission requirements should be authorized and funded* both to develop mature operational processes and to enhance and sustain skills in joint and combined (i.e., active/reserve military and civilian emergency management/response) HLS/MACA mission support.

SUMMARY

Adopting the Task Force's recommendations with regard to the roles of the National Guard in Homeland Security would result in an End State in which:

- The National Guard of the several states acts as the principal DoD agent for assessing, planning, training, deterring, defending against and responding to terrorist threats and other HLS/MACA requirements in coordination with and in support of lead civilian agencies, while simultaneously providing the primary reserve combat force for the United States Army and Air Force for OCONUS wartime missions.
- The National Guard is utilized, to the maximum extent possible, in Title 32 federal duty status for all domestic missions, thereby leveraging the fiscal and operational advantages of continued state control while accomplishing DoD prescribed tasks, standards and conditions and overall mission objectives. Such a policy will also maximize the

readiness of Guard forces for short-notice, simultaneous deployments in support of OCONUS combatant commanders.

- The National Guard maintains a CST in every state and territory, including at least ten (10) single-unit CBIRF-equivalent CSTs strategically located throughout the CONUS, plus a multi-unit CBIRF-like capability in all states achieved through coordinating the training and deployment capabilities of each state's CST and Army Guard and Air Guard engineering, medical and security police units.
- The National Guard Bureau and state Joint Forces Headquarters perform as true joint force military echelons, populated with Title 10 and Title 32 personnel from the Army, Air Force, Navy and Marines and Title 14 personnel from the Coast Guard and in which the National Guard Bureau serves as the primary channel of communications between the several states and the Secretaries and Chiefs of Staff of the Army and Air Force, the Secretary of Defense, the Assistant Secretary of Defense for Homeland Defense, the Joint Staff and NORTHCOM.
- The National Guard establishes and operates a Joint CONUS Communications Support Element (JCCSE) as a national mission in primary support of OSD and NORTHCOM and secondary or incidental support of the Department of Homeland Security and other lead federal agencies. The JCCSE will rely on the GIG-BE for IT backbone services and will develop an enterprise-wide wireless, local area net in conjunction with the DHS SAFECOM program.
- Command and Control at the Joint Forces Headquarters in each state will be strengthened as Emergency Preparedness Liaison Officers (EPLOs), Defense Coordinating Officers (DCOs), and Joint

Reserve Augmentation Detachments will be working together as an integrated joint unit reporting to NORTHCOM. In addition, the Senior Army Advisor, dual-hatted as the Defense Coordinating Officer for each state, will also be reporting to and operating under the direction of NORTHCOM.

- Both NORTHCOM planners and Joint Forces Headquarters planners in each state will have a complete database of Reserve Component units and facilities that will include unit and facility capabilities and availabilities, as well as transportation requirements.

SECTION B: THE ROLE OF THE RESERVES

The Summer Study team had inputs from each of the Reserve forces describing their HLS/MACA roles and capabilities. Although there are similarities in their approaches, there are also important differences. Section B therefore addresses each of the Reserve Forces separately. They each recognize the necessity of a careful balance of homeland defense and homeland security needs (see Defense Planning Guidance FY 04-09) with the requirements of the ongoing global war on terror.

THE ARMY RESERVE

Capabilities and Functions

Numerous studies and other initiatives--all with long-term ramifications for the Army Reserve--are in progress to define policies, programs and roles of the military in HLS. The *National Strategy for Homeland Security* and several "companion strategies" that have not yet been published provide essential focus to these ongoing efforts. As discussions focus on the role of the military, potential emerging roles and functions for the Army Reserve will need to be based on established warfighting capabilities. Army Reserve support to Combatant Commanders for Combat Support (CS) and Combat Service Support (CSS) forces highlight their capability to execute a dual-mission in support of homeland security missions and requirements and represent critical capabilities in the overall federal emergency response capability, particularly in Military Assistance to Civil Authorities (MACA) in support of homeland security and NORTHCOM anti-terrorist operations. The Army Reserve is well positioned to assume a significant role as a DoD response force provider for homeland security in concert with the National Guard, local first responders, and other federal agencies.

Currently, there is a tiered military response to an emergency situation in which community-based National Guard elements in state active duty and Title 32 status assist local first responders.

When local and state assets (to include the National Guard) prove insufficient to cope with a crisis, the President can activate federal assets that may include use of military assets. A provision in DoD Directive 3025.1, Military Support to Civil Authorities (MSCA) provides for a commander's immediate response in order to save lives, prevent human suffering, or mitigate major property damage. The Army Reserve's core competencies of Combat Support, Combat Service Support, and Training Support provide significant capability to support civil support operations. Core competencies include Regional Readiness Commands (command and control capability), Chemical, Biological Identification and Detection, Decontamination, Medical, Mortuary Affairs, Civil Affairs, Psychological Operations, Aviation, Information Operations, Logistics, Military Police, Engineer, Installations, Signal, and Training Support.

Examples of Army Reserve capability to contribute significantly to homeland security today include the ability to quickly establish hospital services in areas where such facilities are insufficient or nonexistent; deployment of chemical/biological reconnaissance and decontamination assets; and general military support and assistance such as was used during the 2002 Olympic Games in Salt Lake City, Utah. Army Reserve Emergency Preparedness Liaison Officers (EPLOs) work with the National Guard and FEMA region headquarters for consequence management purposes. The interaction and coordination between established organizations will enhance national preparedness as well as individual and collective readiness of the Army Reserve.

The Army Reserve with its specialized capabilities in its CS/CSS core competencies can augment the federal role in homeland security at the local and state levels, particularly in assistance for pre-event planning and training for homeland security emergencies. Assisting and training local pre-event planning exercises, involvement in training first responders in activities such as crowd control, chemical and biological responses, mass casualty management and medical triage, and information operations are capabilities the Army Reserve possesses to support its role in homeland security. Army Reserve soldiers can fill gaps, augment, and reinforce the National Guard and local first responders, as part of the Federal response.

Infrastructure

Army Reserve installations can serve as a significant mission multiplier to local agencies. For example, the Army Reserve is "forward deployed" in communities through its installations at Fort Dix, NJ; Fort McCoy, WI; Fort Hunter Ligget, CA; Camp Parks, CA; and Devens Reserve Forces Training Area, MA. In addition, there are 962 other facilities positioned throughout the homeland where Army Reserve capabilities reside. Army Reserve capability that is closely located to hometown communities reduces response times should it be necessary to assist in a response.

The Army Reserve Role

The Army Reserve will exercise its core competencies to enhance and support the National Strategy for Homeland Security. When directed in accordance with a tiered response plan, it will respond by applying expertise, training and warfighting capabilities to assigned homeland security missions, to include provision of military assistance to civil authorities. The Army Reserve is a significant federal force provider that is "forward deployed" in communities with an established nationwide structure. As such, it is well positioned to assume the role of a primary DoD response force using its specialized capabilities in its core competencies. Additionally, the Army Reserve can augment the federal role at the local and state levels and assist local and state governments to plan and train for homeland security emergencies.

The Army Reserve's Role in Future Homeland Security Support

The Army Reserve is a full partner in the critical Army mission of future homeland support. The capabilities resident in the Army Reserve need to be considered at all levels of planning to support critical homeland security planning tasks. The nature and degree of severity of catastrophic homeland security incidents necessitate reinforcing accessibility to the Army Reserve in a compressed manner to provide prompt and adequate response. The variety of capabilities that exist in the core competencies of the Army Reserve will be skill

sets that will be in demand in a response to a catastrophic homeland security incident. Therefore, *the Task Force recommends that when there is a need for these core competencies the Army Reserve should be considered as the lead Title 10 response force*.

THE NAVAL RESERVE

Concept of Operations

The Navy will remain forward deployed. Navy provides the firepower and flexibility to deal with crises anywhere in the world. The Navy's primary role in Homeland Security is to maintain a forward presence and take the Global War on Terrorism (GWOT) to the adversary's homeland.

The Coast Guard is the lead for Homeland Security –Maritime (HLS-M). The Navy and the Coast Guard have been actively conducting experiments and exercises to identify the gaps and seams within the HLS-M support process. The Navy has years of experience working with the Coast Guard in the Maritime Defense (MARDEZ) organization, and can move forward quickly because of those established working relationships. The Navy needs to strengthen its Reserve Liaison organization with the Coast Guard by adding more Full-Time Support (FTS)/Selected Reserve (SELRES) billets at key Coast Guard commands and vice versa.

Northern Command (NORTHCOM) has significant expertise in the Air Defense arena. NORTHCOM should clarify their requirements with regard to the sea services (Navy, Coast Guard, and Marine Corps) and, especially, with regard to an acceleration of manning documents and an immediate assignment of FTS/SELRES to NORTHCOM to support the development of HLS-M requirements. There should also be continuing NORTHCOM support for the development and stand-up of LSS capability. Additional FTC/SELRES billets will be required at Joint Forces Command (JFCOM) and Commander Fleet Forces Command (CFFC) as the emergency roles and missions of HLS-M are defined.

The Naval Reserve is ideally suited to take on Navy's future HLS-M missions. One hundred percent of the Naval Coastal Warfare (NCW) and Naval Control and Protection of Shipping (NCAPS) capability reside in the Naval Reserve. Navy capabilities can be leveraged off that experience to move quickly into the still undefined HLS-M mission. Naval Reserve units have played a significant role in counter drug missions and that experience can be leveraged into HLS-M missions. The requirements are not going away, and the Naval Reserve remains one of the lowest cost alternatives.

Today's technology can be leveraged to implement a robust HLS-M capability. Many Naval Reserve assets including aircraft and NCW systems, especially the Littoral Surveillance System (LSS), are compatible with existing USN systems. A Joint Fires Network/Littoral Surveillance System functional demonstration is scheduled for November 2003 to validate the capabilities to quickly move into HLS-M missions. Another proposed C4ISR JFN/LSS demonstration, which would take place in the U.S. Gulf Coast over a two-year period, will help to further define the capabilities of the Naval Reserve in the HLS-M mission area.

THE AIR FORCE RESERVE

The Air Force Reserve (AFR) provides twenty percent of the Air Force capability for a mere four percent of the Air Force budget. The AFR units contribute in virtually every mission, and in some areas, are the sole provider of capabilities to include weather reconnaissance and aerial spray. Reservists from communities around the country have answered the call following September 11th, and others continue to provide humanitarian assistance, fight forest fires, and provide healthcare and medical supplies to war-torn areas around the world. The AFR continues to explore new mission areas by expanding AFR participation in undergraduate pilot training, test flight support, special operations, space, information operations, and the fighter reserve associate program. While the AFR contributes to the overall capabilities of the Air Force, it also owns and maintains eleven Air Reserve Bases/Stations that resemble active duty installations in which it has sole responsibility for installation security

and force protection. Finally, the AFR has tenants at 58 other locations, creating a highly dispersed command.

How AFRC Presents Forces--The Air and Space Expeditionary Force (AEF)

The Air and Space Expeditionary Force (AEF) concept embodies how the Air Force organizes, trains, equips, and sustains its Total Force (Active Duty, Air National Guard (ANG), and AFR) to meet the security challenges of the 21st Century. This concept maximizes Total Force integration, with ANG and AFR making a significant (25% of aircraft support and approximately 13% of combat support forces) contribution to the AEF composition.

Air Force Reserve Response Post-9/11

While the AFR remained active in the AEF, exercises, and ongoing operations, the main focus of the Air Force Reserve Command (AFRC) was directed at the nation's response to the terrorist attacks on September 11, 2001. Following the attacks in New York City, Reserve airlift supported the movement of fire equipment, search dogs, earth-moving equipment, and mortuary affairs personnel. AFRC tankers conducted airborne and ground alert to provide Combat Air Patrol (CAP) support over major U.S. cities. Reserve airlift assets were placed on alert for rapid stateside deployment support for Army and Marines. The AFR associate AWACS unit was activated to provide airborne surveillance and control of fighters performing escort duty, while F-16s from Homestead ARB, Florida, and Naval Air Station Joint Reserve Base, Fort Worth, Texas, were placed on Homeland Defense CAP alert. Of the 75,000 members in the command, over 23,000 were activated, with 4,500 reservists extended into a second year because of continuing requirements of OPERATIONS NOBLE EAGLE, ENDURING FREEDOM and IRAQI FREEDOM.

Capabilities-Based Approach and Support for Homeland Security (HLS)

The Air Force is transforming to a capabilities-based approach that will allow it to provide more effective and efficient combat power where needed. The Air Force has developed a series of Concepts of Operations (CONOPS) to aid in the transformation of the Air Force planning, programming, requirements, and acquisition processes. The Homeland Security (HLS) Task Force CONOPS spells out the Air Force's expeditionary warfighting concepts and capabilities most applicable to support the Joint Force Commander in defending the homeland. Air Force capabilities from across the spectrum will prevent attacks and mitigate disasters before they occur; protect our critical infrastructure, communities, and U.S. air and space domains; and respond to attacks as well as natural and man-made disasters. Capability priorities will change depending upon the situation, legal limitations, and budgetary constraints. However, the Air Force core competencies continue to serve as the bedrock in performing the Air Force HLS mission by supporting the combatant commanders in defending the homeland, preserving U.S. ability to project forces, and providing support to civilian authorities.

Way Ahead for the Air Force Reserve in HLS Missions

The Air Force will need to anticipate, help plan against, and respond to requests for assistance from local, state, or other federal agencies. In this effort, the AF must determine how to balance its primary responsibility to provide air and space combat forces to Combatant Commanders while simultaneously supporting on-going and contingency employments of forces in support of civil authorities across the land.

On the civil support side, Memoranda of Agreement (MOA) need to be developed between AF*R installations and local, state, and federal entities.* At the local level, such agreements will tie DoD installations to their surrounding communities and serve as the basis for providing support for local communities in response to man-made or natural disasters. The Air Force currently utilizes AFR Emergency Preparedness Liaison Officers (EPLOs) to inform National Guard and

state officials on capabilities that the Air Force may have available to support in a crisis. The EPLOs also inform and educate installation commanders on how to further develop MOA with local emergency response agencies. Via medical, civil engineering, communications, and security forces personnel (within legal constraints such as the Posse Comitatus Act), the Air Force will be able to move quickly to protect critical installation/community assets as well as mitigate further damage caused by a disaster.

As a fully integrated force in the Total Force concept, the AFR is fully committed to support the needs of the Air Force and unified commanders. It should be apparent that the Reserve Components are crucial to the nation's defense. AFRC is working shoulder-to-shoulder with the Active Duty and ANG in the long battle to defeat terrorism. Even before 9/11, AFRC was an active participant in day-to-day AF operations. They are no longer a force held in reserve solely for possible war or contingency actions; they are at the tip of the spear. As NORTHCOM and the Assistant Secretary of Defense for Homeland Defense develop policy and concepts of operations, the role of the AFR will be to continue to provide highly trained, dedicated airmen for national security.

THE MARINE CORPS RESERVE

The Marine Corps contribution to Homeland Security is shaped by their expeditionary nature. The focus is overseas.

The Marine Corps contribution to Homeland Security is to provide organized, trained, and equipped units capable of incident response, deterring, detecting, and defending against asymmetric threats against U.S. territories, population, and critical infrastructure.

Marine Corps Contributions

The 4th Marine Expeditionary Brigade (MEB) Antiterrorism (AT) can provide designated supported commanders rapidly deployable, specially trained, and sustainable forces that are capable of detecting terrorism, conducting activities to deter terrorism, defending

designated facilities against terrorism, and conducting initial incident response in the event of chemical, biological, radiological, or nuclear terrorist attacks, worldwide.

The 4th MEB (AT) Chemical and Biological Incident Response Force (CBIRF) when directed, can forward-deploy and/or respond to a credible threat of a chemical, biological, radiological, nuclear, or high-yield explosive (CBRNE) incident in order to assist local, state, or federal agencies and designated supported commanders in the conduct of consequence management operations by providing capabilities for agent detection and identification; casualty search, rescue, and personnel decontamination; and emergency medical care and stabilization of contaminated personnel.

II Marine Expeditionary Force (II MEF) and I Marine Expeditionary Force (I MEF) have supported NORTHCOM with rapidly deployable Quick Response Forces (QRFs) to support FEMA regions within the continental United States (CONUS).

Marine Forces Reserve (MARFORRES) supports the ten FEMA regions and two Continental U.S. Army (CONUSA) Headquarters through the Marine Emergency Preparedness Liaison Officer (MEPLO) Program. Thirty-seven Reserve officers have been identified to support the program with twenty-four Reserve officers currently assigned.

Marine Corps installations are receiving enhanced First Responder training and equipment and are in the initial stages of fielding limited chemical, biological, radiological and nuclear (CBRN) detection equipment. The Marine Corps takes the position that any CBRN incident affecting a USMC installation will require a coordinated community-wide response and as a result are actively engaged with their surrounding civilian communities in developing mutually supportable plans, training, and exercises to enhance installation and community security, incident response, and communications connectivity.

Additional Marine Corps Support

The Marine Corps supports, and will continue to support, Homeland Security as follows:

- Provide NORTHCOM with a Service Component (MARFORNORTH) to support its Homeland Security mission.
- Provide a Service component (Marine Corps National Capital Region Command) to support JFHQ-NCR for land HLD and Civil Support in the National Capital Region.
- Marine Emergency Preparedness Liaison Officers (MEPLOs) support each of the FEMA Regions and serve as the liaison effort between the Marine Corps and FEMA Authorities for Homeland Security.
- Continue to support NORTHCOM requests for forces (RFFs) as approved by SECDEF for domestic contingency missions.
- Installation commanders continue to have authority to support their local community with emergency assistance.

THE COAST GUARD RESERVE

Coast Guard Authorities/Competences

The Coast Guard is a military, maritime, multimission service with broad statutory authorities, membership in the intelligence community, a well-developed command and control structure and extensive experience in conducting or coordinating complex operations.

The Coast Guard is simultaneously and at all times one of the Armed Forces of the United States (14 USC 1) and a law enforcement agency (14 USC 89). Called up under the Secretary of Homeland Security they are Title 14. Called up by the President they are Title

10. By law, they are a military force and a law enforcement agency. Basically, jurisdiction is U.S. waters and high seas for U.S. ships and vessels of unknown origin. During smuggling operations, the Coast Guard can deputize Navy vessels as law enforcement organizations reporting to the Coast Guard.

Coast Guard Role in Homeland Security

The *National Security Strategy,* the *National Strategy for Homeland Security,* and the *U.S. Coast Guard Maritime Strategy for Homeland Security* define the Coast Guard's Homeland Security mission. The Coast Guard is the lead federal agency for Maritime Homeland Security, and is also Federal Maritime Security Coordinator in U.S. ports as designated by the Maritime Transportation Security Act of 2002.

In addition, the Coast Guard is the supporting agency to the Federal Emergency Management Agency for declared missions or emergencies under the Federal Response Plan, and the supporting agency to the lead federal agency for specific events under the provisions of the current *U.S. Government Interagency Domestic Terrorism Concept of Operations Plan* and its projected replacement by the *Federal Incident Management Plan*.

The Coast Guard can be the supported or supporting commander for military operations conducted under 10 USC.

Coast Guard Strategic Objectives

Coast Guard Maritime Homeland Security Strategic Objectives are to:

- Prevent terrorist attacks within and terrorist exploitation of the U.S. Maritime Domain.
- Reduce America's vulnerability to terrorism within the U.S. Maritime Domain.

- Protect U.S. population centers, critical infrastructure, maritime borders, ports, coastal approaches and the boundaries and seams between them.
- Protect the U.S. Maritime Transportation System while preserving the freedom of the Maritime Domain for legitimate purposes.
- Minimize the damage and recover from attacks that may occur within the U.S. Maritime Domain as either the lead federal agency or a supporting agency.

Coast Guard Reserve Support of Maritime Homeland Security

Maritime Homeland Security is a mission involving virtually all Coast Guard units.

Under Coast Guard Reserve integration, Reserve units were disestablished in the 1990s and virtually all of the Coast Guard's 8,000 Selected Reservists are assigned to Active Component units.

The principal exceptions are the six Port Security Units, or PSUs, which are Coast Guard units manned largely reservists. Of the 140 personnel assigned to a PSU, 135 are Reservists. PSUs are principally intended for Harbor Defense/Port Security overseas, but can be used for Maritime Homeland Security. Accordingly, PSU 305 (Ft. Eustis, VA) and PSU 311 (San Pedro, CA) performed short-term security duties in New York and Los Angeles harbors immediately following the 11 September attacks. PSU 313 (Tacoma, WA) provided long-term security for Navy assets in Puget Sound after 9/11.

New Capabilities with Reserve Support

Maritime Safety and Security Teams have been established to provide a fast response capability for Maritime Homeland Security, the Coast Guard commissioned its first four Maritime Safety and

Security Teams (MSSTs) in FY 2002 and plans two more in FY 2003. Modeled after PSUs, each MSST has 104 personnel, including 33 reservists. Additional MSSTs are planned for FY 2004.

In addition, the Coast Guard has assigned Sea Marshals, trained law enforcement personnel to board high-interest vessels in militarily or economically strategic ports to prevent potential acts of terrorism. Virtually all of the Coast Guard's Sea Marshals are reservists.

Coast Guard Reserve Recall Data:

Since 11 September 2001, a cumulative total of 5,425 Coast Guard Reservists have been recalled to active duty under 10 USC 12302. At the end of June, the number of reservists in recall status stood at 3,088. The peak occurred in April 2003, when 4,412 reservists were on active duty. Of that figure: 551 were assigned to expeditionary forces, including four PSUs deployed in support of Operation IRAQI FREEDOM; and 3,849 were assigned in CONUS, including 372 participating in Operation LIBERTY SHIELD and 3,477 supporting military out loads in U.S. ports.

SUMMARY

U.S. Army Reserve, using its specialized capabilities and core competencies, to include Chem/Bio, Medical, Hospital Services, Civil Affairs, Mortuary, Military Police, and Signal, is well positioned to assume a primary DoD (Title 10) response role.

U.S. Naval Reserve is well positioned to take on the Navy's future Homeland Security-Maritime (HLS-M) mission in support of the Coast Guard, the lead federal agency for HLS-M.

The Air Force Reserve is developing a CONOPS spelling out their support for HLS/MACA to include Reserve Air Lift, Reserve Tankers, Combat Air Patrol (CAP) support over major U.S. cities, as well as civil support MOAs between the AFR and local, state and federal agencies.

Marine Corps Reserve contribution to HLS is shaped by their expeditionary nature with a focus overseas. Plans being developed in support of HLS/MACA will provide USNORTHCOM with a service component (MARFORNORTH) to support its HLS mission. Marine Forces Reserve (MARFORRES) support ten FEMA regions and two continental U.S. Army Headquarters through the Marine Emergency Preparedness Liaison Officer (MEPLO) program.

U.S. Coast Guard Reserve is mostly assigned to active component units. Six Port Security Units (PSUs), largely Reservists, are principally intended for harbor defense/port security overseas, but have been used for Maritime HLS as well. Newly established Maritime Safety and Security Teams (MSSTs) have been established to provide a fast response capability focused on Maritime HLS.

APPENDIX A. TASK FORCE MEMBERSHIP

ROLES AND MISSIONS PANEL

Panel Co-Chairs	
Dr. Ted Gold	Institute for Defense Analyses
GEN William Hartzog, USA (Ret.)	Burdeshaw Associates, Inc.
Members	
Mr. Samuel Adcock	EADS, Inc.
Mr. Michael Bayer	Private Consultant
Mr. Denis Bovin	Bear, Stearns & Co. Inc. Investment Banking
Dr. Craig Fields	Private Consultant
Mr. Robert Fitton	Resource Consultants, Inc.
LTG William Hilsman, USA (Ret.)	Private Consultant
Dr. David McIntyre	ANSER Institute for Homeland Security
Dr. Bert Tussing	U.S. Army War College
Ms. Joan Woodard	Sandia National Laboratory
Government Advisors	
LTC Joe Charagua, USA	Army Reserve/OCAR
COL Bev Garrett, USA	HQ U.S. Army Pacific
LTC Charlotte Hallengren, USA	IDA

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. GLOSSARY OF ACRONYMS AND ABBREVIATIONS

AC	Active Component
ADCON	Administrative Control
AEF	Air and Space Expeditionary Force
AFR	Air Force Reserve
AFRC	Air Force Reserve Command
ANG	Air National Guard
ARNG	Army National Guard
ASD(HD)	Northern Command
ASD-NII	Assistant Secretary of Defense for Network & Information Integration
AT	Antiterrorism
AWACS	Airborne Warning And Control System (E-3A aircraft)
C2	Command and Control
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CAP	Combat Air Patrol
CBIRF	Chemical, Biological Incident Response Force
CBRNE	Chemical, Biological Radiological, Nuclear and Enhanced Conventional Weapons
CFFC	Commander Fleet Forces Command
CJCS	Chairman, Joint Chiefs of Staff
CONOPS	Concepts of Operations
CONUS	Continental United States
CONUSA	Commander, Continental U.S. Army
CONUSA	Continental U.S. Army
CRAF	Civil Reserve Air Fleet
CS	Combat Support
CSS	Combat Service Support
CST	Civil Support Team

DCO	Defense Coordinating Officer
DHS	Department of Homeland Security
DMOSQ	Duty Military Occupational Specialty Qualification
DoD	Department of Defense
DSB	Defense Science Board
EPLOS	Emergency Preparedness Liaison Officers
FBCB2	Force XXI Battle Command, Brigade and Battalion
FEMA	Federal Emergency Management Agency
FTS	Full-Time Support
FY	Fiscal Year
GDP	Gross Domestic Product
GIG-BE	Global Information Grid-Bandwidth Expansion
GWOT	Global War on Terrorism
HLS	Homeland Security
HLS-M	Homeland Security – Maritime
HLS-MACA	Homeland Security/Military Assistance to Civil Authorities
HSPD-5	Homeland Security Presidential Directive
I MEF	I Marine Expeditionary Force
II MEF	II Marine Expeditionary Force
IP	Internet Protocol
IT	Information Technology
JCCSE	Joint CONUS Communications Support Element
JCS	Joint Chiefs of Staff
JDAL	Joint Duty Assignment List
JDAR	Joint Duty Assignment Reserve
JFCOM	Joint Forces Command
JFHQ	Joint Forces Headquarters
JFHQ-NCR	Joint Forces Headquarters/
JPME	Joint Professional Military Education
JRAD	Joint Reserve Augmentation Detachment
JROC/IPL	Joint Requirements Oversight Council
JTDS	Joint Table of Distributions

JTRS	Joint Tactical Radio System
JTTFS	Joint Terrorism Task Forces
LFA	Lead Federal Agencies
LMR	Land Mobile Radio
LSS	Littoral Surveillance System
MACA	Military Assistance to Civil Authorities
MARDEZ	Maritime Defense
MARFORNORTH	Marine Forces North
MARFORRES	Marine Forces Reserve
MEB	Marine Expeditionary Brigade
MEPLO	Marine Emergency Preparedness Liaison Officer
MOA	Memoranda of Agreement
MSCA	Military Support to Civil Authorities
MSSTS	Maritime Safety and Security Teams
NBC	Nuclear, Biological, Chemical
NCAPS	Naval Control and Protection of Shipping
NCW	Naval Coastal Warfare
NGB	National Guard Bureau
NIMS	National Incident Management System
NORTHCOM	Northern Command
NRP	National Response Plan
OCONUS	Outside Continental United States
OPCON	Operational Control
OSD	Office of Secretary of Defense
PSU	Port Security Units
QRFS	Quick Response Forces
RC	Reserve Component
REPLOS	Regional Emergency Preparedness Liaison Officers
SAFECOM	Safety Interoperable Communications
SECDEF	Secretary of Defense
SELRES	Selected Reserve
SRAAG	Senior Army Advisor Guard

STARC	State Area Command Headquarters
TACON	Tactical Control
U.S.	United States
USC	United States Code
USMC	United States Marine Corps
USN	United States Navy
WMD-CSTS	Weapons of Mass Destruction