HOMELAND SECURITY ADVISORY COUNCIL
WEAPONS OF MASS EFFECT TASK FORCE

ON

Preventing the Entry of Weapons of Mass Effect Into the United States

January 10, 2006

Table of Contents

EXECUTIVE SUMMARY

Throughout history societies have been threatened by enemies willing to attack civilian targets with weapons of catastrophic impact. As the weapons and the people who would use them have changed over time, defensive strategies and systems have evolved as well. A central tenet of Cold War strategy was to deter first use of nuclear weapons by the Soviet Union. The vast destructive potential of such weapons made a nuclear exchange totally unacceptable; every possible measure was taken to avoid nuclear war including massive investments in capabilities to detect weapon launch and assure retaliatory capability. With the demise of the Soviet Union, the nature of the threat has changed but the danger has not necessarily diminished. We still face the potential for hundreds of thousands of casualties and massive economic disruption from attacks on our homeland.

The United States is vulnerable to massive loss of life and economic devastation from the covert or terrorist delivery of a weapon of mass effect (WME).[1] This is an unacceptable condition. As an open society, the U.S. will never be able to construct impenetrable defenses to the entry of such weapons or the people who would use them. Attempts to "seal off" the borders to such entry have limits—physical limits in our ability to detect weapons or people entering the country and limits of acceptability since restrictions on the movement of cargo and people ultimately pose a risk to the flow of commerce and to personal freedom. Despite these limits, the country can and should be better protected from the threat posed by the entry of WME.

Charge to the Task Force

The Homeland Security Advisory Council, an independent advisory body offering advice, analysis and recommendations to the Secretary of Homeland Security, charged a Task Force composed of Council members, Senior Advisory Council members and government representatives with recommending specific steps the nation can take to prevent the entry into the country of weapons of mass effect and the people who would use them. Preventing the entry of the people who would use such weapons is of great importance in that WME and components of WME as defined in this study are found within the United States. Preventing the use of WME by individuals who may already be in the U.S. is not within the scope of the charge.

The Task Force decided that a systematic approach must guide its work and the recommendations it provides to the secretary. The Task Force met with experts from inside and outside of government at all levels to understand current plans, systems and practices in WME prevention and receive input on how to improve upon current capabilities. The Task Force developed a systems view of WME prevention, assessed the gap between the current fragmented system and a more unified approach, and made recommendations to close the gaps.

[1] Weapons of mass effect, or WME, are weapons capable of inflicting grave destructive, psychological and/or economic damage to the United States. These include chemical, biological, nuclear, radiological, or explosive weapons. While the Task Force recognizes the significant differences in the nature of these weapons, they share many common elements in terms of the requirements for preventing entry into the U.S. For the purposes of this study, cyber threats are not considered since cyber attacks can be launched from outside the country.

Findings

The Threat

An attack on our country by a WME is arguably the gravest danger to American national security. Different WME scenarios—use of nuclear, biological, chemical, radiological, or conventional weapons against U.S. targets—have different likelihoods and impacts, including civilian casualties in the hundreds of thousands. Regardless of the scenario, the consequences are almost unimaginable. Preventing WME use on U.S. soil must become our most urgent priority and the subject of focused and integrated effort. That it isn't today is a grave concern.

Determining the magnitude of resources that should be devoted to negating WME threats is greatly complicated by the fact that such threats (hopefully) have a very low probability of occurrence, at least at the present time, but have extremely significant consequences. In addition, the probability of attacks of the type discussed in this report is never likely to be reduced to zero. Nonetheless, the likelihood that a specific attack can be prevented is significantly enhanced if the country is willing to invest precious resources on WME prevention.

General Observations

WME prevention is a daunting management, technical, operational, and systems challenge and although significant progress has been made in recent years, much remains to be done. Authority, decision making, and operational control are distributed across individuals and organizations at multiple levels. The multiple participants involved in WME prevention share a common focus on security yet are diverse in mandates, memberships, capabilities, cultures, and motivations. This diversity is an advantage only if it is managed systematically; it is not today. The uncertainty over the threat and the wide range of potential threat scenarios compound the complexity.

Critical Deficiencies

The Task Force identified critical deficiencies in the current state of WME prevention: the absence of a systematic, risk-based approach to investment; dispersed capabilities, leadership and decision making; inadequate attention to engaging foreign partners; deterrence concepts in need of updating; need for greater urgency and priority for investments in technological innovation; and lack of citizen engagement.

Addressing Critical Deficiencies

Conceptual framework. To decrease the risk of a successful WME penetration of U.S. borders, the WME prevention system should be designed to address WME threats as close to the point of origin as possible. To achieve that objective, the U.S. should implement a WME prevention strategy and system which has the following three thrusts:

- Neutralize known terrorists
- Secure or eliminate sources of WME and/or critical components
- Detect and interdict WME in transit

The first thrust, neutralizing terrorists, is primarily a responsibility of the military and the intelligence community. The second thrust, securing or eliminating sources of WME, is also a joint responsibility of several government agencies, with the newly-established National Counterproliferation Center (NCPC) in a coordinating role.

This report focuses primarily on the third thrust, detecting and interdicting WME in transit, while recognizing that the first two are essential, interrelated, and ultimately preferable elements of a prevention strategy and that a systems view of the problem and

an integrated effort across all three thrusts is critical.

The Task Force found it useful to conceive of the WME prevention problem as consisting of three dimensions: 1) how WME materiel or people move across international borders toward a location in the United States—the geographical or spatial dimension; 2) what can be done along the path from source to target—the functional dimension; and 3) how the functions are carried out and by whom—the operational dimension.

Risk reduction and layered approach. Reducing or minimizing the risk of a WME entering the U.S. should be the central decision-making criterion for designing, developing, deploying, and operating a WME prevention system. Risk reduction analyses should be structured to address the fundamental choices available to the country in confronting the WME prevention challenge. With a broad systems view, fundamental questions can be asked and answered, such as:

- What should be the relative balance of investments for the three basic thrusts: neutralizing terrorists, securing potential WME sources, and detecting WME in transit?
- Are investments correctly balanced between air, land and sea corridors as a function of threat and risk?
- How should investments in alternative detection technologies be balanced in relation to the threat?
- What interfaces must exist between different entities with complementary functions?

Resource allocation decisions must be based on the greatest security impact rather than parochial interests.

Based on historical success in other complex systems, the Task Force believes that "layering" defensive capabilities would provide the necessary redundancy, flexibility, and robustness so that failure of any one element of the system is not catastrophic, and the protective effect of individual elements is cumulative or multiplicative. In the case of WME prevention, a "layer" is any combination of the above three dimensions that reduces the risk of entry of WME capability.

Management process. An integrated, system-wide WME prevention management process must be established as the basis for subsequent system design and implementation decisions. Through an architecturally-driven system definition, design, and management process, decision makers can perform risk assessments and determine the value of different components of a system by seeing their functions, costs and interactions in broader context rather than in isolation. Gaps in capability can be more readily identified along with alternative pathways for filling those gaps and reducing risk.

Recommendations

The Task Force generated many suggestions for improving WME defense. Recommendations were organized to address the major areas of concern with the current WME prevention system—authority, alignment and incentives, deterrence, risk and system management, and innovation. Specific supporting implementation actions are offered in each of these areas.

Leadership

Recommendations

Strengthen leadership structures. Clarify lines of authority and control by having the president designate the Secretary of Homeland Security as the lead individual responsible for preventing WME attacks in the

United States and strengthen his/her access to the information and assets needed to carry out this function. The secretary should immediately initiate a risk assessment and system management effort and adopt a model such as a Joint Program Office to coordinate the program elements and control the integrated WME prevention budget. Strengthen the White House Homeland Security Council (HSC) to make it comparable in authority and responsibility to the National Security Council (NSC).

Engage internationally. Better engage foreign governments and multilateral organizations with more individuals in the diplomatic corps responsible for WME prevention, and together focus more effort on developing a common understanding of the WME threat posed by terrorism, sharing best practices for preventing WME attacks, and developing the strategic cooperation necessary to deploy and manage a mutually reinforcing layered defense.

Require joint effort. Break down organizational barriers between the Department of Homeland Security (DHS) and other agencies by creating incentives and opportunities for career advancement based on such joint effort and cultivating a joint culture through more cross-training and transfer of personnel between different agencies involved in WME prevention.

Improve WME intelligence. The traditional customer set for WME intelligence does not fully accommodate the challenges posed by today's WME threat and the role played by DHS. Include DHS as a principal driver for WME intelligence collection and analysis.

Clarify the Department of Defense (DOD) role in disaster response. At the federal level, Northern Command, the Pentagon, and DHS should develop a cohesive strategy in consultation with state governors to respond to terrorist attacks or emergencies that exceed the states' resources. Governors and their respective homeland security advisors should plan more effectively for a wide range of contingencies that will inevitably require the unique capabilities of the military.

Supporting Actions

Improve interagency coordination. Develop policies, planning, and processes that support an integrated program budget and facilitate joint efforts across the federal government. Develop a government-wide system that rewards interagency cooperation and coordination focused on preventing the entry of WME. Institutionalize response organizations such as the Interagency Incident Management Groups to take on prevention functions during non-emergency periods.

Eliminate unnecessary bureaucratic redundancies. De-conflict overlapping or conflicting requirements placed on industry, such as multiple background checks and certifications for cross-border truckers, while retaining redundancies that are built into the layered defense system.

Create country or region-specific DHS portfolios. Provide each U.S. Mission/Embassy with clear-cut DHS strategic guidance. Leverage existing DHS resources currently assigned to U.S. Missions/Embassies abroad. Create dedicated DHS foreign service attaché positions.

Selectively engage multilateral organizations on homeland security-related issues. Use strategic partnerships as force multipliers and a means to extend reach into regions that are breeding grounds for terrorism.

Institutionalize DHS participation in NATO through a "reinforced North Atlantic Council (NAC.)" Through NAC pursue common objectives, share best practices, and develop joint competencies.

Participate in joint contact/working groups. Work bilaterally on WME prevention programs.

DHS leadership should actively task WME intelligence analysis. WME intelligence has traditionally been applied to supporting demarches about treaty violations and sanctions. Today, the Weapons of Mass Destruction (WMD) intelligence consumer should be defined by a broader constellation of authorities, to include DHS, Health and Human Services, and the Federal Bureau of Investigation (FBI). Preventing WME attacks on the homeland requires a forthright role for DHS in the consumption of intelligence analysis.

Deterrence

Recommendations

Make deterrence policy clear. The president should announce, and the national leadership should reiterate, a policy of swift, certain, and severe consequences for any nation associated with a terrorist act using WME.

Expand deterrence into the WME context. Beyond retaliation, which registers little with a committed terrorist group, the layered defense system increases uncertainty and therefore the *likelihood of failure* for potential attackers thus diminishing the attractiveness of WME use in the view of a potential perpetrator desiring massive effect. When coupled with resilience in managing the aftermath of an attack, this enhanced defensive posture should be a component of expanded deterrence.

Engage citizens. Bridge the preparedness gap between an overextended National Guard and the crisis management needs of the federal and state level leadership by engaging citizen volunteers. Proposals such as the non-expeditionary Home Guard, operating under gubernatorial control, and other volunteer-based measures can provide Americans with a way to contribute to national preparedness and demonstrate national resilience by assisting law enforcement and other officials with support such as traffic control and delivery of food and water during a crisis.

Supporting Actions

Create uncertainty for potential attackers. Complicate their plans and force them into modes of operation that are more susceptible to detection and interdiction.

Understand and prevent radicalization. Target root causes of international terrorism.

Build in adaptive capability. Use constant change in defensive posture to increase uncertainty for would be attackers and to counter changes in their tactics.

Adapt or update existing models for marshalling citizenry. The Civil Air Patrol, the Coast Guard Auxiliary, and the National Defense Executive Reserve should be adapted and serve as models for a "Home Guard" with specialized skills such as quarantine implementation, vaccine administration, and crisis communications.

Risk and System Management

Recommendations

Institute a risk-based process for resource allocation. An open transparent process for targeting prevention funding should be instituted. To ensure that investments deal with the greatest needs from a national as well as

a local perspective, consider establishing an independent body, comparable to the Base Realignment and Closure Commission (BRAC) as a check and balance to review integrated WME prevention budget allocations and provide insulation from political liabilities.

Improve private sector contributions to the process for risk management. Outside experts can help design and evaluate the approach to managing risk. Public-private partnerships remain a valuable vehicle for this involvement, but require different approaches for the demands of developing and managing a layered prevention strategy.

Initiate a system management effort. The Secretary of Homeland Security should adopt one of several architecturally-based models of integrated systems management to help guide and oversee the planning, development, and integration of the national WME prevention system.

Supporting Actions

Help industry make the business case for security and determine if/when government should provide assistance. The federal government should assist the private sector in making the business case for security by, for example, developing cost benefit analysis models, creating market-based incentives for security investments, and clarifying the dividing line between government and private sector responsibilities.

Study the security risks posed by U.S. companies operating globally and outsourcing to foreigners. Security experts throughout the private sector are concerned that, due to increased overseas operations, outsourcing and supply chains, increasing numbers of people from foreign countries now have access to substantial information about U.S. companies and their business models.

Establish joint government/industry working groups. Pattern the groups after the existing National Security Telecommunications Advisory Committee to promote coordinated government/private sector counterterrorism efforts.

Promote Standards for Products Useful in the Anti-terrorism Campaign. Through national standards, create the potential for a large enough market to warrant industry investment.

Provide Selective Indemnification. Indemnify firms that are seeking to assist in the war on terrorism with indemnification against adverse consequences which they could not reasonably be expected to have foreseen.

Create a system management board. Since WME prevention spans multiple organizations, the Board should include representatives of component elements of the WME prevention system and should meet periodically with the WME System Manager. The Board should be the forum for stakeholder agencies to participate in risk assessments and decision making on aspects of the WME prevention system.

Appoint a WME system manager. Have him/her report directly to the secretary and have authority to manage investments in system capabilities.

Publish a DHS directive on WME prevention system management. Specify the roles, authorities, and organizational relationships in the system management process, including the DHS role as lead, the system approval processes, national and international relationships, and the role of the system management board.

Innovation

Recommendations

Make detection a priority for innovation. The secretary, the HSC, and the president should make it among the highest national priorities to bring together elements of the research community to undertake transformational research.

Encourage and nurture new ideas. Create a process that encourages new ideas from people within and external to the department by encouraging out of the box ideas from all levels across the homeland security and related communities and providing a clear path for those ideas to gain visibility, be tested, and ultimately be acted upon by decision makers.

Supporting Actions

The Domestic Nuclear Detection Office (DNDO) model should apply to other WME threats such as biological, radiological, and chemical agents and explosives. Rapid progress can be made by marshaling relevant assets across the executive branch to focus efforts on research, development, testing, and evaluation of transformational detection capabilities and strategies. Wherever possible, technologies should be developed that have dual use benefits (e.g., detecting drug contraband as well as WME).

Develop and apply performance metrics to guide organizational behavior toward long-term goals. When necessary, officials outside of the organization that will be assessed should set performance metrics.

Systematically institute frank and candid "after action reports." Management must value frank and constructive criticism by and of all parties (supervisors and subordinates) by incorporating input into planning and practice and ensuring there is no retribution for candid contributions.

Make "Red Teaming," the process of gaming an adversary's actions, a more integral part of training and routine operations. Purposefully testing a system, people, and equipment to probe for weaknesses can improve their security by mimicking the techniques the adversary would use to carry out an attack. When done at the system (rather than component) level, management can identify system improvements.

Create a long-range review process akin to the DOD's "Quadrennial Defense Review" that takes into account strategy, research and development, budgeting, and other factors. Investments in infrastructure, science, and technology require long-range planning. Management and operators must systematically feed requirements into the research and system development process and provide continuous updates. Such a tool would need to go beyond DHS and include all relevant agencies to be effective.

I. INTRODUCTION

Purpose

As an independent advisory body, the Homeland Security Advisory Council (HSAC) exists to provide advice, analysis, and recommendations to the Secretary of Homeland Security to support the creation and implementation of actionable policy. The HSAC charged this Task Force to provide a framework and associated recommendations to prevent the introduction of Weapons of Mass Effect (WME) and/or persons who would use them from reaching U.S. soil. For the purpose of this discussion, the Task Force defined WME as weapons capable of inflicting grave destructive, psychological, and/or economic damage on our nation. These include chemical, biological, nuclear, radiological, or explosive weapons. While the Task Force recognizes the significant differences in the nature of these weapons, they share many common elements in terms of the requirements for preventing entry into the U.S. For the purposes of this study, cyber threats are not considered since cyber attacks can be launched from outside the country.

Scope and Approach

The challenge in WME defense is to reduce the risk of WME entry, while minimizing impacts on legitimate commerce and passenger traffic. The Task Force focused on the introduction of weapons, weapon components, and persons into the country. Related issues of preventing attacks carried out by persons *already* in the United States were of concern but beyond the scope of this effort.

Several other considerations impinged on the scope of this study:

Defining the Border

The Task Force assumed that the U.S. border was the last line of defense. However, the term "border" should include the physical border, institutional borders such as the Air Defense Identification Zones (ADIZ), or other potential inspection locations such as international airports.

Non-proliferation

Non-proliferation and the securing of existing weapons, although perhaps the best WME defense, are not addressed in detail in this report since there are already several well-studied programs, including those undertaken by the newly-established National Counterproliferation Center (NCPC) and other agencies. The Task Force stresses the importance of aggressively pursuing the very basic nonproliferation goals of securing known sources of nuclear weapons and other WME materiel with significantly greater financial and political investments.

Minimizing the Consequence of a WME Attack

Should prevention systems fail, the consequences of a WME attack can be limited. The response to Hurricane Katrina demonstrated how far we must go to have the capabilities and the leadership to mitigate the impact of even foreseen natural disasters. Reducing the ultimate effect of a WME attack reduces the attractiveness of WME to an adversary. Reducing the impact of a WME attack is addressed only briefly in this study as it is, in part, the subject of another HSAC Task Force on critical infrastructure resilience.

While the scope of the Task Force's work was limited as described above, the development of a WME prevention system must

be broadly scoped to take into account all aspects of the problem.

Members of the Task Force met on 12 occasions between March and October of 2005 and received input from a diverse group of experts from within and outside government including presentations on the activities of multiple agencies at all levels of U.S. government, American allies, and the private sector given by officials and subject matter experts from the strategic, tactical, and operational levels. The Task Force gathered information on current systems, plans, and practices in WME prevention and current understanding of the threat. The elements of a systems approach to WME prevention were identified. Requirements to reach a more unified, systematic approach to WME prevention were defined and the Task Force developed recommendations on evolving national capability toward this goal.

Organized functionally into three interconnected subgroups, the Task Force examined major WME threats, vulnerabilities, and cross-cutting factors from the perspectives of the major corridors of WME entry: air, land, and sea. An HSAC or Senior Advisory Council member chaired each subgroup with a senior government representative serving as a senior subject matter expert. Task Force Chair, Dr. Lydia Thomas, President and Chief Executive Officer of Mitretek Systems and Co-Chair of the National Academies Government-University-Research Roundtable and Dr. Jared Cohon, Vice Chair, President of Carnegie Mellon University, presided. The following served as Subgroup Chairs.

Air Domain Subgroup
Chair. Mr. Norman Augustine, Member of the President's Council of Advisors on Science & Technology; former Chairman of the Executive Committee, Lockheed Martin Corporation.

Supporting official (prior to his departure from the Transportation Security Administration (TSA)). Rear Admiral David M. Stone, USN (Ret.), Assistant Secretary, TSA, Department of Homeland Security (DHS).

Land Domain Subgroup
Chair. Dr. James Schlesinger, Chairman, Board of Trustees, The MITRE Corporation; former Secretary of Energy, Assistant to the President, Secretary of Defense, and Director of Central Intelligence.

Supporting official (prior to his departure from Customs and Border Protection). Mr. Robert Bonner, Customs Commissioner, DHS

Sea Domain Subgroup
Chair. Dr. David Abshire, President, Center for the Study of the Presidency and President of the Richard Lounsbery Foundation; former Ambassador to NATO, Counselor to the President, and co-founder and CEO of the Center for Strategic and International Studies.

Supporting official. Vice Admiral Terry Cross, Vice Commandant, United States Coast Guard, DHS.

Primary federal participants included the HSAC Executive Director, Daniel Ostergaard, and two Task Force Directors, Kathryn Knapp and Richard Davis. Benjamin Gray served as an Associate Director.

II. CURRENT STATE

The Threat

An attack on our country by a WME is arguably the gravest danger to American national security. Different WME scenarios—use of nuclear, biological, chemical, radiological, or conventional weapons against U.S. targets—have different likelihoods and impacts, including civilian casualties in the hundreds of thousands. Regardless of the scenario, the consequences are almost unimaginable. Preventing WME use on U.S. soil must become our most urgent priority and the subject of focused and integrated effort. That it isn't today is a grave concern.

In terms of consequences, if not likelihood, nuclear weapons comprise the greatest threat against America by a terrorist organization. An explosion of even a low yield device in a large city such as many of those found on both coasts and in the Gulf region would immediately kill hundreds of thousands of people, followed by a comparable number of deaths as well as economic and psychological impacts in the lingering aftermath.

Constructing a weapon from nuclear material would be a very difficult undertaking for a terrorist group, suggesting that it is much more likely that such a group would attempt to buy, steal or be given an existing weapon. Potential sources include the stockpiles of the former Soviet Union, states hostile to the U.S., such as North Korea and Iran, that currently possess nuclear devices, and declared nuclear states, such as Pakistan, that could lose control of their nuclear arsenal in a political crisis.

A variety of means of introducing such weaponry into the U.S. is available, including penetrating from the sea, from the air, and over land. So, despite the technical difficulty, the threat of terrorist use of nuclear weapons is real, as are threats posed by biological, chemical, and other WMEs.

Determining the magnitude of resources that should be devoted to negating WME threats is greatly complicated by the fact that such threats (hopefully) have a very low probability of occurrence, at least at the present time, but have extremely significant consequences. In addition, the probability of attacks of the type discussed in this report is never likely to be reduced to zero. Nonetheless, the likelihood that a specific attack can be prevented is significantly enhanced if the country is willing to invest precious resources on WME prevention.

Preventing an attack with WME should be the highest priority and should receive the maximum attention from the president, the secretary, and the Congress, as well as from within the department. The recommendations offered in this report are a first step toward what must be a sustained national effort.

General Observations on WME Prevention

The Task Force is resolved that concerns with the current state of WME prevention should be a priority for the nation and must be addressed.

The country has multiple, independently developed systems that constitute the *de facto* national defense against entry of WME. (In this context and throughout this report, the term "system" includes people, organizations, processes, and technologies that are applied together to achieve a common objective.)

Many WME prevention systems seek to detect and interdict the illicit entry of people and materiel of concern. These systems selectively focus on borders, ports of entry, and modes of transport to varying degrees. In many cases, there are multiple systems managed by different organizations to tackle a single problem. Preventing entry of WME through seaports for example is a focus of several programs, including the Container Security Initiative, operated by DHS, and the Megaports Initiative, which is a Department of Energy program.

The WME prevention mission is not limited to detection and interdiction. It is wide ranging and includes organizations and programs in intelligence, threat analysis, research and development, technology acquisition, test and evaluation, diplomacy, minimizing consequences, managing recovery, and other functions. The organizations involved span the federal, state and local levels of government, foreign governments and international organizations, research institutions, and private industry. In some agencies, dedicated internal units are responsible for functions such as intelligence and threat analysis. In other cases those capabilities are a shared function across agency lines. Some functions are duplicated in multiple locations without a rationale other than their legacy presence. For example, explosives security groups in DHS can be found under the Immigration and Customs Enforcement Federal Air Marshal Service, the Science and Technology Directorate, the Office of Infrastructure Protection, the Office of Domestic Preparedness, and the TSA. Similar duplications are evident in other federal agencies.

WME prevention is a daunting management, technical, operational, and systems challenge. Authority, decision making and operational control are distributed across participants at multiple levels. The multiple participants involved in WME prevention share a common focus on security yet are diverse in mandates, memberships, capabilities, cultures, and motivations. This diversity is an advantage only if it is managed systematically. The uncertainty over the threat and the wide range of potential threat scenarios compound the complexity.

In the *National Strategy for Homeland Security (March 2002)*, the Office of Homeland Security provided a vision to mobilize and organize the U.S. to secure the homeland from terrorist attacks. The strategy acknowledges that this is an exceedingly complex mission that requires coordinated and focused effort from our entire society—the federal, state, local and tribal governments, the private sector, and the American people. This requirement for coordination and focus has not been reached with regard to U.S. efforts in WME prevention. This Task Force also acknowledges the need to work collaboratively with foreign governments and multinational institutions as well.

Vulnerabilities attributable to deficiencies in the current state of WME prevention are real and must be addressed. It is essential that the distinct entities in WME prevention operate in a unified manner and that resources be allocated based on relative contribution to risk reduction rather than parochial or legacy entitlements. Moving to a more effective WME prevention system requires more than overhauling strategy. Key investments in infrastructure, technology, and long-range human resources must match the challenge at hand. Congress and the Administration must pursue legislative and policy solutions that provide consistent support for these objectives.

The Task Force focused its efforts on how to achieve a unified system with risk-based management.

Critical Deficiencies

The WME threat focuses directly on weaknesses—vulnerabilities and gaps in our defense—not strengths. It adapts and evolves. To combat this threat our critical deficiencies must be assessed and receive immediate attention from national homeland security leadership. The Task Force explored the root causes of such weaknesses in the current WME prevention system. Critical deficiencies in the current state of WME prevention include the following:

- There is no systematic, risk-based approach to a national investment strategy for WME and no unified set of policies, procedures, people, and technology.
- Critical WME prevention capabilities and decision making about deploying those capabilities are dispersed within DHS and across the executive branch without a coherent strategy to leveraging them in prevention efforts. As a result, it is not clear who is in charge of decision making for developing, deploying, and managing a WME prevention strategy.
- The WME threat is global in scale which requires that DHS engage foreign countries and gain their cooperation. The Department and the Executive Branch are not appropriately organized and resourced to accomplish this task.
- Today's concepts of deterrence are too reminiscent of the Cold War era and must be updated.
- The government is not investing with sufficient urgency and priority in technological innovation that could lead to breakthrough advances in WME prevention.
- The nation's armed services, National Guard, and Reserve have served repeat tours fighting terrorism in Iraq and Afghanistan but American citizens have not been engaged at a level that allows them to share in the responsibility to secure the homeland.

With these general and specific concerns in mind, the Task Force developed a systems view to help improve WME prevention, assessed the gap between the current fragmented WME prevention system and a more unified system, and offered specific recommendations to close the gap.

III. ADDRESSING THE CRITICAL DEFICIENCIES

Conceptual Framework

To decrease the risk of a successful WME penetration of U.S. borders, the WME prevention system should be designed to address WME threats as close to the point of origin as possible. To achieve that objective, the U.S. should implement a WME prevention strategy and system which has the following three thrusts:

- Neutralize known terrorists
- Secure or eliminate sources of WME and/or critical components
- Detect and interdict WME in transit

Screening at foreign ports of origin (e.g., through the Container Security Initiative) is an example of extending defenses closer to the point of origin within a corridor of entry. However, other defenses can be extended to the more easily manipulated stages of the supply chain that occur prior to arrival at the seaport, such as during the phase when shipping containers are packed and sealed.

The first thrust, neutralizing terrorists, is primarily a responsibility of the military and the intelligence community. The second thrust, securing or eliminating sources of WME, is also a joint responsibility of several government agencies, with the newly-established NCPC in a coordinating role. Detecting and interdicting WME in transit is similarly a joint effort of multiple entities. The Task Force believes that DHS should have the lead responsibility to coordinate this aspect of the WME prevention system.

This report focuses primarily on the third thrust, detecting and interdicting WME in transit, while recognizing that the first two are essential, interrelated and ultimately preferable elements of a prevention strategy, and that a systems view of the problem and an integrated effort across all three thrusts is critical.

WME prevention is a complicated problem, with many interrelated elements and many participating agencies, at all levels of government and including foreign governments and private sector entities. The challenge is to coordinate and integrate WME prevention policies, operations, systems development, research, and funding. The Task Force found it useful to conceive of the problem of preventing WME entry into the United States as consisting of three dimensions: 1) how WME materiel or people move across international borders toward a location in the United States—the geographical or spatial dimension; 2) what can be done along the path from source to target—the functional dimension; and 3) how the functions are carried out and by whom—the operational dimension.

For the spatial dimension, depicted in Figure 1, there are three stages of threat—origin and movement within a foreign country and across international borders, international transit, and entry to the United States and movement to target. Movement can occur through different combinations of three corridors of entry: land, sea, and air, as illustrated by the example path depicted in Figure 1.

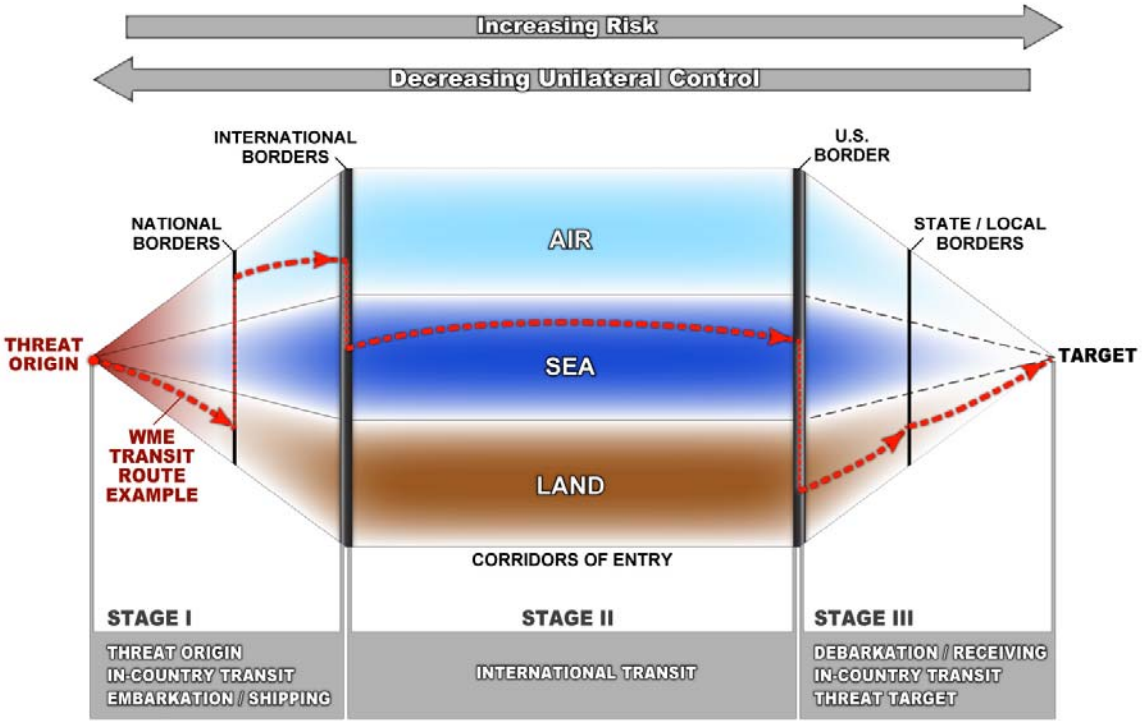

Figure 1. The spatial dimension of a WME defense system

Therefore, the system must operate flexibly at all points across the different corridors of entry and modes of transport. At each transition point—crossing borders and changing transportation modes—there is a greater opportunity to interrupt the movement of persons or WME components.

Along the path from origin to target, the functional dimension includes the following:

Dissuasion
The effort to de-legitimize violent extremism, radicalization, and terrorist strategies and practices on a moral, cultural, and social basis.

Deterrence
The ability to convince the enemy that an attack will fail, that perpetrators will be captured and prosecuted, and that nations associated with an attack will incur severe consequences.

Detection
Identifying the presence of potential perpetrators and/or materiel prior to an attack.

Denial
Preventing access to source materials, knowledge, expertise, a consequence-rich target environment, and/or potential recruits.

Disruption
Creating sufficient confusion or uncertainty on the part of perpetrators to reduce their ability to succeed and increase their risk of detection and interdiction.

Interdiction
Capturing elements of the threat—people and/or materiel—before they reach their intended target.

Elimination
Permanent eradication of the threat.

Success in some combination of these functions contributes to the overall objective of preventing WME from entering the U.S.

Finally, for each of the above functions, there is the operational dimension—how the above functions are carried out and by whom. This third dimension of WME prevention should include combinations of the following elements:

Institutional Elements
Institutions play a role in regulating the movement of people and materiel. These institutions include both governmental and private sector entities.

Tools
Institutions have various tools at their disposal to undertake their respective responsibilities. These tools can be categorized as follows:

Transactional. Transactional tools are processes that intersect with the human and the materiel components of a WME threat. Processes associated with purchasing, shipping, travel, customs, immigration, and other activities are all potential transactional tools.

Informational. Informational tools can be applied at the earliest stages of intelligence collection and analysis of a threat, or to guide operations in real time. Watch lists and command center situational displays are examples of informational tools.

Technological. Detecting people and materiel of concern, for example, is dependent, in part on identity management systems and sensors. These tools include non-invasive detection systems (e.g., x-rays, radiation and explosives detectors, and magnetometers), as well as "active interrogation" techniques to help identify the presence of shielded nuclear material. Such tools also complement biometric identification systems and data mining systems.

Strategies, policies, programs, and resource allocation decisions should be evaluated based on how they contribute to minimizing the risk of WME capability entering the country. The remaining challenge is to institute a mechanism for setting priorities, determining what capabilities will be implemented, and then allocating resources targeted toward those ends.

Moving from a Framework to Solutions: A Risk Reduction Approach

Reducing or minimizing the risk of a WME entering the U.S. (risk reduction) should be the central decision-making criterion for designing, developing, deploying, and operating a WME prevention system. The Task Force recognized however that while a sharp focus on risk reduction is essential, there are other considerations that can and should enter into decision-making. These include cost, economic impacts, ancillary or secondary benefits (e.g., reduction of drug and other forms of smuggling), availability of technology, international relations, and contingency for unpredictable threats such as natural disasters.

Risk reduction analyses should be structured to address the fundamental choices available to the country in confronting the WME prevention challenge. Each option, representing different combinations of policies, organizations, technologies, or processes, should be assessed in terms of its benefits in relation to its costs. Ultimately, the benefit in terms of risk reduction is the most important measure of value.

Decision makers can determine the value of different options, make trade-offs, achieve balance in overall capability when they can see the overall WME prevention system in broader context rather than the pieces of it in isolation. With a broad systems view, fundamental questions can be asked and answered, such as:

- What should be the relative balance of investments for the three basic thrusts: neutralizing terrorists, securing potential WME sources, and detecting WME in transit?
- Are investments correctly balanced between air, land and sea corridors as a function of threat and risk?
- How should investments in alternative detection technologies be balanced in relation to the threat?
- How much of the investment portfolio should go to longer range technology development versus shorter range improvements?
- What combination of approaches should be used for WME detection in non-U.S. controlled areas?
- What functions should be assigned to specific government entities?
- What interfaces must exist between different entities with complementary functions?

Although the scope of this study is limited, it is essential that a systems view be adopted by decision makers that embraces all aspects of the problem.

A risk-based approach tends to be controversial since by definition some organizations or programs will "score low" and receive less funding than they would otherwise receive under a different scheme (e.g., per capita funding, or equal share distribution). This is an expected outcome of a risk-based approach and should be viewed as a net benefit for the nation rather than a negative attribute.

The resource allocation process should minimize parochial and political influences by incorporating a mechanism for placing the national interest above parochial interests. What is needed is a single, integrated WME prevention budget which captures all funds approved for that mission. Further, the creation of that budget should be a result of the risk-based analytical approach discussed above with a mechanism similar to that used in base closure as a check and balance.

Such a mechanism for independently reviewing resource allocation decisions might be similar to the selection process in base closure. The Base Realignment and Closure Commission (BRAC) recommends which American military bases should be closed after receiving input from the Department of Defense and the affected bases and communities. Because closing military bases has proven to be politically difficult if not impossible, the BRAC process assumes political liability while preserving legitimacy by operating independently and submitting recommendations through the President to Congress for an up or down vote on the complete recommendation. This model applies to the politically difficult challenge of risk-based investment, particularly when the investments are needed to shore up weaknesses rather than reinforce strengths.

A risk-based approach identifies strengths in order to avoid reinforcing them at the expense of known or emerging weaknesses. Investments informed by this approach seek to "buy down" risk by closing gaps in our defenses that terrorists would seek to exploit. Doing so requires

knowledge of the enemy—their motivations, capabilities, doctrine, tradecraft, practices, movements, targets and identities—knowledge of our vulnerabilities, and an ability to manage consequences. This in turn places a premium on focused intelligence—dynamic, all-source information processed through an analysis structure that produces focused, timely, predictive, and actionable products. A risk-based approach also values a strategy for reducing vulnerabilities by hardening targets and diminishing consequences by increasing resilience.

Such an undertaking should be started immediately. It is not new or novel to the U.S. as discussed below.

Layered Approach

The nation has a long history of developing and deploying unprecedented systems to address complex, variable and evolving threats. These systems have been successfully applied in both the civilian and military sectors. Examples include the following:

- Conventional warfare
- Air defense
- Strategic nuclear defense
- Crisis management
- Nuclear power safety
- Controlling infectious diseases
- Preventing entry of foreign animal diseases
- Drug interdiction

Given the nature of the WME threat, the Task Force believes that "layering" our defensive capabilities is an essential characteristic of the architecture and would provide the necessary redundancy, flexibility, and robustness so that failure of any one element of the system is not catastrophic, and the protective effect of individual elements is cumulative or multiplicative. In the case of WME prevention, a "layer" is any combination of the three dimensions—geographical/spatial, functional, and operational—described above.

In the above context a "layer" is a conceptual designation that nonetheless yields tangible results. A layer adds value when: 1) a combination of prevention-related capabilities are deployed together at some stage of the progression of the threat from attack planning to entry into the country, and 2) that combination of capabilities acts as a barrier reducing the risk of entry of a WME.

In a nuclear power plant, for example, the layers include geographical/spatial dimensions to include the facility security with perimeters and barriers; functional dimensions, including identity-based access controls to protect the reactor, control room and other location; and operational dimensions such as the redundant engineering of reactor control mechanisms and other safety systems, and the screening and training of operators and maintenance staff.

The challenge in WME defense is similar in some respects. Rather than protecting a single fixed asset from a known threat, WME defense protects multiple assets and populations nationwide from multiple, changing threats. Layers help counter uncertainty over the exact nature of the risks (targets, weapons, and modes of attack) and exactly how and when the protective system will be challenged.

Example: The passport control process should be thought of as one layer. It is deployed at several points prior to the border and seeks to interdict or disrupt unauthorized entry. The process incorporates several of the above tools—

institutional (involving joint effort of various national border control authorities), transactional, informational and technological (use of biometrics and networked databases to match identities to watch lists).

The question becomes what set of choices in the layered model provides the greatest risk reduction at a reasonable cost.

Management Process

A structured risk analysis process, as outlined above, will define the fundamental policy direction and operational and technological components that represent the optimum blend of WME prevention mechanisms. An integrated, system-wide WME prevention management process must be established as the basis for subsequent system design and implementation decisions. These include decisions on budget priorities, tradeoffs between competing requirements, and integration of disparate capabilities. Instituting a risk management and layered approach in the absence of an overarching management process will only yield incremental improvements at best. An effective WME prevention system will not emerge from isolated, incremental efforts.

Through an architecturally-driven system definition, design, and management process, decision makers can perform risk assessments and determine the value of different components of a system by seeing their functions, costs and interactions in broader context rather than in isolation. Gaps in capability can be more readily identified along with alternative pathways for filling those gaps and reducing risk. WME prevention, as with homeland security generally, is a highly federated challenge bringing together multiple participants across agencies of government, international bodies, and the private sector, with differing cultures, technologies, missions, and processes. These entities must act together in a unified and coordinated fashion with an integrated government budgeting and management process that supports such unity of effort. Finally, the value of a program management process is lost without a program manager; one with the authority and influence to drive change across the WME prevention system.

Many of the layered defense systems mentioned above—air defense, strategic nuclear defense, crisis management—were successful to some degree because the complex planning, development and implementation was guided by a system architecture process. Such architecturally-based management models should be considered for WME prevention, a challenge of comparable if not greater scope and complexity.

IV. PATH FORWARD: DEVELOPING, DEPLOYING, AND MANAGING A LAYERED DEFENSE SYSTEM

In its current state, WME prevention is critically flawed and must be improved. The various elements of WME prevention do not work together as an integrated system to achieve the strategic functions of WME defense. Resources are not systematically allocated based on their contribution to risk reduction and there is a lack of sufficient urgency and priority to technology innovation.

Improvement is urgently needed given the catastrophic potential of a WME attack. Considering the deficiencies in current WME defenses and the features of a risk-based and layered WME prevention system, the Task Force identified four areas for improvement.

- Authority, alignment, and incentives
- Deterrence
- Risk and system management
- Innovation

The Task Force developed recommendations to move toward the goal of a risk-based, layered defense system for preventing entry of WME into the country. The majority of recommendations can be acted upon within the secretary's purview; others require Congressional and/or presidential action. Specific supporting implementation actions are summarized below and presented with additional detail in Appendix A.

Authority, Alignment, and Incentives

A layered defense system depends on the joint effort of multiple participants domestically and internationally, spanning all levels of government and working across lines between the public and private sectors. This effort goes beyond coordinating individual agency plans to the joint execution of commonly held strategies.

Strengthen Leadership Structures

Clarify lines of authority and control by having the president designate the Secretary of Homeland Security as the lead individual responsible for preventing WME attacks in the United States and strengthen his/her access to the information and assets needed to carry out this function. The secretary should immediately initiate a risk assessment and system management effort and adopt a model such as a Joint Program Office to coordinate the program elements and control the integrated WME prevention budget. Without becoming overly involved in the operational dimensions of homeland security policy, a strong HSC is important for coordinating policy, helping to implement resource allocation decisions, and getting agencies to work together. The president should give the HSC Director the authority and influence to build the HSC into a counterpart and complement to the NSC as it was envisioned in the Homeland Security Act of 2002. If the HSC is not strengthened as recommended it should be merged with the NSC.

Engage Internationally

Better engage foreign governments and multilateral organizations to develop a common understanding of the WME threat, to share best practices for preventing WME attacks, and to develop the strategic cooperation necessary to deploy and manage a mutually reinforcing layered defense. U.S. homeland security objectives increasingly require the cooperation of foreign governments, especially in pursuit of a layered approach to

preventing WME attacks. Doing so requires new bureaucratic capacity at DHS and more individuals in the diplomatic corps dedicated solely to homeland security and WME prevention (rather than as an added responsibility). The United States should selectively engage foreign governments and multinational organizations on WME prevention through creative use of multilateral entities such as NATO, the European Union, and the Association of Southeast Asian Nations.

Require Joint Effort
Break down organizational barriers between DHS and other agencies by creating incentives and opportunities for career advancement based on such joint effort and cultivating a joint culture through more cross-training and transfer of personnel between different agencies involved in WME prevention.

Improve WME Intelligence
The traditional customer set for WME intelligence does not fully accommodate the challenges posed by today's WME threat and the role played by DHS. Include DHS as a principal driver for WME intelligence collection and analysis.

Clarify the Department of Defense (DOD) Role in Disaster Response
At the federal level, Northern Command, the Pentagon, and DHS should develop a cohesive strategy in consultation with state governors to respond to terrorist attacks or emergencies that exceed the states' resources. Governors and their respective homeland security advisors should plan more effectively for a wide range of contingencies that will inevitably require the unique capabilities of the military.

Supporting Actions

Improve Interagency Coordination
Develop policies, planning, and processes that support the integrated program budget and facilitate joint effort across the federal government. Develop a government-wide system that rewards interagency cooperation and coordination focused on preventing the entry of WME. Institutionalize response organizations such as the Interagency Incident Management Groups to take on prevention functions during non-emergency periods.

Eliminate Unnecessary Bureaucratic Redundancies
De-conflict overlapping or conflicting requirements placed on industry, such as multiple background checks and certifications for cross-border truckers, while retaining redundancies that are built into the layered defense system.

Create Country or Region-specific DHS Portfolios
Provide each U.S. Mission/Embassy with clear-cut DHS strategic guidance. Leverage existing DHS resources currently assigned to U.S. Missions/Embassies abroad. Create dedicated DHS foreign service attaché positions.

Selectively Engage Multilateral Organizations on Homeland Security-related Issues
Use strategic partnerships as force multipliers and a means to extend reach into regions that are breeding grounds for terrorism.

Institutionalize DHS Participation in NATO through a "Reinforced North Atlantic Council (NAC)"
Through NAC pursue common objectives, share best practices and develop joint competencies.

Participate in Joint Contact/Working Groups
Work bilaterally on WME prevention programs.

DHS Leadership Should Actively Task WME Intelligence Analysis
WME intelligence has traditionally been applied to supporting demarches about treaty violations and sanctions. Today, the weapons of mass destruction (WMD) intelligence consumer should be defined by a broader constellation of authorities, to include the Departments of Homeland Security, Health and Human Services, and the FBI. Preventing WME attacks on the homeland requires a forthright role for DHS in the consumption of the analysis produced by the National Intelligence Directorate, including specifically the National Counterproliferation Center and the National Counterintelligence Center. However, doing so entails DHS leadership actively tasking these and other intelligence community organizations with fulfilling analysis requirements about the WME/WMD threat. For example, the Department's Domestic Nuclear Detection Office (DNDO) is responsible for creating a deployment strategy, or "global architecture," to operate across all layers in defending against smuggled nuclear weapons and material. To do so, the DNDO must consider intelligence about the trajectory of the current nuclear threat, including potential perpetrators, means of delivery, and likely sources of illicit nuclear material. All of this informs the ultimate characteristics of a global deployment strategy, and none of this information comes from just one source.

Deterrence

The best way to prevent WME from entering the country is to deter its use in the first place. As it was in the Cold War, deterrence and strategic alliances should be strategic elements of the War on Terrorism and the WME prevention mission. The Task Force offers the following recommendations in this area:

Make Deterrence Policy Clear
The president should announce, and the national leadership should reiterate, a policy of swift, certain, and severe consequences for any nation associated with a terrorist act using WME.

Expand Deterrence Into the WME Context
Beyond the traditional emphasis on deterring adversaries through threat of overwhelming retaliation, which registers little with a committed terrorist group which may not be state sponsored, the layered defense system increases the *likelihood of failure* for potential attackers by introducing uncertainty in their planning through diversion, disruption, detection, or interdiction, thus forcing the adversary toward a decision against WME use. Similarly, increased resilience to the consequences of an attack, through, for example, advance planning on maintaining essential transportation and other functions in the aftermath, diminishes the attractiveness of WME use by a potential perpetrator desiring massive effect. This enhanced defensive posture should be a component of expanded deterrence.

Engage Citizens
Bridge the preparedness gap between an overextended National Guard and the crisis management needs of the federal and state level leadership by engaging citizen volunteers. Proposals such as the non-expeditionary Home Guard, operating under gubernatorial control, and other volunteer-based measures can demonstrate national resilience and provide Americans with a way to contribute to national preparedness by assisting law enforcement and other offi-

cials with support such as traffic control and delivery of food and water during a crisis.

Supporting Actions

Create Uncertainty for Potential Attackers
Complicate their plans and force them into modes of operation that are more susceptible to detection and interdiction.

Understand and Prevent Radicalization
Target root causes of international terrorism.

Build in Adaptive Capability
Use constant change in defensive posture to increase uncertainty for would be attackers and to counter changes in their tactics.

Adapt or Update Existing Models for Marshalling Citizenry
The Civil Air Patrol, the Coast Guard Auxiliary, and the National Defense Executive Reserve should be adapted and serve as models for a "Home Guard" with specialized skills such as quarantine implementation, vaccine administration, and crisis communications.

Risk and System Management

Moving from the current state to a unified WME prevention system will involve tradeoffs in resource allocation and new approaches to cross-agency system management. As the threat evolves and new approaches and technologies are developed over time, new choices will need to be made on an ongoing basis. Risk management within a system perspective should be the driving force in making such tradeoffs.

Institute a Risk-based Process for Resource Allocation
An open process for targeting prevention funding should be instituted. To ensure that investments deal with the greatest needs from a balance of national and local perspectives, consider establishing an independent body, comparable to BRAC as a check and balance to review integrated WME prevention budget allocations and provide insulation from political liabilities.

Improve Private Sector Contributions to the Process for Risk Management
Outside experts can help design and evaluate the approach to managing risk, but, in addition to a technical resource, the private sector is a likely target of WME attacks and therefore has a vital interest in an effective defense program. Public/private partnerships remain a valuable vehicle for this involvement, but require different approaches for the demands of developing and managing a layered prevention strategy. Programs such as the Smart and Secure Trade Lanes Initiative (SSTLI), the U.S. Customs-Trade Partnership Against Terrorism (C-TPAT), and the Container Security Initiative (CSI) are models of private and public/private partnerships.

Initiate a System Management Effort
The Secretary of Homeland Security should adopt one of several architecturally-based models of integrated systems management to help guide and oversee the planning, development, and integration of the national WME prevention system.

Supporting Actions

Help Industry Make the Business Case for Security and Determine If/When Government Should Provide Assistance
The federal government should assist the private sector in making the business case for security by, for example, developing cost benefit analysis models, creating market-based incentives for security investments, and clarifying the dividing line between government and private sector responsibilities.

Study the Security Risks Posed by U.S. Companies That Have Extensive Global Operations or Outsource To Foreigners
Security experts throughout the private sector are concerned that, due to increased overseas operations, outsourcing, and supply chains, increasing numbers of people from foreign countries now have access to substantial information about U.S. companies and their business models.

Establish Joint Government/Industry Working Groups
Pattern the groups after the existing National Security Telecommunications Advisory Committee to promote coordinated government/private sector counter-terrorism efforts.

Promote Standards for Products Useful in the Anti-terrorism Campaign
Through national standards, create the potential for a large enough market to warrant industry investment.

Provide Selective Indemnification
Indemnify firms that are seeking to assist in the war on terrorism with indemnification against adverse consequences which they could not reasonably be expected to have foreseen.

Create a System Management Board
Since WME prevention spans multiple organizations, the board should include representatives of component elements of the WME prevention system and should meet periodically with the WME system manager. The board should be the forum for stakeholder agencies to participate in risk assessments and decision making on aspects of the WME prevention system.

Appoint a WME System Manager
Have him/her report directly to the secretary and have the authority to manage investments in system capabilities.

Publish a DHS Directive on WME Prevention System Management
Specify the roles, authorities, and organizational relationships in the system management process, including the DHS role as lead, the system approval processes, national and international relationships, and the role of the system management board.

Innovation

A national commitment to innovation is crucial to preventing the WME threat for several reasons: 1) new technologies are needed to detect WME components under different conditions (e.g., during acquisition phases, during production, enclosed in containers), 2) the threat evolves and our capabilities must evolve as well, and 3) “out of the box” thinking is needed to devise new strategies and tactics and to challenge our existing strategies, tactics, and systems. The Task Force offers the following recommendations in this area.

Make Detection a Priority for Innovation
The secretary, the HSC, and the president should make it among the highest national priorities to bring together elements of the research community to undertake transformational research.

Encourage and Nurture New Ideas
Create a process that encourages new ideas from people within and external to the department. Drawing from organizational innovation models from government and industry, create an Innovations Office, similar to Lockheed Martin’s “Skunk Works,” and institute other mechanisms to encourage out of the box ideas from all levels and sectors across the homeland security and related

communities. Provide a clear path for those ideas to gain visibility, be tested, and ultimately be acted upon by decision makers.

Supporting Actions

The DNDO Model Should Apply to Other WME Threats Such as Biological, Radiological, and Chemical Agents and Explosives

Rapid progress can be made by marshaling relevant assets across the executive branch to focus efforts on research, development, testing, and evaluation of transformational detection capabilities and strategies. Wherever possible, technologies should be developed that have dual use benefits (e.g., detecting drug contraband as well as WME).

Develop and Apply Performance Metrics to Guide Organizational Behavior Toward Long-term Goals

When necessary, officials outside of the organization that will be assessed should set performance metrics.

Systematically Institute Frank and Candid "After Action Reports"

Management must value frank and constructive criticism by and of all parties (supervisors and subordinates) by incorporating input into planning and practice and ensuring that there is no retribution for candid contributions.

Make "Red Teaming," the Process of Gaming an Adversary's Actions, a More Integral Part of Training and Routine Operations

Purposefully testing a system, people, and equipment to probe for weaknesses can improve their security by mimicking the techniques the adversary would use to carry out an attack. When done at the system (rather than component) level, management can identify system improvements.

Create a Long-range Review Process Akin to the DOD's *Quadrennial Defense Review* That Takes Into Account Strategy, Research and Development, Budgeting, and Other Factors

Investments in infrastructure, science, and technology require long-range planning. Management and operators must systematically feed requirements into the research and system development process and provide continuous updates. Such a tool would need to go beyond DHS and include all relevant agencies to be effective.

Appendix A—Detailed Supporting Actions

The recommendations offered in Section IV are supplemented here with specific proposals for implementation.

Authority, Alignment, and Incentives

Strengthen Leadership Structures for Enhanced Joint Effort

Under direction of the Secretary of Homeland Security, the multilateral layered defense framework also depends on the coordinated effort of multiple participants spanning all levels of government and working across lines between the public and private sectors. Coordination and integration of policies, planning, and operations is hard work that is not a matter of coordinating individual agency plans but the joint execution of commonly held plans. Recommendations along these lines include the following:

Improve interagency coordination—develop policy, planning, and processes that facilitate joint effort across the federal government. In cross cutting areas such as maritime security and biodefense, national strategy must be accompanied by clear guidance and lines of responsibility and authority. The layered defense approach provides a framework for reviewing and, where necessary reengineering interagency processes to fill gaps and improve clarity.

Develop a government-wide system that rewards interagency cooperation and coordination. To be effective DHS must create and manage a coordinated network of stakeholders who (1) understand and accept their roles/responsibilities as part of a joint effort to ensure prevention, and (2) are actively engaged in collaborative efforts to reduce WME security risks. Incentives must be aligned with these objectives and barriers to cooperation and coordination removed.

Develop Institutional Capabilities to Engage Internationally

To defend the homeland, America must promote collective security extending beyond our borders and those of our allies. To do so requires that DHS develop strategic and ongoing relationships with similar institutions of foreign governments. Such relationships exist currently between selected component DHS offices and foreign governments but no comprehensive and coordinated engagement program exists. In many cases, State Department foreign service officers or Defense Department attachés have assumed responsibility for any DHS questions or inquiries forthcoming from host nations. First, DHS should provide country or regionally specific portfolios to U.S. Missions (i.e., NATO, European Union, and Association of Southeast Asian Nations) and Embassies with the necessary information, programmatic insight and strategic vision to help guide DHS policy internationally. Second, development of an attaché program will ensure an institutional approach providing resident DHS expertise in those missions/embassies with international components of our homeland security policies.

Create country or region-specific DHS portfolios to provide each U.S. mission/embassy with clear-cut DHS strategic guidance. Dynamic DHS "portfolios" of evolving issues/policy objectives should guide existing foreign service officers, defense attachés, and existing DHS personnel located at missions/embassies on:

- Elevating and enhancing bilateral coordination of DHS policies involving the cooperation of, or coordination with, a specific foreign country or grouping of countries
- Sharing and gathering information and best practices for anti- and counterterrorism measures, nonproliferation/counterproliferation efforts, and WME prevention policies
- Communicating both concerns and lessons learned from a particular country's homeland security programs and practices to DHS headquarters, the intelligence community where appropriate, and homeland security leadership at the White House level

Leverage existing DHS resources currently assigned to U.S. missions/embassies abroad. DHS should ensure employees assigned to U.S. missions/embassies carry and represent the entire DHS portfolio, not just that of their component agency (i.e., U.S. Coast Guard, Immigration and Customs Enforcement).

Create dedicated DHS foreign service attaché positions. Ultimately, DHS should create a unified presence abroad by introducing a cadre of DHS attachés at U.S. foreign embassies. DHS attachés would institutionalize relationships thereby coordinating and advancing the department's strategic objectives with relevant U.S. departments abroad and with foreign governments.

Engage multilateral organizations on homeland security-related issues. A true commitment to building international partnerships is essential to global security. The security of our allies aids our own security. Strategic partnerships become force multipliers by increasing fungible resources, increasing knowledge, and avoiding replication of work when the U.S. leverages the work these trusted partners have accomplished.

Programs like the CSI are a good start. For example, CSI-enabled partnering with foreign customs officials inherently reduces the pool of containers to be inspected ensuring greater volume of inspected containers and reducing duplication of effort at border crossings. Whereas CSI is a bilateral initiative, there are many circumstances when multilateral approaches should be implemented by partnering with large organizations such as the Organization for Cooperation and Security in Europe and the Asian Pacific Economic Cooperation.

These organizations have reach into regions of the world where overt bilateral cooperation with the U.S. would be extremely unpopular domestically. Additionally, these organizations have reach into regions that may actually be the true breeding grounds of terrorism abroad and thus be in a unique position to help address the root causes of terrorism.

Example: The 166 countries of the World Customs Organization (WCO) circulated a set of common standards for international customs agencies and private shippers that would tighten cargo security while expediting trade. Certain standards address advance trade data information and shipper verification agreements like the Customs-Trade Partnership Against Terrorism, or C-TPAT. Countries that meet those standards receive expedited cargo clearance as a "carrot" for compliance. For those countries willing but unable to comply, the WCO agreement includes capacity-building measures and additional resources to help them adhere. The U.S. joined about 100 other countries when it

announced plans to adopt the WCO standards in June 2006.

Institutionalize DHS participation in NATO through a "Reinforced North Atlantic Council (NAC)." The NAC and its auxiliary structures should serve a greater cooperative role pursuing common homeland security objectives, sharing best counterterrorism practices with other NATO members and Partners, and developing security competencies related to fighting terrorism globally.

NATO structures—in coordination with the European Union, the G8, and others—can help achieve three interlocking security objectives:

- Deterring, co-opting, and destroying terrorist organizations
- Developing more effective emergency response capabilities and contingencies
- Improving information sharing throughout its growing territory that includes unique relationships with the Middle East

A "reinforced NAC" today should address critical issues such as homeland security and counterterrorism, which can be separated for now from the more polarizing debates about commitments in Iraq and Afghanistan.

Participate in joint contact/working groups. DHS should seek to work with countries on a bilateral basis and seek to participate in existing forums to strengthen international cooperation and to garner support for programs to prevent the use of WME throughout the world. Two groups that represent this type of effort include the US-UK Joint Contact Group on Homeland Security and the U.S.—India Joint Working Group on Counterterrorism.

Require Joint Effort

Create joint task forces focused on preventing the entry of WME. DHS should consider creating joint homeland security task forces to coordinate roles and missions in developing, deploying, and managing a layered prevention strategy in the air, land, and sea domains. These planning and coordination mechanisms would match up with the National Incident Management System, which would engage at the moment an attack or incident of national significance occurred.

Coordinate within the federal government to avoid duplication of effort and conflicting guidance. The private sector would like the government to take responsibility for identifying and de-conflicting requirements placed on industry that reflect overlapping or conflicting interests between departments and agencies. An example of this is one department's requirement to harden the underside of passenger airplanes, and another department's requirement to decrease the weight of aircraft to make them more fuel efficient.

Institutionalize response organizations such as the Interagency Incident Management Groups (IIMG) to take on a prevention function during non-emergency periods. To the same extent that managing the response to terrorist attacks and natural disasters requires a robust interagency approach, so also do the strategic prevention measures of a layered defense. Institutionalizing the IIMG to allow for ongoing coordination at this level would strengthen DHS capabilities as well as national efforts in preventing WME threats via several modes of attack. A layered prevention effort must operate across federal entities and defend in the air, land, and sea domains.

Eliminate unnecessary bureaucratic redundancy. The Task Force acknowledged a distinction between bureaucratic redundancies and the kind of redundancies purposefully built into a layered defense system. Duplication and gaps are inevitable in a complex system developed and operated at different times by many different participants. They are frustrating to system users, especially when perceived as arbitrary or bureaucratically motivated and tend to increase costs for commercial enterprises (especially those relying on just-in-time operations). On the other hand, extreme efficiency obtained by eliminating all duplication tends to increase vulnerability to single point and catastrophic failures. The system architecture should guide the introduction of desirable redundancy to increase system robustness with minimum impact on system efficiency. Duplication should be by design, not by accident.

Ultimately, leaders should use risk management principles to make informed decisions and tradeoffs; redundancies, the design of specific elements, the sequence and timing of system development, and other features should be the product of risk management calculations. Examples of rational choices include the following:

- Background checks and certification for transportation workers such as cross-border truckers should be consolidated to one standardized and reliable process.
- Screening of trusted individuals should be based not only on the past but regularly updated to reflect changing circumstances.
- Where an existing process is not effective for WME prevention purposes, a separate system, although appearing on the surface to be duplicative would be advisable. The use of the Department of Transportation's HAZMAT list to guide inspections was noted as an example. A very small percentage of the chemicals of concern on the list could be weaponized and others absent from the list could pose a WME risk.

Expand the Customer Set for WME Intelligence

DHS leadership should actively task WME intelligence analysis. WME intelligence has traditionally been applied to supporting demarches about treaty violations and sanctions. Today, the WMD intelligence consumer should be defined by a broader constellation of authorities, to include the Departments of Homeland Security, Health and Human Services, and the FBI. Preventing WME attacks on the homeland requires a forthright role for DHS in the consumption of the analysis produced by the developing bureaucracy of the National Intelligence Directorate, including specifically the National Counterproliferation Center and the National Counterintelligence Center. However, doing so entails DHS leadership actively tasking these and other intelligence community organizations with fulfilling analysis requirements about the WME/WMD threat. For example, the Department's Domestic Nuclear Detection Office is responsible for creating a deployment strategy, or "global architecture," to operate across all layers in defending against smuggled nuclear weapons and material. To do so, the DNDO must consider intelligence about the trajectory of the current nuclear threat, including potential perpetrators, means of delivery, and likely sources of illicit nuclear material. All of this informs the ultimate characteristics of a global deployment strategy, and none of this information comes from just one source

Engage Citizens

Readiness and response capabilities depend greatly on the ability to defend the "layers" closest to the homeland. In addition to the

quality programs underway at the federal, state, and local levels, doing so demands the active commitment of Americans to contribute their time, expertise, and resources for this vital component of a layered prevention strategy. Nevertheless, there has been much public discussion about the lack of a sense of "shared sacrifice" in the war against terrorism and many Task Force members identified a lack of urgency among the public as to the nature of the threat.

The ongoing deployment of the National Guard and Reserves in Iraq and Afghanistan highlight the need to reassess how the U.S. structures and utilizes forces traditionally considered the cornerstone of homeland security. The U.S. has always reviewed and restructured local militias and the National Guard when the nation is in danger. Over the centuries, our nation's National Guard has evolved from being colonial homeland defenders, to expeditionary forces, to part of a total force in the 21st century. It is equally important that the White House and DHS create an atmosphere of trust, collaboration, support, and hope for the families and employers of our citizen patriots through a call for shared sacrifice. Now it is time to consider establishing a non-expeditionary "Home Guard" to meet state and local challenges to safety and security. We should marshal the nation's citizenry through trained and standardized volunteer networks to serve as force multipliers when needed.

A Potential Model. Several models were put forth of organizations created in previous times of conflict that should be re-engaged. The Civil Air Patrol, Coast Guard Auxiliary, and various state defense forces serve as existing organizations with real utility that DHS should invest in, populate, and popularize to great strategic value. However, a *new* model might include a standardized, trained, and modestly funded volunteer corps, the characteristics and capabilities of which would reflect the needs of individual states as a national Home Guard.

A Home Guard should augment the active military, the National Guard, the Reserves, and the Coast Guard. This specially trained corps would not be eligible for deployment abroad, and would be capable of rapid response when called upon by governors to respond to domestic emergencies. Some states already have militias, but this would *qualitatively* upgrade America's homeland defense.

Home Guard forces would contain special skills, such as quarantine, rapidly dispersing and administering vaccines, crisis communications, fire fighting, first aid, and complex policing duties. Perhaps most important to Home Guard members would be command and communications capabilities—a domestic reservoir of soldiers skilled in a number of vital tasks will maximize local efforts to secure communities.

Recruitment and training also would be guided by the need to conduct tasks peculiar to the cyclical demands of each state (i.e., hurricanes, earthquakes). Training would build upon best practices of National Guard, Coast Guard Auxiliary, Civil Air Patrol, local police reserves, existing state militias, and other similar organizations. A full-time professional staff of active duty Home Guard personnel, drawn from the ranks of the Home Guard, would ensure organizational readiness.

Existing Efforts Can Help. A Home Guard provides a cost-effective option for assisting in the nation's security and defense needs within a layered strategy. The Joint Force Multiplier Command, for example, is a group of civilians, most of whom have substantial military or law enforcement back-

grounds, and who have formed a non-profit corporation with the objective of assisting federal, state, and local authorities in meeting the challenges of terrorism and associated threats to national security and defense. This organization, in addition to other volunteers, should be empowered, invested in, and made part of a national Home Guard, reporting to state governors with training and funding provided by a national command or headquarters and the DHS.

The National Defense Executive Reserve provides another model for marshaling the nation's citizenry with specific skills associated with emergency preparedness and emergency response. Established by President Eisenhower in 1956, the National Defense Executive Reserve is composed of persons selected from the civilian economy for employment in federal executive positions when needed during an emergency of national significance. Statutorily, the Director of FEMA administers this program and coordinates other agency work in the establishment of National Defense Executive Reserve (NDER) units. The NDER should be updated by being placed under the Secretary of Homeland Security and within the Home Guard Command. Furthermore, its roles should be redefined to accommodate new doctrines such as the National Incident Management System and the National Response Plan.

Meeting National Demand with Local Response. Citizens signing up to be a part of this nationwide resource should be assured that their commitment is to protect the homeland at home, not overseas. In addition, the Home Guard would only be federalized under two specific circumstances: for multi-state disasters requiring a concentration of forces beyond a single state's capacity, and to augment existing National Guard and active military in the event of an actual attack on the U.S. Incentives should be provided to encourage enlistment. Tuition reductions or wavers and deferred federal student loan repayment should both entice enlistment and support Home Guard forces while serving. A Home Guard would meet national demand with local response.

Deterrence

Expand Deterrence Within the WME Context

Create uncertainty for potential attackers. The risk reduction approach emphasizes the importance of introducing uncertainty into a terrorist's ability to plan and conduct an attack against the U.S. In this regard a nuclear weapon would represent a very major asset to a terrorist organization and as such it would seem likely that any such organization would be reluctant to lose control of the device (for example, by subjecting it to the vagaries of a commercial shipping system). Similarly, they would want a very high degree of assurance that whatever attack was planned would in fact be successful. Thus, by implementing a defense in depth that changes character at frequent intervals (e.g., by varying the types of inspections that are conducted, varying the sensors which are used and their locations, etc.) the U.S. will substantially diminish an attacker's confidence. This in turn would force a potential attacker to adopt more complex plans, perhaps involving more personnel. Such attacks would, because of their size and complexity, be more subject to discovery.

Understand and prevent radicalization. The root causes of international terrorism must be better understood and countered over time. The spread of radicalism occurs in a political, sociological, psychological, and religious context that influences recruitment, modes of operation, communication, organization, financing, and training, among other

aspects. Each of these functions must be the subject of in depth analysis and a strategy finds and exploits weaknesses. Targeting root causes takes time and persistent effort. In the meantime, today's threats must be addressed by improved knowledge of the progression of the threat and effective strategies to shape it in our favor. Several of our European allies have done a great deal of work along these lines. Collaboration on this issue with our international allies would prove extremely beneficial.

Build in adaptive capability—use change to advantage. The system architecture should—at a minimum—adapt to accommodate changes in an enemy's tactics, targets, etc. Reactive adaptation however necessary is insufficient. Constant adaptation must be the norm so as to keep the enemy off-balance and uncertain about the possibility of success.

- Processes that involve inspection and surveillance should vary their sampling approach over time. A changing mix of random, targeted, and 100 percent checks or inspections generates the most uncertainty for attackers and prevents their ability to game the system.
- Flexibility of response must be built into system capabilities. Holding assets in reserve, increasing the dual-use of existing assets, and increasing their mobility/ability to deploy are ways to generate efficiencies to counter multiple threats. This approach favors capabilities-based planning over threat-based planning, a particularly desirable strategy given uncertainties about the threat.

Risk and System Management

(No additional specific recommendations offered.)

Innovation

Make Detection a Priority for Innovation
The DNDO model should apply to other WME threats such as biological, nuclear, and chemical agents and explosives. Rapid progress can be made by marshaling relevant assets across the executive branch to focus efforts on research, development, testing, and evaluation of transformational detection capabilities and strategies. Wherever possible, technologies should be developed that have dual use benefits (e.g., detecting drug contraband as well as WME).

Encourage and Foster New Ideas
Developing and applying performance metrics to guide organizational behavior toward long-term goals. When necessary, officials outside of the organization that will be assessed should set performance metrics.

Systematically institute frank and candid "after action reports." Management must value frank and constructive criticism by and of all parties (supervisors and subordinates) by incorporating input into planning and practice and ensuring there is no retribution for candid contributions.

Make "Red Teaming," the process of gaming an adversary's actions, an integral part of training and routine operations. Purposefully testing a system, people, and equipment to probe for weaknesses can improve their security by mimicking the techniques the adversary would use to carry out an attack. When done at the system (rather than component) level, management can identify system improvements.

Creating a long-range review process akin to the DOD's Quadrennial Defense Review that takes into account strategy, research and development, budgeting, and other factors. Investments in infrastructure, science,

and technology require long-range planning. Management and operators must systematically feed requirements into the research and system development process and provide continuous updates. Such a tool would need to go beyond DHS and include all relevant agencies to be effective.

Improve Private Sector Contributions to the Process for Risk Management

Help industry make the business case for security and determine if/when government should provide assistance. The federal government should assist the private sector in making the business case for security through:

- Development of cost benefit analysis models that the industry can employ to make sound business case justifications for increased security measures
- Development of a process that assists industry in assimilating security as part of the business model in a manner similar to that of quality control
- Development of market-based financial incentives to encourage security investments
- Clarifying, in specific cases, the dividing line between government responsibilities versus a private sector responsibility

---

Another HSAC Task Force is working on Critical Infrastructure Resiliency issues and is expected to produce a business case for the private sector. This report is expected in early 2006.

Study the security risks posed by U.S. companies outsourcing to foreigners. Security experts throughout the private sector are concerned that, due to increased overseas outsourcing and supply chains, increasing numbers of people from foreign countries now have access to substantial information about U.S. companies and their business models. These groups largely operate outside the control of the U.S. government and also the span of control of private sector security personnel.

Appendix B – Member Biographies

Chairman, Task Force
Lydia Thomas of Maryland is president and CEO of Mitretek Systems, Inc., and she was previously vice president and general manager responsible for the company's Center for Environment, Resources and Space. Dr. Thomas served two terms on the Environmental Advisory Board to the Chief of Engineers, U.S. Corps of Engineers and was chairperson of the Chemicals Regulation Sub-Group of the United States Energy Association. In February 2003, Dr. Thomas was recognized as "Black Engineer of the Year" by the Black Engineer Selection Panel. She is a member of the Homeland Security Advisory Council

Vice-Chairman, Task Force
Jerry Cohon of Pennsylvania is the president of Carnegie Melon University. He is a national authority on environmental and water resource systems analysis. He served as a member of the Nuclear Waste Technical Review Board and was named chairman in 1997. In 1992, he was named the dean of the School of Forestry and Environmental Studies at Yale University. He is the Vice-Chair of the Academe, Policy and Research Committee of the Homeland Security Advisory Council.

Judge Webster of the District of Columbia will serve as Vice Chair. In 1977, Webster became director of the FBI after serving as a judge on the U.S. Court of Appeals for the Eighth Circuit. In 1987, Webster became the director of the CIA, which he led until 1991. Since then, Webster has practiced law at the Washington, D.C. firm of Milbank, Tweed, Hadley and McCoy. Judge Webster served as vice chairman of the PHSAC from 2002-2003. He is the Acting Chairman of the Homeland Security Advisory Council.

Chair, Air Domain Subgroup
Norm Augustine of Maryland is currently a member of the Board of Directors of Conoco Phillips, Black & Decker, Procter & Gamble and Lockheed Martin and a member of the Board of Trustees of Colonial Williamsburg, MIT and Johns Hopkins University. Mr. Augustine served as Chairman and Principal Officer of the American Red Cross for nine years and is a former Chairman of the National Academy of Engineering, the Association of the United States Army and the Defense Science Board. Mr. Augustine represents the Panel on Science and Technology of Combating Terrorism, on the President's Council of Advisors on Science and Technology on the HSAC.

Chuck Canterbury of South Carolina is a Major in the Horry County Police Department where his career of more than 25-years has included service in the Patrol Division and the Criminal Investigations Division. He also served as the Training Division Supervisor, during which he was certified as an instructor in basic law enforcement, firearms, chemical weapons, and pursuit driving. He currently serves as the President of the Grand Lodge of the Fraternal Order of Police, an organization representing more than 300,000 law enforcement professionals nation-wide. He is Vice-Chair of the Emergency Response Senior Advisory Committee of the HSAC.

Lee Hamilton, Director of the Woodrow Wilson International Center for Scholars in January, 1999. Prior to becoming Director of the Woodrow Wilson Center, Lee Hamilton served for thirty-four years as a United States Congressman from Indiana. Mr. Hamilton established himself as a leading congressional voice on foreign affairs, with particular interests in promoting democracy and market reform in the former Soviet Union and Eastern Europe, promoting peace and stability in the Middle East, expanding U.S. markets and trade overseas, and overhauling U.S. export and foreign aid policies. He is a member of the Homeland Security Advisory Council.

Chair, Land Domain Subgroup
James Schlesinger of Virginia has a long and distinguished record of public service. He has served as Secretary of the Energy, Secretary of Defense, Director of Central Intelligence, and chairman of the Atomic Energy Commission. Schlesinger is currently the chairman of the Board of Trustees of the MITRE Corporation. He is a member of the Homeland Security Advisory Council.

Chair, Sea Domain Subgroup
David Abshire of Virginia, is the President of the Center for the Study of the Presidency and Vice President of the Center for Strategic and International Studies, which he and Admiral Arleigh Burke founded in 1962. A graduate of West Point, Dr. Abshire has served as an Assistant Secretary of State for Congressional Relations and as an Ambassador to NATO. He is a member of the Academe, Policy and Research Senior Advisory Committee of the HSAC.

Victoria Haynes of North Carolina, is the Chief Executive Officer of the Research Triangle Institute. Dr Haynes is a leader in technology leadership, management and new business development. Prior to joining RTI, Dr. Haynes was the Vice President of the Advanced Technology Group and Chief Technical Officer at the BF Goodrich Company, and served in managerial roles with the Monsanto Corporation. She is a member of the Academe, Policy and Research Senior Advisory Committee of the HSAC.

Dan Goure of Virginia, is the Vice President of the Lexington Institute, a non-profit policy-research organization in Arlington, Virginia. As a Senior Advisor to the Secretary of Defense, Dr. Goure conducted in-depth studies on long-range budget projections, analyses of major weapons programs and force sizing metrics. He currently serves as an Adjunct Professor in the graduate program of the Center for Peace and Security Studies at Georgetown University. He is a member of the Academe, Policy and Research Senior Advisory Committee of the HSAC.

Roxane Silver of California, is a Professor in the Department of Psychology and Social Behavior and Department of Medicine at the University of California, Irvine. A national expert in the field of stress and coping, she is a Fellow of both the American Psychological Association and the American Psychological Society. Dr. Silver is principal investigator of the only ongoing national study of psychological responses to the September 11th terrorist attacks. Dr. Silver also serves as Director of Graduate Affairs for the Department of Psychology and Social Behavior and the coordinator of its doctoral program in Health Psychology. She is a member of the Academe, Policy and Research Senior Advisory Committee of the HSAC.

Rocky Spane of California, is the Commissioner of the Unified Port of San Diego. A career naval officer with 33 years of service, he commanded the Theodore Roosevelt Battle Group during Operation Desert Storm and was the Captain of the nuclear aircraft carrier USS Enterprise. During his final assignment, he commanded all naval aviation assets in the Pacific and Indian Oceans. He currently serves on the boards of several privately and publicly held companies. . He is a member of the Academe, Policy and Research Senior Advisory Committee of the HSAC.

Steve Gross of California, is the Owner and President of Border Trade Services (BTS), a warehousing and distribution company headquartered in San Diego. He is a past Chairman and current Board Member of the Border Trade Alliance, a tri-national organization headquartered in Phoenix that represents trade and advocacy issues affecting Canada, the U.S. and Mexico. He is also past President of the Otay Mesa Chamber of Commerce. He is a member of the Private Sector Senior Advisory Committee of the HSAC.

Kathleen Bader of Michigan is a Business Group president with Dow Chemical Company and the corporate vice president for Quality and Business Excellence. She joined Dow in 1973 and has held a variety of positions in sales and operations. She is the Chair of the Private Sector Senior Advisory Committee of the HSAC.

Jack Skolds of Illinois, is the Executive Vice President of Exelon Generation; President and Chief Nuclear Officer of Exelon Nuclear; and the Chief Executive Officer of AmerGen, a partnership between Exelon and British Energy. Prior to his current positions, Skolds was the General Manager of Station Operations at the V.C. Summer Nuclear Plant with South Carolina Electric and Gas (SCE&G). Skolds is a graduate of the United States Naval Academy.

Dirk Kempthorne was reelected as Idaho's Governor in November of 2002. He was first elected as Idaho's 30th Chief Executive in 1998, following a successful six-year term in the United States Senate. As a Senator, he wrote, negotiated, and won passage of two major pieces of legislation: a bill to end unfunded federal mandates on state and local governments, and a substantial revision of the federal Safe Drinking Water Act. He also worked to improve the quality of life for American active duty military personnel, reservists, their families, and veterans. He is a member of the State & Local Senior Adviory Committee of the HSAC.

Brian Sandoval was sworn in as Nevada's Attorney General on January 6, 2003. In 1998 he was appointed to serve on the Nevada Gaming Commission. One year later, he was appointed as Chairman of the Nevada Gaming Policy Review Panel. He also served two terms in the Nevada Legislature, where he sponsored fourteen bills that became law. Attorney General Sandoval is a member of the Nevada State Boards of Pardons, Prisons, Examiners, Transportation, Domestic Violence and Private Investigators and the Board of Trustees for Children's Cabinet of Reno, Nevada, St. Jude's Ranch and Washoe County, Nevada Law Library.

Bernard Kerik of New York, is the Chief Executive Officer of Giuliani - Kerik LLC. He most recently served as the Interim Minister of Interior and Senior Policy Advisor for the U.S. led Coalition Provisional Authority in Iraq. His 28-year career in law enforcement includes four years in various security positions in the Kingdom of Saudi Arabia and as the First Deputy and Commissioner of the New York City Correction Department. He retired after serving as the 40th Police Commissioner of the NYPD overseeing the rescue, recovery, and investigation of the attack on the World Trade Center on September 11, 2001. He is a member of the Emergency Response Senior Advisory Committee of the HSAC.

Scott Lillibridge of Texas is the Director of the Center for Bio Security at the University of Texas. Mr. Lillibridge was previously the Director of Bioterrorism Preparedness and Response Program at the Centers for Disease Control and Prevention. He is a member of the Emergency Response Senior Advisory Committee of the HSAC.

Jane Perlov of North Carolina is the Chief of Police of Raleigh, North Carolina. Chief Perlov previously served as the Secretary of Public Safety for the Commonwealth of Massachusetts.

Edward Plaugher of Virginia is the Fire Chief for Arlington County. Chief Plaugher is the Immediate Past President of the State Fire Chiefs of Virginia and a member of the International Association of Fire Chiefs. He is a member of the Emergency Response Senior Advisory Committee of the HSAC.

Steve Kerr of New York is the Chief Learning Officer (CLO) and a Managing Director of Goldman Sachs. From 1994-2001 he was the Vice President-Leadership Development and CLO for General Electric, and was responsible for their renowned leadership education center at Crotonville, NY. Dr. Kerr has served as a member of the faculties of Ohio State University, the University of Michigan and the University of Southern California, where he was Dean of the faculty of the business school. He is a member of the Academe, Policy and Research Senior Advisory Committee of the HSAC.

Homeland Security Advisory Council Staff

Daniel Ostergaard, **Executive Director**

Richard Davis

Carnes Eiserhardt

Michael Fullerton

Jeff Gaynor

Katie Knapp

Mike Miron

Candace Stoltz

Associate Director

Benjamin Gray

Writing Team

Bob Clerman

Ann Buckingham

Jonah Czerwinski

Edward Kittel

John Daggett

GLOSSARY
OF ACRONYMS

ADIZ Air Defense Identification Zones
ASEAN Association of Southeast Asian Nations
BRAC Base Realignment and Closure Commission
C-TPAT U.S. Customs-Trade Partnership Against Terrorism
CIA Central Intelligence Agency
CSI Container Security Initiative
DOD Department of Defense
DHS Department of Homeland Security
DNDO Domestic Nuclear Detection Office
EU European Union
FBI Federal Bureau of Investigation
FEMA Federal Emergency Management System
HHS Department of Health and Human Services
HAZMAT Hazardous Materials
HSAC Homeland Security Advisory Council
HSC Homeland Security Council
IIMG Interagency Incident Management Group
NAC North Atlantic Council
NACIC National Counterintelligence Center
NATO North Atlantic Treaty Organization
NCPC National Counterproliferation Center
NIMS National Incident Management System
NDER National Defense Executive Reserve
NRP National Response Plan
NSC National Security Council
NSTAC National Security Telecommunications Advisory Committee
QDR Quadrennial Defense Review
SSTLI Secure Trade Lanes Initiative
WCO World Customs Organization
WMD Weapons of Mass Destruction
WME Weapons of Mass Effect