DHS 2.0

RETHINKING THE DEPARTMENT OF HOMELAND SECURITY

DECEMBER 13, 2004

David Heyman
James Jay Carafano, Ph.D.

DHS 2.0

Rethinking the Department of Homeland Security

James Jay Carafano, Ph.D., and David Heyman

James Jay Carafano, Ph.D., is Senior Research Fellow for Defense and Homeland Security in the Kathryn and Shelby Cullom Davis Institute for International Studies at The Heritage Foundation.

David Heyman is Director and Senior Fellow of the Homeland Security Program at the Center for Strategic and International Studies.

The task force co-chairmen and participants would like to acknowledge the helpful support provided by the Center for the Study of the Presidency and the use of its online Homeland Security Database and Information Exchange Site, which facilitated the task force's deliberations. The site is located at *www.thepresidency.org/hsdatabase.htm*.

Table of Contents

Executive Summary

This report presents the conclusions of a task force charged with examining the organization and operations of the U.S. Department of Homeland Security (DHS). The task force included representatives from academia, research centers, the private sector, and congressional staff and was chaired by homeland security experts from the Center for Strategic and International Studies and The Heritage Foundation. The task force evaluated DHS's capacity to fulfill its mandate as set out in the Homeland Security Act of 2002 based on four criteria: management, roles and missions, authorities, and resources.

Based on this analysis, conducted through seminars, an extensive literature search, and interviews, the task force developed over 40 major recommendations. Together, these proposals make the case for a significant reorganization of the department to make it a more effective and efficient instrument for preventing and responding to terrorist threats.

Each section consists of findings and recommendations agreed upon by the task force. Major recommendations in the report include:

- **Strengthening** the Secretary of Homeland Security's policymaking function by creating an Undersecretary for Policy.
- **Empowering** the secretary by establishing a "flatter" organizational structure through (1) consolidating and strengthening agencies with overlapping missions; (2) eliminating middle-management (directorate) layers over border and transportation security, preparedness and response, and information analysis and infrastructure protection; and (3) having the agencies report directly to the secretary via the Deputy Secretary of Homeland Security.
- **Rationalizing** government spending by establishing a risk-based mechanism for department-wide resource allocation and grantmaking and by developing pre-determined "response packages" to respond to catastrophic terrorism.
- **Clarifying** authorities and national leadership roles for bio-defense, cyberdefense, and critical infrastructure protection.
- **Improving** departmental oversight by rationalizing congressional committee structure and establishing permanent oversight committees in the House of Representatives and the Senate.

Congress and the Administration should develop a comprehensive plan to restructure the department, including establishing a nonpartisan commission to review the performance of the department and assess its capacity to fulfill the missions outlined in the Homeland Security Act in the areas of management, missions, authorities, and resources and to report back within six months.

Introduction

On November 25, 2002, the Homeland Security Act of 2002 transferred over 22 federal entities—some intact and some in part—and 180,000 employees into the newly created U.S. Department of Homeland Security (DHS). According to the legislation, the department's mission is (1) to prevent terrorist attacks within the United States, (2) to reduce the vulnerability of the United States to terrorism, and (3) to minimize the damage and assist in the recovery from terrorist attacks that do occur within the United States. Created as part of the national response to the horrifying terrorist attacks on New York and the Pentagon on September 11, 2001, DHS is the single most ambitious and sweeping bureaucratic initiative undertaken by the federal government to protect Americans against future terrorist threats.

This report assesses progress in that effort. A task force representing academia, research centers, the private sector, and congressional staff chaired by homeland security experts at the Center for Strategic and International Studies and The Heritage Foundation examined the effectiveness of the new department in four areas: management, roles and missions, authorities, and resources. Based on this analysis, conducted through seminars, an extensive literature search, and interviews, the task force developed 40 major recommendations for improving the oversight, organization, and operation of DHS.[1] We believe that, taken together, these recommendations make the case for a significant reorganization of the department to empower the Secretary of Homeland Security and make the department a more effective and efficient instrument for preventing and responding to terrorist threats.

Why This Report? Why Now?

We have learned a lot since 9/11. In the three years following the most serious attacks on U.S. soil since Pearl Harbor, Americans have had ample time to dwell on the challenges of protecting the nation against foreign threats in the 21st century and to review the efficacy of our response to these dangers. The results of both efforts suggest that it is time to rethink the place of the Department of Homeland Security in this effort.

There are no frontiers in 21st century national security. Distinguishing clear lines of responsibility between foreign and domestic security is a thing of the past. Additionally, the age when only great powers could bring great powers to their knees is over. The specter of catastrophic terrorism that could threaten tens of thousands of lives and hundreds of billions of dollars in destruction will be an enduring concern. A review of the initial conception for DHS in the Homeland Security Act suggests that the department's original organization does not reflect these realities well.

Putting it bluntly, the current organization of DHS must be reformed because it hampers the Secretary of Homeland Security's ability to lead our nation's homeland security efforts. The organization is weighed down with bureaucratic layers, is rife with turf warfare, and lacks a structure for strategic thinking and policymaking. Additionally, since its creation, whether one looks at the department's capacity to organize and mobilize a response to a catastrophic terrorist attack or at the international dimension of DHS programs, the department has been slow to overcome the obstacles to becoming an effective 21st century national security instrument.

A new threat environment requires a new approach to security. A nimble, highly adaptive adversary necessitates a bureaucracy that is flexible and responsive to a constantly changing threat. The melting of borders and blurring of foreign and domestic interests means that we need to foster new working relationships at home and abroad. The two lead agencies charged with protecting America are the Department of Defense (DOD) and the Department of Homeland Security. If the Department of Defense has been a primarily outward-looking institution, it must now provide greater support to domestic security. If the Department of Homeland Security has been primarily inward-focused, it must now also embrace the international dimensions of security, especially given the globally interconnected networks of our global society.

1. To the greatest extent possible, this document reflects a consensus of the task force members. However, not all members of the task force agreed with each and every recommendation. This document and all of its recommendations are intended to initiate a dialogue and to provide options for consideration by those in Congress and the executive branch responsible for protecting America.

It is not prudent to wait much longer before addressing this issue. Experience reminds us that it takes only a few years for a bureaucracy to become entrenched. After that, it becomes nearly impossible to change. The creation of the Department of Defense is a case in point. In the debates over the 1947 National Security Act and again as President, General Dwight D. Eisenhower lobbied for reorganizing the Pentagon to ensure that Army, Navy, Marine, and Air Force assets would work closely together. However, he failed to overcome the political opposition and service parochialism that blocked reforms. As a result, fundamental problems in joint operations went unaddressed until passage of the Goldwater–Nichols Act in 1986. The lesson is clear: Fix it at the beginning or live with the mistakes for a long time.

Organization of the Report

The task force's conclusions are organized into four parts that address the key areas that affect how well the organization and operations of DHS fulfill the department's mandate as defined in the Homeland Security Act:

- **Management** considers the organization and functions of the DHS secretariat and their capacity to integrate and effectively direct departmental activities and to provide a coherent vision for the future.
- **Roles and Missions** presents findings and recommendations concerning the organization and conduct of operations for the department's most critical security tasks.
- **Authorities** addresses the adequacy of the legal authorities and policies governing significant department activities.
- **Resources** looks at limitations on the department's ability to allocate resources efficiently and respond effectively to critical missions.

Major Recommendations

Each section consists of findings and recommendations agreed upon by the task force. The findings are what we believe to be significant statements of fact that describe and explain the department's performance. The recommendations are measures that the task force proposes that the Administration and Congress undertake to improve the organization and operation of the department. The recommendations are not intended to be comprehensive. They represent what the task force felt were the highest-priority initiatives. Major recommendations in the report include:

- **Strengthening** the Secretary of Homeland Security's policymaking function by creating an Undersecretary for Policy.
- **Empowering** the secretary by establishing a "flatter" organizational structure through (1) consolidating and strengthening agencies with overlapping missions; (2) eliminating middle-management (directorate) layers over border and transportation security, preparedness and response, and information analysis and infrastructure protection; and (3) having the agencies report directly to the secretary via the Deputy Secretary of Homeland Security.
- **Rationalizing** government spending by establishing a risk-based mechanism for department-wide resource allocation and grantmaking and by developing "response packages" to respond to catastrophic terrorism.
- **Clarifying** authorities and national leadership roles for bio-defense, cyberdefense, and critical infrastructure protection.
- **Improving** departmental oversight by rationalizing congressional committee structure and establishing permanent oversight committees in the House of Representatives and the Senate.

Next Steps

Addressing the task force's recommendations in a piecemeal manner would be wrong. None of these measures is individually sufficient to create the DHS that America needs for the future. Indeed, the efficacy of many of these

initiatives depends on the adoption of the others. Congress and the Administration should develop a comprehensive plan to restructure the department. The task force recommends the following agenda for reform.

- The first action of the 109th Congress should be to consolidate oversight and establish permanent committees in the House and Senate with jurisdiction over all of the homeland security responsibilities of the department.
- The President and Congress should establish a nonpartisan commission to review the performance of the department and assess its capacity to fulfill the missions outlined in the Homeland Security Act in the areas of management, missions, authorities, and resources and to report back within six months. The commission should hold public hearings in addition to its other deliberations and develop a specific and detailed reorganization proposal.
- As part of the process for developing recommendations, the President and Congress should establish principles to guide the commission's efforts.
- Congress should develop and pass a reorganization bill in the next succeeding session.

There is little room for complacency. The threat of transnational terrorism will be enduring. America needs a DHS that is well prepared for the long fight.

I. Management

Management of Operations

Findings. DHS represents a complex merger of many agencies, combined with a number of start-up activities and compounded by the lack of a pre-existing senior management team. The U.S. Government Accountability Office (GAO)[2] rated the management challenge facing the department as "high risk" and noted that the successful transformation of a large organization takes from five to seven years.

While DHS has made progress in rationalizing many basic operations, including finance, contracting, information technology, human resources, and grant management, many operations still lack adequate coordination. According to DHS's Office of Inspector General (OIG), the department remains a "collection of separate components operating under a common organizational umbrella."

The Undersecretary for Management adds an unnecessary layer of bureaucracy. Other key management officials—the Chief Financial Officer (CFO), the Chief Information Officer (CIO), and the Chief Procurement Officer (CPO)—who report to the undersecretary also lack effective department-wide authority. In the private sector, chief management officers such as a CFO or a CIO report directly to the company's top executives, the chief executive officer or the chief operating officer (COO). Some federal agencies such as the Department of Energy follow this model. However, DHS does not.

Recommendations. The DHS Deputy Secretary should be invested with powers and responsibilities similar to those of a COO, and this role should be codified.

The authority of the management directorate should be strengthened. Options for accomplishing this include moving management responsibilities into the Office of the Deputy Secretary or having the department's CFO, CIO, and CPO report directly to the secretary through the deputy secretary as proposed in the House version of the 2005 Homeland Security Appropriations Bill.

Clear policies and procedures must be established to ensure that the CFO and CIO comply with the requirements in the CFO Act and the Clinger–Cohen Act. These two acts aim to increase federal government efficiency, primarily through improving financial, acquisition, and information technology management practices.

Policy Formulation and Implementation

Findings. The DHS Secretary currently lacks a policy apparatus with which to lead the development of proactive, strategic homeland security policy, let alone do anything beyond "managing by the in-box" and responding to the crises of the day. DHS also currently lacks a high-level policy officer with the staff, authority, and gravitas to articulate and enforce policy guidance throughout and across the department. DHS needs a more substantial capability to provide guidance for integrating current efforts. When DHS was formed from dozens of existing U.S. government agencies and programs, it absorbed several legacy policy analysis units from its component agencies. In addition, the patent need for policy analysis led some DHS components to form their own small policy analysis units. The proliferation of policy centers within DHS has only magnified the challenge of forging coherent guidance.

Recommendations. DHS should establish a unified policy planning staff headed by an Undersecretary for Policy who would report directly to the secretary via the deputy secretary. The undersecretary would serve as the secretary's chief policy official within the department. The responsibilities of the Undersecretary for Policy should be established by law and should include:

2. Formerly the U.S. General Accounting Office.

1. Coordinating DHS policy. The undersecretary would establish and direct a formal policymaking process for the department and oversee a policymaking board.
2. Conducting long-range policy planning. The undersecretary's staff would conduct long-range strategic planning, including "what if" scenario-based planning—a task that other DHS components invariably neglect as they grapple with daily crises and other pressing short-term demands.
3. Preparing critical strategic documents, such as a national strategy for preventing terrorists from entering the United States. The undersecretary's office would help to compose the department's most important documents.
4. Conducting program analysis. The undersecretary would assist with DHS programming. In particular, the undersecretary's analysts would evaluate ongoing and proposed programs (including planned research and development efforts) in terms of overall DHS priorities and resources.
5. Preparing net assessments. The undersecretary's planners would conduct periodic net assessments and research specific issues of interest to the secretary and other DHS leaders that cut across the department's components or for which the leadership desires another opinion.

Human Capital Management (Personnel Programs)

Findings. Beyond the numerous pressing short-term operational priorities, the department faces serious long-range challenges, including the development of a common vision, culture, and management philosophy that are necessary to align and integrate all the discrete parts of the organization. This means not only meshing the diverse operations and functions of those component parts, but also developing a new and fundamentally different leadership culture within the department: a challenge equal in magnitude—and importance—to all the immediate priorities facing DHS. Such an integration of vision and purpose is imperative if DHS is to realize its massive agenda.

Similarly, retaining and attracting the best personnel is one of the toughest challenges faced by organizations in the midst of reorganization and transition. During significant organizational change, productivity and morale suffer, as does cooperation among employees, particularly from different parts of an organization. DHS is no exception. For example, in the first year of DHS operations, turnover among divisional CIOs was 45 percent. Personnel turbulence within the Border and Transportation Security Directorate was also significant. Further, an August 2004 report from the Office of Management and Budget (OMB) found that DHS needed to reduce talent gaps in mission-critical positions.

Recommendations.

- Establish an executive leadership program. Higher priority must be given to establishing leader and personnel development programs for a more homogeneous and unified workforce across the department, both in terms of building a shared DHS culture and in developing the skills and attributes required to deal with the challenges of the 21st century. The department needs something similar to the requirements established for the Department of Defense by the Goldwater–Nichols Act of 1986, which prescribed education, interagency and interdepartmental assignments, and skill levels for senior leaders.
- Continue to build and strengthen human resources. Congressional action may be required to further reform personnel regulations to include management and skills-based education; and career incentives and rewards that support internal department "cross fertilization," interagency operations, innovation, and rewards for non-standard career paths that benefit the department.
- Develop innovative means to attract the right people. Institute a program of undergraduate and graduate scholarships that creates a pool of professional recruits from multiple disciplines. The program might be roughly modeled on the Department of Defense's Reserve Officer Training Corps program.
- Establish an aggressive mid-grade and senior-grade recruitment program to attract talent from the private sector.

- Create a manpower "float" that allows all agencies of the department to institute long-term education programs in support of DHS professional development goals.
- Enact regulations that hold sub-department agencies and leadership responsible for specific personnel goals and performance criteria.

International Affairs

Findings. The global networks that sustain our economy and foster our way of life—e.g., transportation, energy, communications, and finance—can be exploited by terrorists to attack us at home. In addition, adversaries could attack these globally integrated networks directly, causing major disruptions in the global economy. "Homeland" security activities in many areas—including ports and cargo, aviation, public health, visa and passport standards, and consular affairs—do not stop at America's geographic borders and really must be viewed as "international" security activities. Such activities necessarily involve diplomatic intelligence, information sharing, and other cooperative activities within foreign countries.

Although DHS has established an Office of International Affairs (OIA) to set strategic direction for the department's international activities, DHS international efforts remain fragmented among multiple offices, including the OIA, the Border and Transportation Security's (BTS) Policy Office, and other agency policy and operational activities within Immigration and Customs Enforcement (ICE), Citizenship and Immigration Services (CIS), Customs and Border Protection (CBP), and the U.S. Coast Guard.

Because of this fragmentation (which reflects DHS's overall incomplete integration), DHS is unable to present a unified effort and presence overseas. As a result, DHS remains disenfranchised from the foreign policy apparatus. Within embassies, DHS presence is ad hoc and its role, mission, and relationship with the rest of the embassy is unclear. Foreign governments that share security interests with the U.S. may fail to build effective partnerships because of the lack of a clear path to partnership. DHS is poorly represented among important international organizations, including the European Union and the Organization for Security and Cooperation in Europe, which could play extremely helpful roles in homeland security.

Recommendations.

- Reorganize responsibilities for international affairs in the secretariat.
- Eliminate redundancy of roles between the Chief of Staff's office and the OIA.
- Realign all DHS-wide international policymaking activity under an undersecretary.
- Convert the position of OIA Director to an assistant secretary under the Undersecretary for Policy.
- Clearly delineate the key responsibilities of the Assistant Secretary for Policy (International Affairs). They should include: (1) coordinating policy regarding international activities among DHS agencies; (2) coordinating international visits of the secretary related to protocol issues, and (3) ensuring DHS representation in dealing with international institutions, including the United Nations, NATO, the EU, the International Maritime Organization, and the World Customs Organization.

Integrating Operations with Non-Federal Entities

Findings. It is improbable that a catastrophic terrorist attack would affect only a single city or that a single city would be sufficiently prepared to mount a sufficient response. At a minimum, response efforts would likely require mutual aid from multiple jurisdictions. Despite this, DHS lacks an effective regional structure to facilitate coordination with state and local governments and with the private sector. Although efforts such as the National Response Plan and the National Incident Management System are providing a framework for this activity, DHS still lacks a suitable operational structure to support them.

The Homeland Security Advisory System (HSAS) is an important component of the intelligence and early warning mission area. The HSAS employs a series of color codes to designate various levels of national preparedness in

anticipation of a terrorist attack. Associated with each threat condition are a range of suggested protective measures—such as implementing various contingency plans—with federal, state, and local agencies responsible for developing and implementing their own specific response activities.

Application of the HSAS to state and local governments, as well as to the private sector and the American public, is problematic. A survey of various state and local response organizations conducted by the Gilmore Commission showed overwhelmingly that these organizations want more information on the type of attack, where it is likely to occur, and when. Currently, few organizations have the classified intelligence and the sophisticated analytical capabilities to evaluate threats. Without concrete assessments, many states, counties, and cities typically react in two ways: doing nothing or piling on layers of possibly unneeded security that generate exorbitant overtime costs and other expenditures.

Of even greater concern is the impact of shifts in the threat level on average citizens. Many appear perplexed by changes in threat condition. In short, the current national homeland security advisory system is inadequate.

Recommendations.

- Consolidate DHS critical infrastructure protection, preparedness, and state/local/private coordination efforts under an Undersecretary for Protection and Preparedness. This would consolidate the following agencies, components, and authorities: (1) the Infrastructure Protection component of the Information Analysis and Infrastructure Protection Directorate; (2) the Office of State and Local Government Coordination and Preparedness; (3) the non-operational transportation infrastructure protection mission of the Transportation Security Administration (TSA); (4) the "preparedness" piece of the Emergency Preparedness and Response Directorate; (5) the private sector preparedness mission of the Office of Private Sector Liaison; and (6) DHS grantmaking authority. Consolidating these disparate efforts would provide the DHS Secretary with a stronger platform from which to lead national efforts, determine priorities, identify critical vulnerabilities, work with state/local/private sector entities on securing those vulnerabilities and preparing for attacks, and make grants to help get the job done and to induce cooperation.
- Construct a DHS regional structure. The first priority of this regional organization should be to support the flow of information and to coordinate training, exercises, and professional development for state and local governments and the private sector. The regional structure's key operational mission would be to support preparedness, response, and critical infrastructure protection. DHS regional directors should not have authority over existing DHS agencies (such as the Coast Guard or Customs and Border Protection Bureau). On the other hand, consolidation of support activities and facilities would be appropriate under the regional structure where it is apt to garner efficiencies or cost savings. The Federal Emergency Management Agency (FEMA) should remain an independent agency responsible for coordinating federal response to natural and man-made disasters, including terrorism.
- Enhance the Homeland Security Advisory System. The national alert to state and local governments should be replaced with regional alerts and specific warnings for different types of industries and infrastructure. This will become easier once the Department of Homeland Security completes its comprehensive risk-level ranking of all areas in the country. Hopefully, the ranking will address criteria such as population, threat assessment, number of important sites, and level of vulnerability, and then classify each area as low, medium, or high risk. In addition, DHS must establish capabilities-based performance standards of preparedness and response for state and local authorities. National performance standards will provide a guide to help state and local governments determine what they need to do to counter terrorist threats and what help they should expect from the federal government.

II. Roles and Missions

Border, Immigration, and Transportation Security

Findings. Prior to the creation of DHS, seven agencies (among others) were involved in securing U.S. borders, enforcing immigration laws, and securing the transportation system: the U.S. Customs Service, Immigration and Naturalization Service (INS), Executive Office of Immigration Review, Bureau of Consular Affairs, U.S. Coast Guard, TSA, and Animal and Plant Health Inspection Service (APHIS). Agency missions overlapped to greater or lesser extents, and because the agencies resided in different Cabinet departments, it was difficult to resolve operational and policy conflicts without open turf warfare or resorting to the cumbersome interagency process.

The creation of DHS was supposed to consolidate agencies with overlapping missions and to better integrate our efforts in this area. It has succeeded to some degree. INS has been abolished, and its border inspectors and Border Patrol Agents have been merged with most of U.S. Customs and the border inspectors of APHIS to create U.S. Customs and Border Protection—a single uniformed face at our borders.

However, in "consolidating" responsibility for border, immigration, and transportation security, DHS actually increased the number of involved agencies to eight and created additional problems that now need solving. In addition, it has failed to clearly delineate the missions of DHS agencies that also have border, immigration, or transportation security responsibilities.

Additionally, the split of responsibilities between the CBP and ICE was done without a compelling reason—other than the vague (and ultimately incorrect) descriptive notion that the Customs and Border Protection would handle "border enforcement" and ICE would handle "interior enforcement." Indeed, in various interviews, not one person has been able to coherently argue why the CBP and ICE were created as separate operational agencies. Indeed, some have compared it to deciding to break up the New York Police Department into two separate agencies—one housing the uniformed "beat cops" (analogous to the CBP's uniformed officers) and the other housing the detectives (analogous to ICE's plain-clothes investigators).

Complicating the border security picture is the unclear mission of the TSA. While most Americans associate TSA with baggage screeners at airports, the Aviation and Transportation Security Act that created TSA also makes it responsible "for security in all modes of transportation," including ensuring the "adequacy of security measures for the transportation of cargo." This has injected TSA into the realm of border security and created friction with other DHS agencies historically in charge of securing the movement of cargo into the United States—the Coast Guard and CBP. The BTS has not been particularly effective in clearly delineating the relative responsibilities of the CBP and TSA (and it has no authority over the Coast Guard), resulting in policy impasses such as the fights about who is responsible for moving forward on "smart" containers and who is in charge of such programs as Operation Safe Commerce.

Under the Homeland Security Act, responsibility for ensuring that terrorists do not obtain visas to enter the United States is shared by DHS and the State Department's Bureau of Consular Affairs. This has led to a significant turf struggle. Indeed, the process of negotiating a memorandum of understanding between the State Department and DHS delineating their respective responsibilities took over one year. Additionally, there has been policy paralysis, even as many observers have viewed post-9/11 U.S. visa policy as a disaster—with security trumping all other objectives and deterring many individuals who present no threat from seeking to come to the U.S. or tying them up in excessive bureaucratic delays. The problems associated with post-9/11 visa policy—because of their impact on economic, diplomatic, academic, and scientific exchanges—have the potential to undermine long-term security interests.

Recommendations.

- Rationalize border security and immigration enforcement by merging the CBP and ICE, eliminating the Directorate of Border and Transportation Security. BTS has neither the staff nor the infrastructure to integrate the operations of the CBP and ICE on a consistent basis outside of the occasional task force, such

as the Arizona Border Control Initiative. Nor does it have a policy operation with sufficient influence with the secretary to resolve policy conflicts. Merging the CBP and ICE will bring together under one roof all of the tools of effective border and immigration enforcement—Inspectors, Border Patrol Agents, Special Agents, Detention and Removal Officers, and Intelligence Analysts—and realize the objective of creating a single border and immigration enforcement agency. This reform could be accomplished by executive decision, without the need for legislative action.

- Eliminate the BTS. With the merger of the CBP and ICE into a single agency, there is no need for the BTS middle-management layer. All operational agencies should have a direct reporting relationship to the secretary via the deputy secretary. This will allow for a better, DHS-wide (including the Coast Guard) policy and operational strategic approach to border security matters.
- Consolidate the U.S. Visitor and Immigrant Status Indicator Technology program (US-VISIT) program office into the merged border agency. Currently, the US-VISIT program is run by a stand-alone office in the BTS.
- Refocus and rename the TSA. The TSA should be solely an operational agency with no oversight or infrastructure protection policy functions. The agency should focus on overseeing DHS deployments protecting elements of transportation infrastructure deemed to be of national importance. The most prominent such deployment is currently the TSA screeners at airports, but one could imagine TSA officers deployed to other key transportation nodes if required. Restructuring the TSA's mission would eliminate the policy and regulatory conflicts with CBP and the Coast Guard.
- Responsibility for non-operational transportation infrastructure protection oversight should be in the DHS secretariat. There is no reason to separate transportation infrastructure protection from other types of critical infrastructure protection oversight, state/local/private coordination, and DHS grantmaking.
- Consolidate responsibility for visa operations within a single federal agency. Splitting responsibility for visa issuance and management between DHS and the State Department was a mistake. Operations could be managed more efficiently under one department and would place responsibility and accountability in one place. The choice is difficult. Arguably, the State Department is better positioned to consider the diplomatic, economic, and cultural issues at stake in issuing visas. On the other hand, if DHS were responsible, it would be better able to seamlessly integrate visa management into its other border control responsibilities and coordinate visa operations with its other international responsibilities.

Critical Infrastructure Protection, Preparedness, and Response

Findings. The vast majority of the nation's critical infrastructure is in private, state, or local hands. Likewise, most preparedness efforts are being undertaken by state, local, and private sector entities without federal leadership or control. However, a key and unique DHS mission is leading national—not just federal—efforts to protect critical infrastructure, prepare for possible attacks and other emergencies, and respond to catastrophic incidents such as the 9/11 terrorist attacks.

However, the DHS Secretary's ability to lead is hampered not only by the absence of an Undersecretary for Policy, but also by the fragmentation of key responsibilities among nine entities, both within and outside of DHS:

The DHS Emergency Preparedness and Response Directorate (EP&R) is primarily FEMA, but it also includes certain efforts to coordinate with state, local, and private entities in preparing for disasters, including terrorist attacks.

The Infrastructure Protection (IP) piece of the DHS Information Analysis and Infrastructure Protection Directorate (IAIP) identifies critical infrastructure warranting protection, prioritizes efforts, and works with state, local, and private entities to secure this infrastructure. Within the IP sub-directorate is the office in charge of cybersecurity.

The Office of State and Local Government Coordination and Preparedness in DHS is the product of merging the Office of State and Local Coordination and the Office of Domestic Preparedness. It works with state and local governments on identifying needs, coordinating efforts, and doling out DHS grant money for critical infrastructure protection and preparedness.

The Transportation Security Administration. TSA is primarily responsible for aviation security.

The Coast Guard, in addition to its operational responsibilities, is responsible for protecting seaports through risk assessments, reviewing facility security plans, developing Area Maritime Security Plans, coordinating Area Maritime Security Committees, and facilitating Port Security Grants with the Maritime Administration. The Coast Guard also has Strike Teams and Maritime Safety and Security Teams to respond to incidents at ports.

The Office of Private Sector Liaison has primarily been an ombudsman for private efforts to influence DHS policy in various areas, but it conceivably could be a forum for working with the private sector on critical infrastructure protection and preparedness for attacks.

The DHS Science and Technology Directorate Office of WMD Operations and Incident Management is a new office within the Science and Technology Directorate and is intended to provide rapid scientific and technical expertise and decision making in response to weapons of mass destruction (WMD) attacks and incidents.

The Assistant Secretary for Public Health Emergency Preparedness in the Department of Health and Human Services (HHS) and the *Centers for Disease Control and Prevention* also play a part. These agencies outside DHS are central to our ability to prepare for and respond to a bioterrorism attack.

The Department of Energy Nuclear Response Teams provides lead federal response to radiological incidents.

The fragmentation of the U.S. government's leadership efforts into all these discrete—and often competing—agencies has hampered the effort. While we do not recommend transferring outside agencies into DHS given the important interrelationships with their home departments (e.g., the interrelationship between the HHS Assistant Secretary for Public Health Emergency Preparedness with broader public health issues), we do advocate—at a minimum—further consolidations within DHS to unify and focus DHS efforts and to enable the secretary to work effectively with other departments on the critical national priorities of securing critical infrastructure, preparing for terrorist attacks, and responding to them.

Recommendations.

- As much as practicable, consolidate DHS response missions into FEMA and strengthen that agency. FEMA should be engaged squarely in its traditional role of planning for the national (not just federal) response to emergencies—including terrorist attacks—and then implementing them where necessary.
- Eliminate the EP&R. Both the proposed Undersecretary for Protection and Preparedness and FEMA should report directly to the secretary via the deputy secretary. As with the BTS, consolidating operational efforts renders the middle-management directorate layer unnecessary. A "flatter" structure is preferable here and will better enable the secretary to exercise leadership. It will be important for the secretary to ensure close coordination between the Undersecretary for Protection and Preparedness and FEMA because the nation's "preparedness" and "response" efforts are clearly interrelated and require coordinated leadership.

Intelligence Analysis

Findings. The Homeland Security Act created the DHS Intelligence Analysis and Infrastructure Protection Directorate and envisioned that it would serve as the nation's mechanism for fusing all foreign and domestic intelligence relating to potential terrorist threats against the homeland, consolidating all of the disparate terrorist and law enforcement watchlists, and generally "connecting the dots" needed to prevent another attack—correcting a problem seen as contributing to the 9/11 tragedy.

However, this role has not developed as envisioned by the act. Instead, after a significant period of bureaucratic competition among the DHS, CIA, and FBI, the President established the Terrorist Threat Integration Center (TTIC) to perform the task of "connecting the dots" and facilitating the sharing of intelligence among federal agencies under the direction of the Director of Central Intelligence with the DHS and FBI serving as deputy directors. In a subsequent executive order, Homeland Security Presidential Directive 6, the President created the Terrorist Screening Center (TSC) and established it as a mechanism for consolidating the watchlists. The TSC is also an interagency activity, but it operates under the FBI with DHS serving in a deputy role.

By creating the TTIC and TSC, the President diminished the importance of the IAIP's intelligence fusion role. The DHS Assistant Secretary for Information Analysis now plays a much less significant role than originally envisioned by Congress. His current roles are: (1) serving as the DHS Secretary's intelligence advisor; (2) coordinating the intelligence and information analysis components within DHS, including those resident in the agencies; (3) serving as DHS's voice to the intelligence community, including the TTIC and TSC; and (4) ensuring that the TTIC and TSC are adequately staffed with DHS personnel. DHS also has a significant operational role in analyzing information to determine targets for greater scrutiny. Indeed, this is the key mission of the National Targeting Center (NTC), which is currently run by U.S. Customs and Border Protection and which works closely with the IAIP, TTIC, and TSC.

The National Commission on Terrorist Attacks Upon the United States (the "9/11 Commission") recommended the creation of a National Counterterrorism Center (NCTC), which would serve under a National Intelligence Director and be responsible for coordinating all domestic and foreign counterterrorism operations. Legislation proposed by the U.S. House and Senate calls for implementing this measure and placing the TTIC within the NCTC. This initiative may serve to further marginalize the intelligence integration function of DHS and its capacity to represent the terrorism intelligence "consumer" community, including its subordinate agencies and a host of state, local, and private sector entities.

Recommendations. DHS should have a chief intelligence officer whose responsibilities include: (1) acting as the secretary's principal intelligence advisor and providing integrated analysis for the department and wider homeland security community; (2) disseminating and incorporating intelligence into other DHS components; (3) receiving, integrating, and disseminating intelligence and threat warnings to the private sector and state and local governments; and (4) representing the secretary to the intelligence community.

Placement of the TTIC should be carefully considered. There is a strong consensus that the nation requires a greater capacity to share and compare intelligence regarding terrorism. Clearly, the TTIC has a critical role to play in accomplishing this task. For the TTIC to accomplish this mission it must have both the authority of the President and the ability to tap the resources of all federal agencies. In addition, it must be able to draw on information and expertise from state and local governments and the private sector and equitably serve the needs of all these constituents. These factors need to be weighed carefully in deciding whether the nation would be better served by having the TTIC (while remaining an interagency activity) report to the DHS Secretary and work closely with the TSC, the NTC, and ICE's Law Enforcement Support Center or by making the TTIC part of the NCTC supporting global operations against terrorism.

At its core, the TTIC's mission should be: (1) analyzing domestic and foreign intelligence and law enforcement information to identify potential threats to the homeland; (2) communicating that information to law enforcement and other prevention agencies (many of which are housed in the DHS); and (3) warning the public. There may be other missions envisioned—and these activities are vital to supporting the missions of other agencies—but they are all also central to DHS's intended mission.

III. Authorities

Department Oversight

Findings. Congress has not consolidated oversight of DHS's homeland security functions into single committees in the House and Senate. The final report of the 9/11 Commission reaffirmed the importance of fixing congressional oversight. The commission held that:

> Congress should create a single, principal point of oversight and review for homeland security. Congressional leaders are best able to judge what committee should have jurisdiction over this department [DHS] and its duties. But we believe Congress has the obligation to choose one in the House and one in the Senate, and that this committee should be a permanent standing committee with a nonpartisan staff.

As the report also noted, one expert witness appearing before the commission testified that the lack of effective congressional oversight is perhaps the single greatest obstacle impeding the successful development of DHS.

The creation of various oversight offices within DHS, including a Privacy Office and an Office for Civil Rights and Civil Liberties, is a positive step. However, the functions of DHS, and their coordination and interaction with other homeland security and national security entities, require a more robust and less conventional oversight function than currently exists. Oversight and transparency lend credibility to the exercise of homeland security authorities and instill confidence in the American people. Conversely, without strong oversight, even well-intended initiatives and programs may be weakened or discontinued out of suspicion, ignorance, and lack of credibility with the public. This is especially the case with intelligence collection, intelligence analysis, and information sharing initiatives and activities for homeland security.

Recommendations.

- Create a more robust oversight structure for homeland security, beginning with an effective, rationalized, and consolidated oversight and authorization committee structure in Congress and an enhanced recommitment to intelligence oversight on the part of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence. Oversight should not only protect against abuse, but should also ensure efficiency and effective interagency processes in areas such as information sharing and technology development.
- Inculcate a culture of self-oversight through best management practices, with regular training for line officers on regulations and limitations of authority, utilizing lessons learned and best practices from agencies that have a long, successful history of legal compliance, such as the National Security Agency.

The chief focus of oversight should be to conduct regular audits and periodic reviews of ongoing activities, rather than after-the-fact investigations. As the nation builds the substantive homeland security regime, we must also develop a worthy oversight regime, clarifying oversight mechanisms and determining the appropriate mix of congressional, judicial, administrative, and inspector general oversight.

Specialized offices such as civil liberties boards and privacy officers ought to be reviewed for effectiveness and redundancy. Overseers must review and seek improvements not only in the internal functioning of DHS and other agencies, but also in their interaction with each other—particularly in information sharing, areas of joint or overlapping responsibility, and dealing with unstructured, fluid situations such as cyberattacks and bio-attacks.

Information Sharing and Technology Development and Acquisition

Findings. There exists an intricate, distributed, but necessary web linking the flow of information from intelligence collection and aggregation to analysis and, ultimately, to sharing with appropriate policymakers and security officials. This web is built upon, and sustained by, a mosaic of enabling technology that is integrated into a network

to enhance information sharing. The homeland security community has a fragmented and inadequate process to ensure that technological innovations develop alongside the changes in policy, privacy protection, and oversight that are made necessary by these technological innovations. This gap between technology and appropriate policy structures leads to missed opportunities in homeland security technologies, because promising new technologies are not pursued as aggressively as they might be out of concern for their impact on privacy and civil liberties.

DHS lacks adequate authorities and mechanisms to clarify how the development of controversial new technologies and the development of democratic controls over their use should proceed side by side. The department is missing the capacity to evaluate the intrusive effects of data mining and data aggregation and how they can be mitigated by privacy protection (e.g., anonymization and judicially managed access to identities), guidelines and standards, oversight, and technology to reduce the risk of abuse (e.g., immutable audit trails and strong access and authentication controls). The department also lacks the capacity to efficiently issue appropriate guidelines to ensure that technologies are used appropriately.

It is critical to move forward with developing capabilities and mechanisms for information sharing. This development must proceed hand-in-hand with crafting policy guidelines for information sharing. For example, technology development should be informed by clear policy about necessary predicates for and restrictions on access to sensitive information, controls on retention and dissemination, and requirements for authentication and auditing. Other critical policy questions include determining how private sector information can be accessed and used. DHS should have clear legislative mandates to address these issues.

Recommendations. The federal government must create a process to couple innovations in technology with innovations in law, so that we neither deny ourselves opportunities in homeland security technologies nor erode civil liberties and economic progress. This process must work across all research and development agencies and operational agencies of the government and involve the appropriate congressional overseers.

DHS needs to serve as the lead advocate for funding promising technologies for homeland security and for the development of these technologies in ways consistent with the requirements of civil liberties, privacy protection, and economic efficiency. As new technologies are funded and developed, DHS needs to take the lead—in advisory committees or in insertion of ongoing and milestone legal and policy reviews within technology programs—in identifying, evaluating, and addressing head-on the potential policy and legal problems of technologies. DHS should also work with other agencies, Congress, and appropriate outside experts to provide guidance on how best to prototype, test, and implement these technologies in tandem with the safeguards and standards that should accompany their use.

Protection of Sensitive, but Unclassified Information

Findings. Improving information sharing is critical, but here it is necessary to strike the right balances in sharing information with or withholding information from the public. Policies that are either overly neglectful or overzealous ill serve efforts to enhance homeland security. For example, the discovery on al-Qaeda hard drives of information on critical infrastructure vulnerabilities, bomb making, and other potentially dangerous information downloaded from open websites caused the U.S. government to rethink its policies on information published on government websites. Some agencies responded by withdrawing virtually all information from their public websites. Others have seriously curtailed the amount of useful information or public access to unclassified information that is available from sources other than their websites. At the very least, such wholesale withdrawal of information seems arbitrary and undermines important values of government openness, the development of electronic government (e-gov) to speed the delivery and lower the cost of government services, and public trust.

The Homeland Security Act contained a requirement for regulation of Protected Critical Infrastructure Information (PCII). That regulation was finalized in spring 2004, and DHS now has a PCII office. This effort addresses only some areas of sensitive information. It is not sufficiently comprehensive.

The process for classifying secret information in the federal government is disciplined and explicit. The same cannot be said for unclassified but security-relevant information for which there is no usable definition, no common understanding about how to control it, no agreement on what significance it has for U.S. national security, and no means for adjudicating concerns regarding appropriate levels of protection. To date, there has been no systematic

review of what government information that is now or was formerly in the public domain could be used as a "terrorist roadmap," the likelihood of such a threat, the role that such information would play in terrorists' preparation (including possibilities of alternative sources of the same information), and the countervailing public safety and other benefits of providing different types of information. Furthermore, no authority is clearly designated to make these evaluations at a national policy level. Current evaluations are conducted at the departmental level at best or on an ad hoc, office-by-office basis. Nor has DHS provided any leadership or guidance to the private sector about how the private sector might develop voluntary standards for making decisions about its own disclosures of sensitive information, even without governmental restrictions. For government decisions, there is no single designated authority—in the Office of Management and Budget or elsewhere—for determining the overall policy interests and objectives of information distribution, including common baseline standards to help weigh the benefits and risks of providing the public with specific types of information, regardless of which agencies possess the information. Such a single authority might act as the overall reviewer of agencies' public disclosure policies and their implementation of these policies.

Recommendation. There must be consistent policy and legislation that encourages the sharing of unclassified but security-relevant information between the private sector and the government. This policy must be sensitive to the public benefit of openness and should not unnecessarily remove information from public access. A clear and balanced policy on disclosure would also address private sector fears of business losses due to public disclosure of proprietary information (e.g., through error, court documents, and public security announcements), of liability for disclosure, and of private citizens' fears of inappropriate and overreaching government secrecy.

Clarification of Authorities for Critical Missions

Findings. DHS is an amalgamation of several new and previously existing entities, each with its own organic authorities and regulations. Seams and overlaps in roles, missions, and authorities still exist. Some agencies have overlapping missions, while other missions remain unassigned or unclaimed by specific agencies. Three areas are of particular concern: (1) cyberattack, (2) incidents and attacks involving biological agents and toxins, and (3) activities within the intelligence community.

It is not apparent that DHS has sufficient authorities to meet its assigned responsibilities under the National Strategy to Secure Cyberspace. Nor is it clear who would be in charge of the response to a cyberattack on the United States, what kind of response would be legally authorized, and what authorities would be required in different scenarios of detection, verification/validation, attribution, response, and reconstitution or recovery. It is also not apparent what process would be followed to coordinate investigative steps and responses among agencies and to assign roles and authorities as factual information about the attack emerges. Elements of the National Infrastructure Protection Center transitioned to DHS. At the FBI, these watch, warning, and training elements worked closely with law enforcement agents. At DHS, the role of these elements in a cyberattack is uncertain. The Secret Service, which investigates computer fraud and computer-based attacks on the financial system, is another important element of DHS's cyber-related capabilities.

It is also unclear which agency would have primary responsibility for responding to a biological attack on the United States, which DHS office would lead its operational bio-response (whatever that would be), and whether federal agencies would support or take the lead in supporting a state or local response to a bio-attack. In part, this confusion results from the fact that the agencies with the primary legal authorities and expertise in bio-defense—such as the Department of Health and Human Services (Public Health Service, Centers for Disease Control, National Institutes of Health, and Office of the Secretary of HHS), the Department of Agriculture, and DOD—have responsibilities that transcend homeland security (e.g., public health, epidemiology, and national defense). Thus, the authorities for bio-defense response are neither well-coordinated nor harmonized.

DHS's legal authorities and responsibilities as a member of the intelligence community are unclear. For example, it appears that the department has sufficient authority to accomplish effective information sharing. However, it needs new authorities for a career intelligence service and in support of counterintelligence operations, as well as new dissemination guidelines. Lack of clarity also permeates the roles and missions of DHS within the intelligence community, both as a producer of intelligence and as a consumer of intelligence.

Recommendations. Authorities and national leadership roles for bio-defense, cyberdefense, and critical infrastructure protection need to be clarified by establishing and empowering lead federal executives. The issue of DHS authorities to prepare and respond to cyberattacks requires additional discussion. Clarification of the department's role, in turn, should be reflected in future changes in the roles, missions, and management of the department. Currently, it is unclear which federal agency should lead the response to a cyberattack, given that there are many capabilities for detection and response throughout several federal agencies, including the DHS, Department of Justice, DOD, and intelligence community, as well as in the private sector.

In general, greater consolidation of authorities for bio-defense and medical responses to catastrophic terrorism would likely result in a more efficient and coordinated federal response. Where possible, authorities over national medical response programs such as the Metropolitan Medical Response System and the National Disaster Medical System should be harmonized and coordinated under DHS direction with substantial input from HHS, which has greater expertise and experience in these issues as well as long-standing relations with relevant stakeholders.

The DHS intelligence entity must have well-defined authorities and the legal instruments to accomplish its missions in the intelligence community. These missions include not only DHS as a consumer of intelligence, but also as a disseminator of intelligence to federal, state, and local authorities.

Congress and the executive branch need to make a significant effort to reconcile the information sharing needs of DHS with existing law on sharing information (e.g., the Privacy Act, the USA PATRIOT Act, and classification rules).

Watchlists, Profiling, and Policies for Information Protection

Findings. Although the Homeland Security Act and Homeland Security Presidential Directives 6 and 11 provide clear guidance for managing watchlists, there is inadequate guidance and effort in establishing standards for profiling, composition and consolidation of terrorist watchlists, avenues of recourse for persons who wish to challenge their placement on a watchlist, and review of the government's use of watchlists. First, in view of the significance of terrorist watchlists and the harm to an innocent individual who is erroneously placed on such a list, there is a necessity for government-wide guidance on constructing these lists comprehensively and accurately. Second, there is also a compelling need for an appropriately transparent procedure by which an individual who alleges that he or she has been erroneously placed on the list may contest and overturn the listing. At the same time such a procedure must be sufficiently rigorous and discerning that it prevents efforts by terrorists to remove themselves from watchlists.

In addition, there is insufficient clarity about when and how profiling (singling out certain persons for heightened scrutiny or other actions) is authorized and appropriate. Issues that have not been adequately addressed include: What are the necessary authorities to support profiling? When can profiling be employed? What actions (e.g., further investigation or detention) can be justified by profiling? What standards and safeguards should accompany profiling? Should standards and safeguards differ depending on the mission and potential negative consequences of profiling? For example, should a higher standard be applied to using a profile to prohibit someone from boarding a commercial aircraft in the United States than to conducting a traffic stop to question truck drivers near a sensitive location? If profiling is used, how should it be informed by data mining and other information analysis techniques in addition to watchlists?

Recommendations. The federal government should accelerate its efforts to consolidate and police its watchlists. DHS should take the lead in implementing processes, enforced by authorities, to develop comprehensive and accurate watchlists. This must include authorities and processes to correct errors, configuration control to enhance utility and interoperability of information across agencies, and regular review and oversight. Laws or regulations should be developed specifying standards of proof, limitations on what information related to watchlists can be given to the individual of concern, and requirements to correct errors as they are adjudicated.

As part of the effort to enhance the integrity and value of watchlists, an adjudication process needs to be established with a neutral third-party decision maker operating with defined rules and standards—perhaps an administrative law judge—to oversee the review of lists and adjudicate claims brought by individuals who assert that they were erroneously placed on a watchlist. Similarly, DHS should take the lead in formulating standards for determining what kinds of heightened scrutiny or investigation are appropriate when an individual on a watchlist is identified.

IV. Resources

Authorization Process

Findings. The efficient use of federal resources requires an effective partnership between the executive and legislative branches. Although departments receive daily operational guidance from the executive, Congress has the constitutional responsibility to fund these departments and oversee their operations to achieve efficiency and accountability. Currently, Congress has not responded coherently to the challenge of overseeing DHS's allocation and use of resources. Even though separate appropriation subcommittees have been formed, there is no established process to authorize expenditures.

An authorization bill for DHS could serve as a critical statutory management tool by providing a means to exercise stronger oversight of important DHS activities, such as key personnel programs, performance of critical missions, major research programs, and information technology investments. In July 2004, the House Select Homeland Security Committee unsuccessfully attempted to markup a DHS authorization act.

Congress should reconsider the reauthorization process for the full scope of critical national security programs. Under current law, Congress must pass a Department of Defense authorization bill every year. Historically, this has been appropriate because national security was focused solely on defeating America's enemies overseas. However, 9/11 made it abundantly clear that security at home is equally vital. The magnitude of these dual challenges underscores the need for Congress to pay equal attention to both missions. Homeland security is simply too important to be pushed to the legislative sidelines for years at a time. On the other hand, given the numerous "must pass" bills that Congress already faces each year, requiring passage of an annual DHS authorization bill might be too much.

Recommendations. Congress should legislate a Department of Homeland Security Authorization as envisioned by the House Select Homeland Security Committee. Establishing permanent homeland security committees in both the House and Senate with full jurisdiction over DHS would greatly facilitate this effort.

Congress should consider reauthorizing homeland security and defense spending biannually: Each Congress could pass a DOD authorization bill in one session and a DHS authorization bill in the other. Considering the demands facing Congress, biannual authorization bills would be a realistic approach to focusing lawmakers' attention and balancing oversight of DHS and DOD. Biannual bills would provide greater opportunity for the two departments to implement new congressional directives effectively while allowing Congress more time to evaluate how well the respective departments are implementing statutory guidance. They could also bring additional legislative stability and predictability to annual appropriations for the two departments.

Allocation of Grants

Findings. One of the great strengths of American democracy is the dispersion of power at every level of governance with the goal of allowing local citizens to have the most say in local decisions. Preservation of the principles of federalism must remain a key goal in creating an effective and sustainable homeland security regime. That means that each level of government and the private sector must fulfill its responsibilities.

The federal responsibility of providing financial resources to state and local governments remains a contentious issue. The first and highest priority for federal spending must be investments that assist in creating a true national preparedness system. Federal funding should focus on programs that will make all Americans safer. That includes providing state and local governments with the capability to integrate their counterterrorism, preparedness, and response efforts into a national system and expanding their capacity to coordinate support, share resources, and exchange and exploit information. The federal government must also help to build the capacity to respond to catastrophic terrorism—acts of violence so terrible and destructive that they exceed the ability of any state or local government to respond effectively.

However, there are no federal criteria for the minimum capabilities needed to protect an American community, no funding formula that is based on risk analysis and divorced from politics, and no funding system that can assure a sustained flow of funds for specified projects that are consistent with the real security needs of the community and national strategic priorities. Additionally, there is no legislative requirement for federal grants to be allocated in a manner that supports the national homeland security strategy.

As the 9/11 Commission reported, the current grantmaking process is in danger of becoming pork-barrel legislation. Allocation of most homeland security grants is established by a congressionally mandated formula. Current funding formulas guarantee each state 0.75 percent of the funds available. As a result, 40 percent of funds are immediately tied up, leaving only 60 percent for discretionary allocations. In this manner, in 2003, California received only 7.95 percent of general grant monies, even though the state accounts for 12 percent of the nation's population. Wyoming, which received 0.85 percent, accounts for only 0.17 percent of the population. This translates to $5.03 per capita in California and $37.94 per capita in Wyoming. Within states, rural, less populated areas often receive a disproportionate amount of money as well. Some states distribute funds equally among counties, resulting in amounts that are so small that it is difficult to imagine how they could be used productively. Even the Urban Area Security Initiative grants, monies targeted at major population areas that are also considered potential targets, produce curious results. Under the current formula, San Francisco (with a population of 800,000) and Los Angeles (with a population of 4 million) receive about the same amount of money.

Recommendations. The Department of Homeland Security should continue to implement Homeland Security Presidential Directive 8, which requires DHS to take the lead in rationalizing the funding of homeland security priorities and establishing a set of minimum essential capabilities for every American community so that state, local, and federal governments can work together to achieve these standards. Establishing national performance standards for preparedness is essential to evaluating readiness, determining priorities, and targeting investments.

Congress should establish risk-based funding formulas for port security, emergency responder, and other nonfederal grants that are consistent with the national homeland security strategy. For example, Congress could adopt the proposal in the Cox–Turner bill (Faster and Smarter Funding for First Responders Act, H.R. 3266) that guarantees states only 0.25 percent of funding rather than the current 0.75 percent and assigns the rest of the funds on a risk-based system. Title V of the 9/11 Recommendations Implementation Act (H.R. 10) contained a similar provision.

National Threat/Vulnerability Assessments

Findings. In the three years since the September 11 attacks, our nation has created the third largest bureaucracy in the federal government and spent close to $100 billion on efforts to secure the homeland from further terrorist attack. Yet we still have not completed a threat/vulnerability assessment that can help to develop strategy, set priorities, and guide spending in a targeted, sustainable manner for what will certainly prove to be a long-term conflict against terrorism.

With only limited resources available to achieve the almost limitless goal of protecting the entire United States against terrorist attack, it is critical that we set priorities. These priorities should be based on a comprehensive threat/vulnerability matrix that identifies which areas need the most protection and have the greatest urgency.

Many officials have recognized the need for such an assessment, and it has been promised for years. The latest DHS estimate is that such a study will be completed by 2008, but America cannot wait that long.

Recommendation. The Department of Homeland Security must assume strong leadership of this project and deliver a comprehensive threat/vulnerability assessment to America's top national security decision makers by December of 2006. It should be based on commonly accepted risk-assessment methodology. Spending and missions conducted by DHS could then be logically prioritized based on what is most vital to protect the nation.

Response to Catastrophic Terrorism

Findings. America is not sufficiently prepared to respond fully to a catastrophic terrorist attack on U.S. soil that involves chemical, biological, radiological, or nuclear (CBRN) weapons.

The 9/11 attacks made clear that the number of Americans our terrorist enemies seek to kill is limited only by the power of their weapons and not by the darkness of their imaginations. Current response capabilities for such an attack are scattered across the spectrum of state, federal, and local governments. For example, the U.S. military has some capability to respond in environments contaminated by a CBRN attack. However, these units are primarily trained for maintaining their missions in a battlefield environment rather than restoring order and providing relief in a major American city. Various state National Guards maintain Civil Support Teams, which are being trained for deployment in such hot zones, but the teams are new and are not able to respond nationally. The federal government maintains strategic stockpiles of vaccines at several locations, but the recent shortage of flu vaccine, the inability to mobilize rapidly and efficiently to deliver scarce vaccines to high-risk individuals, and the long gear-up timetable to meet the objectives of Project Bioshield should be causes for concern.

Protecting America from and responding to potential terrorist attacks that utilize weapons of mass destruction is clearly constitutionally mandated by the phrase "provide for the common defense." Only the federal government has the power, personnel, and resources to prepare and organize the massive response that would be needed to respond to the casualties and recover from a WMD attack on U.S. soil. The federal government must provide the means to scale the national response to meet terrorist threats up to—and including—catastrophic attacks.

Recommendations. Based on national risk assessments and a national survey of the capacity and readiness of assets across the country to respond to catastrophic terrorism, DHS should develop contingency plans that include national "response packages," allocations of resources that including regional (e.g., multi-state) and federal entities that would be available to respond to various types of emergencies, from natural to manmade. These response packages should be scalable, in sufficiently modular means so that they can be efficiently deployed to a range of disasters. If DHS determines that these response packages are inadequate, it should explore the feasibility of establishing a Homeland Security strategic reserve that will assemble additional response capabilities.

Border Security

Findings. The 9/11 Commission rightly singled out border security and terrorist travel as subjects of grave concern. Indeed, these represent a complex problem for protecting America at home. However, the challenges of border security are more than just securing the border. They cut across issues of foreign policy, economic development, immigration, internal enforcement, trade, maritime commerce, air travel, rail and ground transport, and border control. On land, at sea, and in the air, providing resources to meet U.S. security needs is a daunting task.

On land, over 1 million non-U.S. citizens illegally cross the U.S. border each year, circumventing U.S. immigration law and identity screening procedures. On the southern border alone, over 20,000 "other than Mexican" people from "countries of interest" (e.g., Pakistan, Iran, and Afghanistan) are detained each year for illegally crossing the U.S. border. Historically, they have been released if they promise to return for a hearing at a future date, but almost all disappear without a trace due to a lack of facilities and personnel.

At sea, the U.S. Coast Guard has been given additional roles in the wake of 9/11. The Coast Guard now must assess port security at hundreds of U.S. ports, monitor the voyages of thousands of foreign-flagged vessels into U.S. ports, and provide rapid response and boarding capability in case of potential danger. As the lead agency responsible for the security of America's shores and waterways, the Coast Guard has a tremendous new responsibility in the 21st century—however, its personnel levels and fleet have not dramatically changed in a generation.

In the air, security is best assured through the diligent and effective efforts of TSA screeners on the ground and air marshals on board passenger aircraft. However, the level of TSA screeners has dropped substantially, from 60,000 to 45,000, with no apparent reason provided for the drop except the will of appropriators on congressional committees.

Recommendation. DHS must conduct a national assessment of the resources required for effective border security, including all the layers of security that impact securing the border. This analysis should be used to help Congress and the Administration determine where to direct resources to ensure that funding is directed toward programs that provide the greatest contribution to supporting the critical border security mission

Task Force Participants

Task Force Co-Chairmen

James Jay Carafano
Senior Research Fellow for Defense and Homeland Security
Kathryn and Shelby Cullom Davis Institute for International Studies
The Heritage Foundation

David Heyman
Director and Senior Fellow, Homeland Security Program
Center for Strategic and International Studies

Participants

Scott Bates
Senior Policy Adviser
Select Committee on Homeland Security
U.S. House of Representatives

Christian Beckner
Fellow, Homeland Security Program
Center for Strategic and International Studies

Jonah Czerwinski
Director of Homeland Security Projects and Senior Research Associate
Center for the Study of the Presidency

James Dean
Deputy Director, Government Relations
The Heritage Foundation

Mary DeRosa
Senior Fellow, Technology and Public Policy Program
Center for Strategic and International Studies

Gerald L. Epstein
Senior Fellow, Science and Security
Homeland Security Program
Center for Strategic and International Studies

Jay Farrar
Vice President for External Affairs
Center for Strategic and International Studies

Brian Finch
Associate
McKenna Long and Aldridge, LLP

Reagan Fuller
Manager, Federal Government Relations
French and Company

Daniel Kaniewski
Deputy Director
Homeland Security Policy Institute
The George Washington University

Alane Kochems
Homeland Security Research Assistant
Kathryn and Shelby Cullom Davis Institute for International Studies
The Heritage Foundation

Ronald D. Lee
Partner
Arnold & Porter LLP

Terry Maynard
Independent Consultant

Lillian McTernan
Program Coordinator, Homeland Security Program
Center for Strategic and International Studies

Steve Metruck
Military Fellow, International Security Program
Center for Strategic and International Studies

Keith Miller
Research Assistant
Thomas A. Roe Institute for Economic Policy Studies
The Heritage Foundation

Ha Nguyen
John F. Kennedy School of Government
Harvard University

Kate Phillips
Research Associate, Homeland Security Program
Center for Strategic and International Studies

Neal A. Pollard
General Counsel
Terrorism Research Center, Inc.

Daniel Prieto
Research Director, Homeland Security Partnership Initiative
Harvard University

Rebekah Robblee
Kathryn and Shelby Cullom Davis Institute for International Studies
The Heritage Foundation

Paul Rosenzweig
Senior Legal Research Fellow
Center for Legal and Judicial Studies
The Heritage Foundation

David Schanzer
Select Committee on Homeland Security
U.S. House of Representatives

Seth M.M. Stodder
Senior Counsel
Akin Gump Strauss Hauer & Feld, LLP

Virginia Thomas
Director, Executive Branch Relations
The Heritage Foundation

Irvin Varkonyi
President
Supply Chain Operations Preparedness Education, LLP

Richard Weitz
Senior Staff Member
Institute for Foreign Policy Analysis

Anne Witkowsky
Senior Fellow, Technology and Public Policy
Center for Strategic and International Studies

Acronyms

APHIS: Animal and Plant Health Inspection Service
BTS: Border and Transportation Security
CBP: Customs and Border Patrol
CBRN: chemical, biological, radiological, or nuclear
CFO: chief financial officer
CIA: Central Intelligence Agency
CIO: chief information officer
CIS: Citizenship and Immigration Services
COO: chief operating officer
CPO: chief procurement officer
DHS: Department of Homeland Security
DOD: Department of Defense
EP&R: Emergency Preparedness and Response Directorate
EU: European Union
FBI: Federal Bureau of Investigation
FEMA: Federal Emergency Management Agency
GAO: Government Accountability Office (former General Accounting Office)
HHS: Department of Health and Human Services
HSAS: Homeland Security Advisory System
ICE: Immigration and Customs Enforcement
INS: Immigration and Naturalization Service
IAIP: Information Analysis and Infrastructure Protection Directorate
IP: Infrastructure Protection
NATO: North Atlantic Treaty Organization
NCTC: National Counterterrorism Center
OIA: Office of International Affairs
OIG: Office of Inspector General
OMB: Office of Management and Budget
PCII: Protected Critical Infrastructure Information
TSA: Transportation Security Administration
TSC: Terrorist Screening Center
TTIC: Terrorist Threat Integration Center
US-VISIT: U.S. Visitor and Immigrant Status Indicator Technology
WMD: weapons of mass destruction

Bibliography

Anderson, Philip, "Threat-Vulnerability Integration: A Methodology for Risk Assessment," Center for Strategic and Integration Studies *White Paper*, at *www.csis.org/isp/homeland_tvi.pdf* (November 12, 2004).

Bush, George W., Homeland Security Presidential Directive-1, "Organization and Operation of the Homeland Security Council," October 29, 2001, at *www.fas.org/irp/offdocs/nspd/hspd-1.htm* (November 24, 2004).

———, Homeland Security Presidential Directive-2, "Combating Terrorism Through Immigration Policies," October 29, 2001, at *www.fas.org/irp/offdocs/nspd/hspd-2.htm* (November 24, 2004).

———, Homeland Security Presidential Directive-3, "Homeland Security Advisory System," March 11, 2002, at *www.fas.org/irp/offdocs/nspd/hspd-3.htm* (November 24, 2004).

———, Homeland Security Presidential Directive-5, "Management of Domestic Incidents," February 28, 2003, at *www.fas.org/irp/offdocs/nspd/hspd-5.html* (November 24, 2004).

———, Homeland Security Presidential Directive-6, "Integration and Use of Screening Information," September 16, 2003, at *www.fas.org/irp/offdocs/nspd/hspd-6.html* (November 24, 2004).

———, Homeland Security Presidential Directive-7, "Critical Infrastructure Identification, Prioritization, and Protection," December 17, 2003, at *www.fas.org/irp/offdocs/nspd/hspd-7.html* (November 24, 2004).

———, Homeland Security Presidential Directive-8, "National Preparedness," December 17, 2003, at *www.fas.org/irp/offdocs/nspd/hspd-8.html* (November 24, 2004).

———, Homeland Security Presidential Directive-9, "Defense of United States Agriculture and Food," January 30, 2004, at *www.fas.org/irp/offdocs/nspd/hspd-9.html* (November 24, 2004).

———, Homeland Security Presidential Directive-10, "Biodefense for the 21st Century," April 28, 2004, at *www.fas.org/irp/offdocs/nspd/hspd-10.html* (November 24, 2004).

———, Homeland Security Presidential Directive-11, "Comprehensive Terrorist-Related Screening Procedures," August 27, 2004, at *www.fas.org/irp/offdocs/nspd/hspd-11.html* (November 24, 2004).

———, Homeland Security Presidential Directive-12, "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004, at *www.fas.org/irp/offdocs/nspd/hspd-12.html* (November 24, 2004).

———, National Security Presidential Directive-17/Homeland Security Presidential Directive-4, "National Strategy to Combat Weapons of Mass Destruction," unclassified version, December 11, 2002, at *www.fas.org/irp/offdocs/nspd/nspd-17.html* (November 24, 2004).

Carafano, James Jay, Ph.D., and Ha Nguyen, "Better Intelligence Sharing for Visa Issuance and Monitoring: An Imperative for Homeland Security," Heritage Foundation *Backgrounder* No. 1699, October 27, 2003, at *www.heritage.org/Research/HomelandDefense/BG1699.cfm*.

Carafano, James Jay, Ph.D., "Intelligence Recommendations Bear Scrutiny," Heritage Foundation *Executive Memorandum* No. 939, July 30, 2004, at *www.heritage.org/Research/HomelandDefense/em939.cfm*.

Carafano, James Jay, Ph.D., Richard Weitz, Ph.D., and Alane Kochems, "Department of Homeland Security Needs Under Secretary for Policy," Heritage Foundation *Backgrounder* No. 1788, August 17, 2004, at *www.heritage.org/Research/HomelandDefense/bg1788.cfm*.

Center for Strategic and International Studies Taskforce, "Meeting the Challenges of Establishing a New Department of Homeland Security," Center for Strategic and International Studies *White Paper*, at *www.csis.org/features/hamrefinalpaper.pdf* (November 12, 2004).

Congressional Research Service, "House Committees: A Framework for Considering Jurisdictional Realignment," November 4, 2004.

———, "Considering Intelligence Appropriation and Authorization in a Single Committee: 9/11 Commission Recommendation and Alternatives," October 29, 2004.

Czerwinski, Jonah, "NATO Can Strengthen the Transatlantic Relationship in the War on Terrorism and Help Define and Pursue Homeland Security Objectives," Center for the Study of the Presidency, October 2004 draft.

Davis, Lynn E., Gregory F. Treverton, Daniel Byman, Sara Daly, and William Rosenau, "Coordinating the War on Terrorism," RAND Corporation *Occasional Paper*, OP–110–RC, March 2004, at *www.rand.org/publications/OP/OP110/OP110.pdf* (December 1, 2004).

Heyman, David. "America's Patchwork of Preparedness in Bio-Defense Reflects a Failure of Leadership" *McGraw-Hill Homeland Security*, June 2004. Page 46.

Homeland Security Act of 2002, Public Law 107–296, at *thomas.loc.gov/cgi-bin/query/D?c107:6:./temp/~c107Ejc8Wt::* (December 1, 2004).

Moteff, John, "Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences," Congressional Research Service *Report for Congress*, September 2, 2004, at *www.fas.org/sgp/crs/RL32561.pdf* (December 1, 2004).

National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington, D.C.: U.S. Government Printing Office, 2004), at *a257.g.akamaitech.net/7/257/2422/05aug20041050/www.gpoaccess.gov/911/pdf/fullreport.pdf* (December 1, 2004).

Office of Homeland Security, "Homeland Security Strategy," July 2002, at *www.whitehouse.gov/homeland/book/nat_strat_hls.pdf* (November 12, 2004).

Rabkin, Norman J., "Homeland Security: Observations on the National Strategies Relating to Terrorism," testimony before the Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, U.S. House of Representatives, GAO–04–1075T, September 22, 2004, at *www.gao.gov/new.items/d041075t.pdf* (December 1, 2004).

Scardaville, Michael, "Homeland Security: Making the New Department Efficient and Effective," in *Agenda 2003: Shaping America's Future* (Washington, D.C.: The Heritage Foundation, 2003), at *www.heritage.org/Research/Features/agenda_homeland.cfm*.

Task Force on National Security in the Information Age, "Creating a Trusted Network for Homeland Security," Markle Foundation, December 2, 2003, at *www.markletaskforce.org/reports/TFNS_Report2_Master.pdf* (November 24, 2004).

———, "Protecting America's Freedom in the Information Age," Markle Foundation, October 7, 2002, at *www.markletaskforce.org/documents/Markle_Full_Report.pdf* (November 24, 2004).

Turner, Jim, Ranking Member, Select Committee on Homeland Security, U.S. House of Representatives, "Bioterrorism: America Still Unprepared," prepared by Democratic staff, October 2004, at *www.house.gov/hsc/democrats/pdf/hsc_docs/finalreportwithcover.pdf* (November 12, 2004).

U.S. Department of Homeland Security, "Securing Our Homeland: U.S. Department of Homeland Security Strategic Plan," 2004, at *www.dhs.gov/interweb/assetlibrary/DHS_StratPlan_FINAL_spread.pdf* (November 12, 2004).

———, "Press Room" Web site, at *www.dhs.gov/dhspublic/theme_home8.jsp* (November 12, 2004).

U.S. Department of Homeland Security, Office of Inspector General, "Improvements Needed to DHS' Information Technology Management Structure," OIG–04–30, July 2004, at *www.dhs.gov/interweb/assetlibrary/OIG_CIOReport_0704.pdf* (December 1, 2004).

U.S. Government Accountability Office, "Homeland Security" Web site, at *www.gao.gov/docsearch/featured/homelandsecurity.html* (November 12, 2004).

———, "Homeland Security: Effective Regional Coordination Can Enhance Emergency Preparedness," GAO–04–1009, September 2004, at *www.gao.gov/new.items/d041009.pdf* (November 30, 2004).

The White House, "Homeland Security" Web site, at *www.whitehouse.gov/homeland* (November 12, 2004).