Homeland Security 3.0

Building a National Enterprise
To Keep America Free, Safe, and Prosperous

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

September 18, 2008

The Heritage Foundation
LEADERSHIP FOR AMERICA
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES
1800 K Street, NW
Washington, DC 20006
(202) 887-0200 | csis.org

Homeland Security 3.0: Building a National Enterprise to Keep America Safe, Free, and Prosperous

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

About the Authors

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

James Jay Carafano, Ph.D., is Assistant Director of the Kathryn and Shelby Cullom Davis Institute for International Studies and Senior Research Fellow for National Security and Homeland Security in the Douglas and Sarah Allison Center for Foreign Policy Studies at The Heritage Foundation.

Table of Contents

Executive Summary

In 2004, a task force chaired by homeland security experts from the Center for Strategic and International Studies (CSIS) and The Heritage Foundation (and consisting of representatives from academia, research centers, the private sector, and congressional staffs) presented its conclusions in "DHS 2.0: Rethinking the Department of Homeland Security." Their report evaluated the capacity of the Department of Homeland Security (DHS) to fulfill its mandate as set out in the Homeland Security Act of 2002. Their evaluation was based on four criteria: management, roles and missions, authorities, and resources. It offered more than 40 major recommendations and made the case for a significant reorganization of the DHS to improve this instrument's effectiveness and efficiency for preventing and responding to terrorist threats. Many of these proposals in the report were subsequently adopted by Congress and the Secretary of Homeland Security.

Four years later, this follow-up report concludes that, while many still find the department a work in progress, the most pressing needs for enhancing the protection of the country from transnational terrorist threats do not lie in further major reorganization of the DHS or revisiting its roles and missions. Rather Congress and the Administration should shift their focus to strengthening the effectiveness of the national homeland security enterprise as a whole.

The terrorist threat is nimble and dynamic. It exploits the seams of our society, operating in the gaps between bureaucratic notions of foreign and domestic, state and federal, civil and military. To counter this threat, we must build a national homeland security enterprise that is as agile and seamless as those who seek to harm us. The objective of this report is to highlight the most critical tasks for building such an enterprise.

To be more agile, our bureaucracy must foster better decision making in Congress and in the interagency process, support the development of a new generation of professionals, and facilitate information sharing throughout all elements of the enterprise. Furthermore, to close the gaps where terrorists hide, we must empower individuals and communities and extend international cooperation throughout our homeland security activities.

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

- **Empowering** a national culture of preparedness by focusing on building more self-reliant communities and individuals,
- **Shifting** to a strategy that is focused on building and sustaining a resilient national infrastructure,
- **Expanding** international cooperation throughout homeland security programs,
- **Developing** a framework for domestic intelligence, and
- **Establishing** national programs to improve professional development at all levels of governance on security and public safety.

The next Congress and Administration have an opportunity to look at our national homeland security enterprise anew. In doing so, they should adopt specific initiatives to address these critical tasks. The Administration should adopt an interagency approach led by a revitalized, reorganized, and integrated National Security Council that treats domestic and international security concerns in a more holistic manner.

In addition to consolidating committee jurisdiction over the DHS and creating committees to oversee interagency education, assignments, and accreditation, Congress should establish a bipartisan caucus that meets regularly to consider issues that affect the national homeland security enterprise. Both the next Congress and Administration need to engage private businesses and the American people—two great, but seemingly forgotten strengths of American society—more effectively to persuade them to contribute to and participate in homeland security.

Protecting America at home is a national mission that requires the concerted effort of the nation, including state and local governments, the private sector and nongovernmental organizations, local communities, families, and individuals. Many of the most vital tasks are conducted most effectively in a decentralized manner. The national enterprise must facilitate cooperation, innovation, resiliency, flexibility, and adaptability, not promote rigid Washington-centric solutions. In addition, virtually every aspect of domestic security from securing the border to disaster response has an international dimension requiring the cooperation of friends and allies around the world. We are facing threats—naturally occurring and deliberate—that can, will, and do target all elements of our society. It is therefore incumbent upon all elements of our society to work together to counter these threats.

While this report's 25 recommendations are grouped by critical task subject, many of the proposals are interdependent, affecting more than one mission area. In particular, the initiatives regarding community preparedness and resiliency of national infrastructure and global systems dovetail closely. Thus, the task force envisions these recommendations as integral parts of a holistic strategy for building the national homeland security enterprise that the nation needs, not as a menu from which policymakers should pick and chose.

Homeland Security 3.0: Building a National Enterprise to Keep America Safe, Free, and Prosperous

On November 25, 2002, President George W. Bush signed the Homeland Security Act of 2002, establishing the U.S. Department of Homeland Security (DHS). Two years later, "DHS 2.0: Rethinking the Department of Homeland Security," a report from a task force chaired by homeland security experts from the Center for Strategic and International Studies (CSIS) and The Heritage Foundation, made the case for a major reorganization of the DHS. The task force report began by assessing the effectiveness of the department.

The Homeland Security Act of 2002 transferred more than two-dozen federal entities—some in their entirety, some only in part—and 180,000 employees to the new department. After passage of the law, a requirement to revisit the organization and management of the department should have been axiomatic. Complex mergers are bound to encounter resistance, unanticipated problems, and obstacles that cannot be overcome without decisive intervention by the organization's leadership. Establishing the DHS proved no exception.

In concert with the "DHS 2.0" report, the DHS Inspector General identified management and organization as significant issues in "Major Management Challenges Facing the Department of Homeland Security" (December 2004): "Integrating its many separate components into a single, effective, efficient, and economical department remains one of DHS' biggest challenges." As the report pointed out, the department lacked authority within its secretariat to set department-wide policies and programs.

The weaknesses in DHS organization were critical because they cut against the core rationale for passing the Homeland Security Act of 2002: gaining the synergy of grouping the key federal agencies with homeland security responsibilities into one department. "DHS 2.0" directly addressed this issue with 40 substantive recommendations for reform.

After the release of "DHS 2.0," the DHS undertook the Second Stage Review, a major review of organization and process. In July 2005, Secretary Michael Chertoff announced the results of the review and a reorganization plan. Subsequently, Congress imposed additional reforms on the department. Many of the changes undertaken addressed the issues and recommendations raised in "DHS 2.0."

Regrettably, Congress did not stop there, instead continuing to impose new reorganization mandates on the DHS. The 2008 elections offer a unique and historic transition in that they will bring a change in leadership that guides our nation's homeland security enterprise. Not since the Eisenhower Administration took over the Department of Defense or the Reagan Administration assumed leadership of the Department of Energy have the stewards of our nation's security—in this case homeland security—been wholly or mostly replaced for the first time. This presents those coming to power with a unique opportunity to reform, revise, and ultimately improve on the policies and processes that shape our national homeland security architecture, but it also presents a temptation to overcorrect.

The constant turmoil imposed on the DHS has adversely affected operations, distracted the leadership, and slowed the process of establishing effective processes and procedures. The first priority of the next Congress and Administration should be to end such unwarranted tinkering. At the very least, Congress should impose a moratorium on restructuring or rethinking the department's roles and missions until after the DHS delivers its first quadrennial security review and Congress has had sufficient time to consider it.

Why This Report? Why Now?

With the upcoming historic change in government, many voices will likely call for revisiting DHS roles, missions, and functionality. One aim of this report is to remind key stakeholders that the DHS is only one part of a much larger homeland security system—or it should be—and to urge completion of the most urgent task at hand, which is establishing a national homeland security enterprise that integrates all elements of society to protect America against catastrophic events.

The fixation of Congress and many others on the department as the only solution to all of the nation's homeland security challenges is unwarranted. While the DHS budget accounts for about half of all federal domestic security expenditures, the homeland security budgets of the Departments of Defense, Health and Human Services, Justice, Energy, and State are also significant. While these departments account for the lion's share of federal homeland security spending, virtually every federal agency has some responsibility for homeland security. Coordinating all of these activities is Washington's most important task.

Furthermore, homeland security responsibilities extend far beyond Washington's purview. Protecting the homeland is a national mission that requires the concerted effort of the entire nation, including state and local governments, the private sector and nongovernmental organizations, local communities, families, and individuals. In addition, virtually every aspect of domestic security from securing the border to disaster response has an international dimension requiring the cooperation of friends and allies around the world. Therefore, the objective of this report is to highlight the most critical tasks for building the homeland security enterprise.

Organization of the Report

The task force's conclusions are organized into five parts that address the key tasks that need to be performed to establish the national homeland security enterprise. Each section consists of findings and recommendations agreed upon by the task force.[1] Major recommendations of the report include:

- **Empowering** a national culture of preparedness by focusing on building more self-reliant communities and individuals,
- **Shifting** to a strategy that is focused on building and sustaining a resilient national infrastructure,
- **Expanding** international cooperation throughout homeland security programs,
- **Developing** a framework for domestic intelligence, and
- **Establishing** national programs to improve professional development at all levels of governance on security and public safety.

While this report's 25 recommendations are grouped by critical task subject, many of the proposals are interdependent, affecting more than one mission area. In particular, the initiatives regarding community preparedness and resiliency of national infrastructure and global systems dovetail closely. Thus, the task force envisions these recommendations as integral parts of a holistic strategy for building the national homeland security enterprise that the nation needs, not as a menu from which policymakers should pick and chose.

1. To the greatest extent possible, this document reflects a consensus of the task force members. However, not all members of the 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.

The Next Steps

The next Congress and Administration need to adopt specific initiatives to address these critical tasks:

- The Administration should adopt an interagency approach led by a revitalized, reorganized, and integrated National Security Council that treats domestic and international security concerns in a more holistic manner.
- Congress should consolidate jurisdiction over the DHS into single committees in each chamber to simplify the challenge of integrating department activities with the other components of the homeland security enterprise.
- Congress should establish committees with narrow jurisdiction over interagency national security professional development (e.g., education, assignment, and accreditation).
- Congress should establish a bipartisan caucus that meets regularly to consider issues affecting the national homeland security enterprise in a holistic manner to inform appropriations and to provide oversight of federal activities.

I. Empowering a National Culture of Preparedness

Findings

FINDING #1: Energizing and engaging individuals in efforts to improve the safety of their families and communities must be the centerpiece of a national homeland security enterprise.

Voluntary community actions have been a longstanding American way of solving thorny problems. Embodied in the U.S. Constitution, the principles of limited government and federalism give citizens and local communities the greatest role in shaping their lives. Government simply cannot be at all places at all times to protect against all contingencies. This principle is evident in the 10th Amendment, which states, "The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people."

In matters relating to their communities, local jurisdictions have the preponderance of authority and autonomy. Moreover, they will be the first on the scene and the first to act in the aftermath of a disaster. The best communities accept these responsibilities and take an all-hazards approach to emergency and public safety planning and preparedness by optimizing community responses to meet the range of natural and manmade dangers (e.g., storms, floods, terrorist incidents, and other malicious acts).

FINDING #2: Federalism must undergird our approach for allocating responsibilities to meet the needs of citizens after disasters.

Remaining committed to a federalist approach is not just being a slave to tradition. It is a precedent based on practicality and experience. Both scientific research on disaster response and an analysis of recent emergencies argue that it is still the right approach. Many of the best efforts to save lives and safeguard property highlight the vital role that nongovernmental organizations (NGOs), private-sector initiatives, and individual civic deeds play during extreme emergencies. In fact, they argue that rather than being supplanted by federal oversight, grassroots community-based responses should be the cornerstone of the national effort. Empowering individuals and businesses at the community level must be the guiding principle for national preparedness.

FINDING #3: Despite a presidential directive (HSPD–7) that emphasized the importance of grassroots efforts, many factors have worked against establishing a national culture of preparedness.

The first factor is the "not me" syndrome. In the aftermath of Hurricane Katrina and just before hurricane season started in 2006, the American Red Cross polled Americans in hurricane-prone areas on their preparedness activities. Given the sheer devastation and extensive reporting on the impact of Hurricane Katrina, most Americans saw hours of videos and pictures that should have driven home the importance of being prepared. Yet the poll results indicated

that the vast majority of households had failed to take even the most basic steps, such as establishing a meeting place, making an evacuation plan, or selecting an emergency contact. According to a Harris poll one year later, the numbers remained largely unchanged. Americans are largely ambivalent to preparedness because they do not believe that they will ever be victims. This is equally true with preparedness for terrorist incidents. The reality is that most Americans live in areas where the risk of and potential danger from a catastrophic incident such as a terrorist attack or natural disaster (except for cybersecurity and pandemic flu) is low.

The second factor is the government's impaired credibility. A pattern over several years of raising and lowering alert levels and of misunderstanding the major threats of the day has led to a public wary and doubtful of government warnings. In regard to terrorism, when the government continues to warn the public that "it's not a matter of if, but when we will be attacked," the question for some becomes "Why should we prepare if the government is just going to get it wrong again?"

The third factor is failed government leadership. Not until a private initiative brought the Ready.gov program in its entirety to federal officials did the government even try to engage individuals and communities in preparedness. Right or wrong, the only elements of the readiness program that people still remember are to buy duct tape and go shopping. Regrettably, when the public was most open to government guidance, botched communications and/or flawed reporting made a mockery of the value of preparedness and the serious steps that individuals can take to help themselves and their communities.

FINDING #4: Congress subverts risk-based funding initiatives by requiring set-asides for every state, which are totally divorced from any risk-based allocation process.

The 9/11 Commission's final report warned that homeland security grants were in danger of becoming pork-barrel legislation. The report was right. Allocating funding based on risks and needed capabilities would substantially reduce the funding to states without large cities, critical infrastructure, or identified threats. Facing this threat to its pork-barrel projects, Congress has knowingly failed to require the DHS to allocate funds only to purposes that would build the 37 critical capabilities listed in the Target Capabilities List (TCL), which was established to identify minimum state and local response capabilities. The DHS has aggravated the problem by not voluntarily adopting such a funding model and by its inability to maintain a fixed number of urban areas eligible for the Urban Areas Security Initiative grant program. As a result, billions of federal dollars have been spent without substantially reducing national risk.

FINDING #5: Federally directed programs to boost local preparedness have had marginal impact.

In the seven years since the attacks on September 11, 2001, and the three years since Hurricane Katrina, citizen programs such as Ready.gov, Citizen Corps, and Community Emergency Response Teams (CERT) have focused on promoting activities rather than building capabilities. For example, the main page of the Citizen Corps Web site states: "There are: 2,318 Councils which serve 223,307,198 people or 78% of the total U.S. population." However, a quick look at the calendar of events reveals that, except for CERT classes, not much is happening in the 2,318 councils.

Recommendations

RECOMMENDATION #1: The U.S. should reclaim September 11 as a day of national preparedness.

The events of 9/11 have made a deep mark on the American psyche, but it need not be permanent. Americans are resilient, and from adversity comes opportunity. The antidote to the terror of 9/11 is to transform that memory into a cause for empowerment, turning a national tragedy into a national strength.

Individuals, families, and communities should honor 9/11 by checking and practicing their response plans for relevant threats, replenishing their Go-kits, updating their emergency contact lists, and engaging in other acts of preparedness. People do this already in some sense for Daylight Savings Time when they change batteries in their smoke detectors. We should build on this notion to foster a culture of national preparedness.

This day should also become the centerpiece for promoting national community planning efforts that encompass far more than the individual and family preparedness measures proposed by Ready.gov and the Red Cross. These might include:

- *Community-based planning.* Planning that includes input from the community produces not only higher quality plans, but also much higher levels of community approval and confidence in the plans.
- *Organizing community needs assessments and situational awareness networks.* Community residents can often be the most important source for collecting and disseminating important information.
- *Mental health response.* One of the most significant and underappreciated aspects of disaster response is responding to mental health issues caused by stress and trauma. The University of Delaware Disaster Research Center report "Disasters and Mental Health: Therapeutic Principles Drawn from Disaster Studies" (1996) found that when community ties "are strong, supportive, and responsive to the individual's physical and emotional needs, the capacity to withstand and overcome stress is heightened."
- *Long-term health monitoring.* Many disasters have long-term health consequences, such as from exposure to toxic particulates that have effects that are unclear at the time. Individuals can help themselves cope with long-term health consequences by knowing what kinds of information to retain to make long-term health monitoring more effective.

RECOMMENDATION #2: The federal government should develop and implement a national planning capability for preparedness to guide resource allocation and investment across the federal government and to state and local communities.

A national homeland security system requires a national planning capability for rational decision making and investments. Such a capability would include continuous assessments of:

- What we need to protect (i.e., criticality assessment);
- Potential threats (i.e., annual national threat assessment);
- Available means of protecting ourselves against these threats (i.e., capabilities list); and
- Protections already in place (biannual gap analysis).

RECOMMENDATION #3: States should take the lead in codifying the TCL, requiring biennial risk and capabilities assessments to identify capability gaps, and ensuring that grant applications do not request any non-TCL capability or an excessive level of a capability.

Because every state and locality faces unique challenges, it is critical that the federal government develop a tier structure to guide TCL implementation. This tier structure would help states and localities to identify their appropriate levels of each capability so that they do not overinvest or underinvest in capabilities. Even with little or no federal aid, all communities need assistance in developing a base level of preparedness. All communities face the threat of pandemic diseases and recurring natural disasters. The federal government should highlight best practices and develop and promote baseline community preparedness capabilities standards. A good example of such an effort is the Council for Excellence in Government's Readiness Quotient Index.

The federal government should also develop a basic risk assessment tool. This tool would enable communities to evaluate relative risks realistically so that they can strengthen their communities by applying their resources to the most likely risks. With this knowledge, states and localities can make informed decisions on the capabilities needed to safeguard their communities.

RECOMMENDATION #4: Washington should target the lion's share of financial and other support to public preparedness efforts by state and local government in the areas at greatest risk of catastrophic natural disaster or terrorist attack.

Congress should stop distributing resources to state and major urban areas based on fixed percentages. Instead, Congress should consider a forced federal funding model similar to the Base Realignment and Closure (BRAC) process in which agencies work with an independent non-partisan commission that develops a proposal, which Congress can either accept or reject in its entirety without amendment.

RECOMMENDATION #5: Government leaders must provide better warning, notification, and public education.

No level of preparedness or countermeasures will suffice without effective, clear, and timely communication to the public. Complex risk communications containing a dizzying amount of information cause confusion and apathy.

Risk communications must be credible, understandable, and actionable. Risk communicators must be trusted. The public must be educated in advance of a crisis about what steps they may need to take, how to prepare, and how to stay informed. Public officials must ensure that individuals have a means to receive public alerts and notifications and that those means are tested, exercised, and understood well in advance of a crisis. Public alerts, when appropriate, should be brief, simple, and clearly worded watch or warning reports that average people can understand. Where possible, national alerts should be replaced with targeted regional or local alerts from state or local governments and specific warnings for different types of industries and infrastructure. The alerts should take advantage of appropriate technologies, such as reverse 911 in urban settings and sirens in remote locations.

II. Shifting to a Strategy Focused on Sustaining a Resilient National Infrastructure

Findings

FINDING #6: Security strategies based on identifying and protecting critical infrastructure are inadequate.

The United States and other countries have not adequately identified truly critical infrastructure and necessary systems, defined terms, or identified areas of potential security improvements. Since 9/11, the federal government has made numerous efforts consistent with HSPD–7 to identify critical infrastructure. Recent efforts, such as the National Infrastructure Protection Plan (NIPP) and its related Sector-Specific Plans, have been more rigorous and substantive.

The next Administration will no doubt build on the National Infrastructure Protection Plan (NIPP), but the process is still not sufficiently discriminating and rigorous. In addition, current processes fail to disaggregate what is "critical" (e.g., essential for sustaining and supporting our daily lives) from what is "dangerous" (e.g., chemical facilities) but not necessarily critical. The colloquial use of the term "critical infrastructure" has often been sloppy and overinclusive, lumping "critical" and "dangerous" into one concept of "critical," resulting in government policies that are inadequate to address both concepts. Critical assets need to be made more resilient through greater redundancy, robustness, and/or decentralization, while dangerous facilities must be protected against attack. Prevention, mitigation, response, recovery, and reconstitution are also vital elements in a national infrastructure strategy that focuses on reducing risks in a sensible and cost-effective manner.

FINDING #7: A strategy of resiliency signifies ensuring that the basic structures and systems of our global, national, and local economies remain strong and can continue even in the face of natural disasters or terrorist attacks.

Fundamentally, building a more resilient society is an effort aimed at prevention and deterrence. Protecting our most critical infrastructure and necessary systems prevents terrorists from exploiting vulnerabilities in our society and dealing blows that could cripple our country. Decentralizing and making our necessary global and national systems less brittle demonstrate to terrorists the futility of attacking them, thus deterring attack.

FINDING #8: The roles and relationship between government and the private sector are still poorly understood.

Certain infrastructure (e.g., financial networks, electric grids, and telecommunications) are the lifeblood of our daily lives. They sustain us, provide for us, and facilitate the rich social fabric that makes America's vibrant economic and political systems hum. Therefore, we have a national interest in ensuring that these infrastructures are robust, reliable, and resilient in the face of possible disruptions from natural disasters and/or terrorist attacks.

The private sector owns and operates more than 85 percent of the nation's critical infrastructure and necessary systems. Thus, the government's role, especially the federal government's role, is generally limited because of our

commitment to free enterprise and our federalist system. At most, responsibility is shared between the government, which has the primary mission of protecting the nation against all threats foreign and domestic, and the private sector, which depends economically on providing the critical services and resources to the government, the public, and the business community. As such, this responsibility can only best be accomplished by a partnership between the government, which might have intelligence about threats, and the private sector, which owns the assets and resources that may be the targets of these threats.

This partnership has been established over the past few years with mixed success. Many factors have influenced the degree to which the government and the various sectors have forged abiding and mutually beneficial operational relationships. These factors include the unique characteristics of each sector; the type and extent of past working experiences between government and businesses, which range from highly regulatory to nonexistent; and the leaders who are responsible for forging or transforming these relationships. What is needed is a renewal of this vital partnership, focused on reinforcing the bonds that have been the basis of successful public–private engagements. This renewal also needs to create a clear path for all sectors of industry and components of government to partner in ways that best serve their mutual interests.

FINDING #9: The vital elements of resiliency—surge capacity, national continuity of operations, reconstitution and recovery of key response systems, and robust public infrastructure—have not been adequately addressed.

For a system or asset to be resilient, it must be designed with qualities that help to ensure its viability under stress—robustness, redundancy, rapid recoverability, and readily reinforceable. For example, a key aspect of national resiliency is ensuring that our necessary response systems possess adequate surge capacity. These systems are not necessarily potential targets, but public infrastructure critical to allowing our society to "bend, not break" during a disaster. Public health, telecommunications, water systems, or other necessary utilities and systems would be severely taxed during a major disaster, but otherwise operate under capacity during normal times. In addition, we need adequate stockpiles of vital response equipment, such as vaccines, ventilators, and respirator masks.

Furthermore, much of the U.S. infrastructure (e.g., roads, bridges, and the power grid) is aging or not keeping up with the demands of a growing economy. Efforts to rebuild or upgrade critical infrastructure are being compromised by politics and inadequate investment in public infrastructure. Lack of robust infrastructure could compromise resiliency in the face of disasters. Regrettably, political influence has misdirected much of the federal largesse into pork-barrel projects that do not reflect true national priorities.

FINDING #10: The resiliency of critical infrastructure and necessary systems is a global issue.

Despite the focus on critical infrastructure and necessary systems within the United States, security and resiliency of the global economy, especially the movement systems that are its essential arteries, might be an even larger issue. These include the global supply chain, the systems for moving energy resources around the world, systems for moving people around the world and lawfully across borders, the cyber and telecommunications infrastructure that moves data around the world, and the banking and money movement systems. While some international and bilateral efforts—such as the World Customs Organization's Standards to Secure and Facilitate Global Trade Framework (SAFE Framework) and the U.S.–European Union agreement on the transmission of Passenger Name Record data to facilitate screening of international air passengers—are trying to protect the arteries of the global economy, most efforts have been country specific.

Recommendations

RECOMMENDATION #6: The federal government should establish a strong regional DHS structure that is focused on preparedness and response and on developing a cooperative state-based regional response network.

A regional response network is an essential next step in building the kind of national security enterprise that the nation needs. This will require state-based regional programs that focus on ensuring that states are prepared to sustain themselves and that facilitate cooperation among federal, state, and local efforts. In the Homeland Security Act of 2002, Congress mandated that the Department of Homeland Security set up a regional structure, but the depart-

ment never carried out this mandate. State-based regional programs would focus on ensuring that states are prepared to sustain themselves. Successful regional programs would focus, not on federal structures in each region, but on regional emergency management programs and capabilities that are developed, coordinated, and managed by the states. Similar small-scale programs that use a regional model, such as the Emergency Management Assistance Compact (EMAC), have already proven successful.

A successful regional program could expand on the idea and focus of EMAC. DHS regional offices should be required to strengthen state and local preparedness capabilities; facilitate regional cooperation among governments, the private sector, and nongovernmental organizations; and plan and exercise with federal entities that support regional disaster response. Such offices would enable regions to access and integrate their capabilities quickly and to improve preparedness. They would have four key missions:

- Facilitating regional planning;
- Organizing regional exercises, training, doctrine, and professional development;
- Helping states and local communities to prepare for catastrophic events, reconstitution, and recovery; and
- Fostering resiliency of infrastructure through cooperative public–private programs.

Other key federal agencies such as the Departments of Defense and Health and Human Services should collocate regional offices with the DHS regional offices.

RECOMMENDATION #7: The federal government should develop stronger national leadership on global and national resiliency issues, especially to deal with national issues (e.g., pandemic influenza, bioterrorism, cybersecurity, electromagnetic pulse attacks, and protection of national infrastructure and systems).

Not everything can be accomplished at the regional level. Some key systems that need protection or greater resiliency are national or global in scope, such as cyber and telecommunications infrastructure. Moreover, certain types of disasters are national or global by nature, such as a pandemic influenza outbreak or contagious bioterrorism attack. The DHS must serve as an effective lead federal agency in this effort and establish a national resiliency council of federal entities and an advisory board.

RECOMMENDATION #8: The federal government should establish a doctrinal model for government–private sector roles.

Defeating terrorists is not the private sector's job. The government is responsible for preventing terrorist acts through intelligence gathering, early warning, and domestic counterterrorism. However, the private sector has a duty to take reasonable precautions to ensure the continuity of business operations and to safeguard its employees and customers, much as society expects it to take reasonable safety and environmental measures. Governments have a role in defining what is "reasonable" as a performance-based metric and in facilitating information sharing that enables the private sector to perform due diligence (i.e., protection, mitigation, and recovery) in an efficient, fair, and effective manner. A model public–private resiliency regime would:

- Define what is reasonable through clear processes and performance measures,
- Create transparency and the means to measure performance,
- Provide legal protections to encourage information sharing and initiative, and
- Be tailored to the unique characteristics of each sector.

RECOMMENDATION #9: The federal government needs to recapitalize the nation's aging critical infrastructure, incorporating appropriate homeland security safety and security measures into the construction of any new infrastructure.

The Administration needs to propose and Congress needs to develop an investment strategy to facilitate public–private partnerships more effectively. This should include targeting national transportation trust funds so that they are spent on national priorities instead of pork-barrel projects. For example, the federal government could:

- *Create an Independent Infrastructure Fund*, as recommended by the CSIS Commission on Public Infrastructure, to provide federal funding for all infrastructure upgrade projects. It would be led by a nonpartisan Infrastructure Improvement Commission, which would oversee the progress of such projects, including evaluating relevant metrics. This commission would have power over all federal funding for infrastructure projects.
- *Encourage public-private partnerships* (PPPs) that invest in border infrastructure. The U.S. has used the PPP model for public highways and other infrastructure projects. For example, the U.S. General Services Administration (GSA) owns, builds, and leases border and port entries. It develops and maintains standard processes and procedures to ensure that land ports of entry are developed consistently and to an acceptable standard. Creating opportunities for the GSA, U.S. Customs and Border Protection, Canada Border Services Agency, and private firms to work together to improve the infrastructure at points of entry would be the most cost-effective and sustainable strategy for a safe and secure border.
- *Turn back federal trust funds*, such as the federal Highway Trust Fund, to the states or allow states to opt out of such programs in return for agreeing to meet a series of quantitative performance criteria.
- *Focus investments on project-based financing*, rather than relying heavily on public subsidies of infrastructure improvements. Project-based financing shifts the risks and rewards to the private sector. It focuses on obtaining stand-alone investments from private investors and could include multiple investors, each with a different level of investment, varying rate of return, and different timeline for realizing those returns. Such strategies not only shift risk to the private sector, but also should lead to improved decision making about infrastructure investments.

RECOMMENDATION #10: The international community and the private sector need to focus on increasing the resiliency of key networks of the global economy.

This effort should continue and be given even greater emphasis over the next few years. Through such engines as the World Customs Organization, the international community and the private sector should build on the SAFE Framework and the International Shipping and Port Facility Security (ISPS) Code to develop more and stronger mechanisms to govern, secure, and increase the resiliency of key components of the global economy's international infrastructure. However, they should take care to preserve the efficiencies that have driven the integration of the global economy.

III. Expanding International Cooperation

Findings

FINDING #11: The national homeland security effort extends globally and requires active cooperation among friends and allies.

The DHS has made great strides in improving international cooperation and outreach. Yet these efforts must become much more robust to facilitate the free, safe, and secure movement of goods, peoples, and ideas. Effective implementation requires not only intergovernmental cooperation, but also the private sector's participation. Programs must facilitate the sharing of best practices, promote effective information exchange, and obtain the technology, products, and services to build more robust security regimes. In particular, the success of these programs, especially those that depend on effective use of technologies and procedures, requires that vendors of security products be willing to deploy their wares outside of the United States.

The United States has traditionally encouraged the sharing of domestically manufactured technologies, particularly through the Defense Security Cooperation Agency. However, liability concerns pose a significant barrier to deploying products outside of the United States. A number of companies have expressed serious reservations about selling security products outside of the United States because they fear that this would expose them to massive and

potentially ruinous liability in the event of a terrorist event. Conversely, foreign companies have significant liability concerns about deploying their products inside the United States.

FINDING #12: While America continues to enjoy strong bilateral relationships with individual states, its relations with the European Union on homeland security matters have been contentious.

The U.S. and EU have different regimes governing individual privacy protections. From 2003 through 2007, DHS and EU representatives engaged in a series of difficult negotiations over U.S. access to airline reservation data or passenger name records (PNR) after Members of the European Parliament objected to such information sharing on privacy grounds. The tensions are also the result of a fundamental disagreement within Europe about the proper allocation of decision-making responsibility between individual EU member states and the Brussels-based EU bureaucracy.

FINDING #13: Cooperating with new partners is a key component of international homeland security efforts.

The first seven years of the war against terrorism demonstrated the importance of developing trust and confidence with nontraditional allies, especially in the Middle East and the Mediterranean. U.S. national and homeland security interests would benefit from developing innovative security cooperation relationships in these areas because they would garner more confidence and trust among countries that, while not pro-American, have not yet assumed entrenched anti-American positions and have unique geographical significance in combating terrorism.

FINDING #14: Engaging the international community in sustained critical deliberations about the security of our societies is an immediate issue.

Encouraging and initiating joint or harmonized initiatives to strengthen preparedness, prevention, response, and recovery efforts in the homeland security domain would benefit all nations. Strengthening our partners makes us more secure. Strong international partnership will not solve all problems, but the absence of partnerships diminishes the hope for a more secure and prosperous global environment.

FINDING #15: U.S. visa polices have not kept pace with demands to facilitate international travel and enhance safety and security.

For example, the Visa Waiver Program (VWP) has admitted no new countries since 9/11. In 2007, Congress modernized the VWP with the twin goals of increasing security requirements and allowing the flexibility to include other members. This approach helps to expand the circle of potential VWP countries and ultimately creates incentives for aspirant countries to enter into arrangements that would expand security. The collaborative relationship between the Administration and Congress is a prime example of working together to achieve the shared goals of strengthening the program's overall security and creating a path to VWP membership for valuable U.S. allies. With such collaborative efforts, we can achieve incremental successes of partnering with more VWP countries.

Currently, 27 countries participate in the program. The DHS has recently concluded six preliminary bilateral agreements with the Czech Republic, Estonia, Latvia, Hungary, Slovakia, and Lithuania. This effort should serve as model for other visa reform initiatives.

Recommendations

RECOMMENDATION #11: The federal government needs to establish a framework for international homeland security cooperation.

This framework should be based on certain principles:

- *Pragmatism*. The DHS should neither seek to exploit divisions between the central EU government in Brussels and EU member states, nor reflexively embrace Brussels as an appropriate interlocutor. Instead, its approach should be governed by a single pragmatic consideration: What is best for American interests? This will sometimes mean negotiating with EU member states on a bilateral basis. At other times, it will mean negotiating with Brussels.

- *Reciprocity*. Neither the United States nor its friends and allies should demand that the other take actions that it is not prepared to take on its own.
- *Appropriateness*. The U.S. and its international allies will inevitably adopt different solutions to commonly recognized problems and even disagree on what constitutes a problem. When such disputes arise, each should acknowledge that it does not have a monopoly on sound policy ideas, and that its partner is entitled to chart a different course than the one it prefers.
- *Free enterprise and private business*. Private businesses with activities that are intertwined with homeland security operations (e.g., airlines and banks) should not be used as pawns in disputes between Washington and its partners. When the U.S. and an ally disagree about the proper resolution of a controversy, private businesses could find themselves subject to conflicting legal requirements. The two governments should agree that they will not threaten to impose civil liability or other penalties on businesses as a way to strengthen their respective hands in intergovernmental negotiations. This framework should be the basis for establishing the international standards and practices of free nations sharing an interest in mutual security.

RECOMMENDATION #12: The U.S. should expand cooperation with new partners and allies through NATO.

NATO's unique map of nearly 60 countries represents the only multilateral consultative environment in the world in which the U.S. retains a significant, albeit underutilized, political advantage. Creative U.S. leadership of NATO in the 21st century can foster a better consensus among the U.S. and the many other countries in that framework for how to combat the evolving terrorist threat, respond to disasters, and improve logistics coordination. This expanded cooperation would include a targeted mix of security cooperation efforts, deeper dialogue on the best practices of counterterrorism, and capabilities training. This type of engagement would enable the development of policy options that help to pursue U.S. homeland security and counterterrorism interests while cultivating a more productive dialogue between the U.S. and critical countries in the Mediterranean and Middle East.

For example, by working with the approximately 15 countries in NATO's Mediterranean Dialogue and Istanbul Cooperative Initiative, the U.S. could focus resources that reinforce a relatively pro-American political environment without forcing these nations to choose between the U.S. and Europe. Additionally, NATO outreach efforts should extend to other regions, including Africa and Asia.

RECOMMENDATION #13: The U.S. should establish security assistance sales, lease, and grant programs that allow the DHS to assist countries in obtaining equipment, support, and financing for homeland security functions.

The Defense Security Cooperation Agency provides $12 billion in security-related equipment and other capabilities drivers to other countries each year, and the Pentagon's International Military Education and Training program trains 14,000 international military students from over 130 countries. The U.S. should begin a counterpart effort, jointly led by the Departments of Homeland Security, Defense, and State, to develop innovative security cooperation relationships with the Middle East and Mediterranean countries already participating in the NATO consultative structures. This effort could be financed through grants, host nation funding, and/or avenues similar to the Pentagon's Foreign Military Financing grants and loans.

Alternatively, the U.S. could establish a Security for Freedom Fund that allows any nation to apply and compete for security assistance funds under an established set of criteria, which should include:

- A demonstrated commitment to freedom and human rights,
- A mutual bilateral security interest with the U.S.,
- A demonstrated need to build capacity to conduct security missions, and
- Adequate governance, including a demonstrated record of meeting its international financial obligations.

A qualifying country should be allowed to apply funds to a range of security and public safety needs.

RECOMMENDATION #14: The U.S. should facilitate international cooperation on liability concerns.

To alleviate liability concerns about the deployment of security technologies outside of the United States, other countries should consider passing legislation similar to the Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act of 2002. The SAFETY Act is a U.S. law that limits damages that can be awarded after terrorist attacks. The State Department and the DHS should work closely with foreign governments to develop liability protections similar to the SAFETY Act, particularly with countries from which significant amounts of goods and numbers of people enter the United States. Other models of liability limitation could also be used, including the liability mitigation steps available through the Public Readiness and Emergency Preparedness Act, which dramatically limits the liability of persons and companies assisting in the event of a pandemic flu outbreak or other serious public health events.

By developing such liability protections, countries would help to ensure deployment of effective anti-terror products and services, thereby improving security for all nations involved. As national liability protection regimes proliferate, new opportunities for international cooperation will emerge. For example, countries with similar liability protection regimes could extend reciprocal privileges. If nations employ equal procedures based on high standards and can verify that their processes are equivalent, they should grant liability protection to providers that have been certified by a country with which they share reciprocal agreements.

RECOMMENDATION #15: The U.S. should continue to emphasize visa reform and modernization.

This process should begin with completing Visa Waiver Program (VWP) modernization. The DHS should aggressively pursue negotiation and signing of bilateral agreements with potential members. Increased VWP participation could encourage other countries to participate, and determined countries will more easily agree to security requirements. This will apply additional pressure on Congress to enter into security agreements. The more countries that are eligible for the program, the more competition there will be.

Adding new members to the program will inevitably raise questions and concerns about implementation and requirements, especially with the recently concluded agreements with Estonia, Latvia, and others. Addressing these questions and concerns will require a join effort of the DHS, the State Department, and the concerned country. These efforts need to be flexible and responsive.

In 2007, Congress gave the DHS the authority to admit countries with a visa refusal rate between 3 percent and 10 percent under certain conditions. One condition is an air exit system that can verify the departure of at least 97 percent of foreign nationals who depart through U.S. airports. Before the DHS can admit VWP countries under this provision, it must implement an air exit system. The lack of technological infrastructure support is the primary cause for the delay in implementing the system.

IV. Developing a Framework for Domestic Intelligence

Findings

FINDING #16: Risks of terrorism are distributed across geographic regions and metropolitan areas.

Terrorists live, work, plan, and act all over the world. Radicalization and terrorist recruitment are on the rise at home and abroad. A few dozen Web sites on the Internet have become "hate central," providing the tools for individuals and groups to self-radicalize. New recruits, particularly those without criminal records or who are not known to law enforcement, can travel with relative ease from country to country and from city to city with little notice.

Potential targets are pervasive. Threatened infrastructure is distributed across vast areas—in commercial districts and along thousands of miles of rail beds, tunnel approaches, and coastal waterways—and jurisdictions that are sparsely populated and rarely patrolled. Many potential targets are also served primarily by police, whose traditional responsibilities cover neither critical infrastructure protection nor terrorism prevention.

As a result, an increased emphasis on understanding and uncovering threats and enhancing domestic intelligence is needed to support post–9/11 homeland security and defense missions. This need transcends concerns about

al-Qaeda and similar groups. Transnational threats of all kinds could become endemic in the 21st century, and the nation must be prepared for them.

FINDING #17: Lack of public discussion of domestic intelligence hampers reasonable debate over new programs for information collection, sharing, and use.

The world of intelligence is largely closed, preventing those who know of intelligence needs, requirements, and eventual uses from commenting publicly. In contrast, those who may have the greatest concerns—civil liberties and privacy groups—may also have the least access to and knowledge of threat and program information. As a consequence, public debate is often one-sided and based on conjecture, worst-case scenarios, and hypothetical situations. Advancing security and protecting constitutional liberties are equally vital, and the government has an obligation to explain how its programs will support both goals equally well.

While the federal government has made individual privacy and protection of liberties core pillars of its policy-making approach, including in its guidance and directives to state and local governments, a lack of discourse on these programs has left the public unaware of the valuable efforts and protections that are already in place throughout domestic intelligence programs. Furthermore, officials at all levels of government often do not even know how to discuss these issues in ways that inform the public of system capabilities and uses, especially privacy protections and anti-abuse features, such as auditing, access controls, and security clearances.

FINDING #18: An adequate national framework for implementing domestic intelligence is lacking.

Since 9/11, new intelligence missions have emerged for homeland defense at the Defense Department and for homeland security at the DHS. New institutions, including the Office of the Director of National Intelligence (DNI) and the National Counterterrorism Center (NCTC), have been created. The FBI has also shifted its primary focus from criminal prosecution to terrorism prevention.

On the threat side, increased radicalization and recruitment of individuals is creating a distinct threat from individuals unconnected operationally with al-Qaeda's leadership and without known linkages to international terrorist networks. This is a worsening global problem, to which the United States is not immune. What intelligence is required, who is responsible for collection, what methods are permitted, and how that intelligence can be used or shared are questions that have been addressed at best in a piecemeal and incoherent fashion.

FINDING #19: Federal, state, and local governments have yet to establish adequate information-sharing systems and processes.

State and local law enforcement are the "first preventers." They are often the first to identify and thwart conspiracies, and they need timely, accurate information to do their jobs. The DHS's and the intelligence community's plans to provide information to intelligence fusion centers remain hopelessly bogged down in information-sharing concerns and concepts based on Cold War paradigms. Despite nascent programs developed by the DNI, such as the laudable Information Sharing Environment (ISE), efforts to move forward with information sharing have been inadequate. State and local agencies remain frustrated and are addressing their local needs by developing work-arounds, such as partnering with other state and local agencies to establish information-sharing programs from the bottom up.

The U.S. government's inability to "connect the dots" was one of the critical failures in the 9/11 catastrophe. A lack of information sharing was a driving force in that failure. The lack of progress with ISE is particularly frustrating. The program manager of the Information Sharing Environment (PM-ISE) has detailed the many shortcomings of the existing environment: overlapping roles and responsibilities; cultural, policy, and technological differences among organizations; policy, process, and procedural differences; and the absence of universal standards to facilitate information sharing. The result is the stubborn persistence of "multiple uncoordinated information products" across the federal government, which impedes a concerted and effective sharing effort. However, the lack of a rapid, uniform government process to obtain clearances for non-federal partners to access classified materials is undermining all efforts to improve information sharing.

FINDING #20: Government efforts to harness cutting-edge commercial technology are inadequate.

Concern for protecting individual constitutional liberties and privacies should always remain paramount. Nevertheless, since 9/11, a concerted effort has been made to argue that enhancing security and protecting free-

doms are mutually exclusive, particularly in applying commercially available technologies. These claims are animated by:

- Concerns over the perceived expansion of executive authority;
- Concerns that the government will use new information technologies, with their superior capacity to manage data, to intrude into our personal lives; and
- Concerns over the efficacy and efficiency of applying new technologies to counterterrorism efforts.

Addressing these concerns and distinguishing real issues from rhetorical arguments is essential to facilitate the adoption of appropriate technologies as quickly as possible.

Recommendations

RECOMMENDATION #16: The President should issue an executive order establishing a national domestic intelligence framework that clearly articulates how intelligence operations at all levels should function to combat terrorism, while keeping citizens safe, free, and prosperous.

This framework must articulate how the homeland security and counterterrorism community, particularly local law enforcement, will conduct counterradicalization efforts. In particular, such a framework needs to establish who can collect intelligence domestically and why, what can be collected and how, and how the government will coordinate and oversee this process. Most important, this doctrine must clearly articulate how all of these activities will support the dual priorities of enhancing security and protecting the liberties of a free society.

RECOMMENDATION #17: The U.S. should establish a federal effort to educate the public on domestic intelligence conducted at all levels of government.

Citizens should be able to access basic information about domestic intelligence programs and the privacy framework in which they operate though a "one-stop shop" that is more user-friendly and focused on the public's concerns. Pursuant to the Intelligence Reform and Terrorist Prevention Act of 2004, the President should direct the DNI to establish a program to coordinate public information efforts across the intelligence community and to research and develop best practices for proactively providing information to the public, media, and civil liberties groups. This information should cover the purposes and value of intelligence programs and describe the relevant safeguards that protect individual privacy and liberties. This program, operating as an ombudsman, should also be responsible for answering media and public inquiries on these issues and advise federal, state, and local agencies on the best approaches to communicating with the public. Congress should explicitly fund this program and direct the DNI to oversee its efforts and evaluate its impact.

RECOMMENDATION #18: The DNI must articulate a quick-implementation plan to provide realistic information-sharing capabilities to state and local authorities based on private-sector best practices.

This effort should include developing a single template for state and local authorities that clearly spells out what kind of information is expected from them, what information they can expect to receive, and how and when to request or access additional information. Consistent with these efforts, the DNI should establish consistent basic training standards for intelligence suppliers and users at the federal, state, and local levels that focus on the core activities of information "sifting" and analysis.

RECOMMENDATION #19: The President should issue an executive order establishing a specific timetable for government-wide compliance with the policies, procedures, standards, architecture, systems, and technologies laid out in the ISE Implementation Plan.

The DNI should be directed to oversee the implementation of the ISE Implementation Plan and report semiannually to the President on progress, opportunities, challenges, and problems in meeting deadlines. The DNI should bring together the heads of all the federal departments and agencies engaged in counterterrorism activities twice a year for a two-day strategic discussion of the progress and problems in implementing the plan.

The President should designate the senior classification and control officer on all federal counterterrorism information with the power to downgrade, declassify, or remove controls on any classified or otherwise controlled information

pertinent to counterterrorism. Through the Office of Management and Budget (OMB), the President should require all federal agencies with counterterrorism responsibilities to invest only in systems fully consistent with the ISE.

The PM-ISE should also create an education and training curriculum for the homeland security information-sharing environment and make it available to all levels of government and to colleges and universities developing technical, policy, or management courses on the information-sharing environment. This curriculum must include a robust national counterintelligence component.

Finally, the government should continue the transition from "need to know" to "need to share" to a higher standard of "responsibility to provide." As such, the government should also examine the feasibility of establishing a secret-level "common clearance" for federal, state, local, and private-sector entities that empowers the "need to share" and "responsibility to provide" concepts and simplifies, reduces the cost of, and accelerates the process of issuing and maintaining clearances.

RECOMMENDATION #20: The President should issue an executive order establishing a national doctrine for applying cutting-edge commercial technology to homeland security and associated activities.

Because technology will be an important part of any set of counterterrorism tools, and because our lives in the Information Age are so dependent on many of the systems and databases that these technologies will access for information about terrorists, the nation needs a set of common agreed-upon rules. These should include:

- No new system, or new access to a nongovernmental system, should alter or contravene existing restrictions on the government's ability to access data about private individuals.
- Development of new technology is not a basis for authorizing new government powers or new government capabilities. Any such expansion must be independently justified.
- To the maximum extent practical, any new system should be made tamperproof. To the extent that prevention of abuse is impossible, the system should have built-in safeguards to ensure that abuse is both evident and traceable.
- To the maximum extent practical, any new system should be developed in a manner that incorporates technological improvements to protect civil liberties.
- No new system should be implemented without this full panoply of protections against abuse.

V. Establishing National Programs for Professional Development

Findings

FINDING #21: Homeland security professional development is the creation of a stable and diverse community of homeland security professionals with relevant skills, attributes, experiences, and a comprehensive knowledge of the homeland security enterprise.

These homeland security professionals include federal, state, regional, and local government employees and contractors; public and private critical infrastructure and key resource personnel (e.g., transit police, chemical plant security, and utility operators); and professionals in other security-related institutions (e.g., academic programs, Federally Funded Research and Development Centers, think tanks, and consulting firms) with responsibilities and missions related to safeguarding the nation. Cross-disciplinary and interdisciplinary education and training are especially valued in preparing professionals. Finally, knowledge of the homeland security enterprise includes a sophisticated familiarity with related institutions of the homeland security community and with relevant supporting disciplines (e.g., public health, safety, and security; science, technology, and engineering; immigration, trade, and international relations; and economics, policy analysis, public management, and law).

Homeland security professional leaders need three distinct elements: education, training, and professional experience and assignments. In 2007, President Bush recognized the need for each of these elements in Executive Order 13434, "National Strategy for the Development of Security Professionals." This executive order established the Secu-

rity Professional Development Executive Steering Committee to develop an implementation plan for the national strategy. The steering committee includes representation from all of the federal entities with national security responsibilities: the DNI, the U.S. Attorney General, the OMB Director, and the Secretaries of State, Treasury, Defense, Agriculture, Labor, Health and Human Services, Housing and Urban Development, Transportation, Energy, Education, and Homeland Security.

Early efforts to carry out this executive order have shown promise in explicitly identifying the need for these three dimensions of professional development. However, differences in the various agencies' policies and approaches have hindered implementation. Efforts thus far have focused on defining a list of core competencies, preparing for the next significant national emergency through training of the National Response Framework, and resolving the difficulties of obtaining diverse professional assignments in this chaotic environment.

FINDING #22: While education is recognized as a critical element of professional development, the current state of the academic discipline is still relatively immature.

According to a Homeland Security and Defense Education Consortium report, there is no consensus or centrally motivated approach to the curriculum requirements, nor would an interested student have any way to evaluate the usefulness of the various offerings. Definition, direction, and clarity of the educational curriculum and training in support of homeland security professional development are lacking.

FINDING #23: The national homeland security enterprise has had difficulty recruiting and retaining talented and diverse professionals.

The homeland security enterprise is characterized by high personnel turnover. The personnel challenges in the DHS are among the most troubling, but reflect problems in the entire community. A 2006 Office of Personnel Management (OPM) survey of federal employees found that the DHS ranked last out of 36 federal agencies on the job satisfaction and results-oriented performance culture indexes and nearly last on the leadership and knowledge management index and the talent management index.

Meanwhile, leadership at the federal level is distracted by fractured congressional oversight. "Facts and Figures About Seven Years of Homeland Security Spending," a March 2008 report from George Mason University, notes that, in 2007, DHS leaders appeared before 86 congressional committees and subcommittees, participated in 206 congressional hearings, attended 2,242 briefings for Members of Congress, wrote 460 legislatively mandated reports, and answered 2,630 questions for the record submitted by Members of Congress after hearings.

FINDING #24: Homeland security lacks a distinct, overarching professional culture.

The Homeland Security Advisory Council's Homeland Security Culture Task Force concluded in its January 2007 report that:

> Success of nearly every large, diverse and geographically dispersed organization requires alignment around a common language, common management process, and common leadership expectations. DHS should adopt…a leadership and training model, including "joint duty and training" experience that will help all DHS leadership to focus collaboratively on key leadership expectations and objectives.

Education, assignment, and accreditation are needed to establish this culture, but implementing mechanisms are lacking. While Executive Order 13434 calls for interagency and intergovernmental assignments, it is unclear that this can be achieved across the homeland security enterprise without additional legislation to de-conflict agency rules and to create management structures that can easily support extended rotations.

Recommendations

RECOMMENDATION #21: The professional development curriculum should include a body of common materials to provide the needed high level of understanding of the national enterprise.

The professional development curriculum should include skills in critical thinking and analytic reasoning, a basic understanding of scientific research methods, knowledge of all-threats and risk-based analysis, and familiarity

with issues of public health, safety, and security; science, technology, and engineering; immigration, trade, and international relations; and economics, policy analysis, public management, and law. With this common grounding in issues across the enterprise, individual institutions could then offer specialized training in first response, WMDs, biodefense, public health, policy analysis, public management, strategic analysis, and other areas. In other words, all institutions would have a broad-based common core curriculum and offer specialized degrees depending on their individual capabilities. Additionally, the Department of Homeland Security should establish standards for mid-level and senior-level executive education.

RECOMMENDATION #22: The federal government should create an academic institution to develop a core curriculum and set guidelines for programs offering specialized degrees.

Congress should establish a Home Team Academy or University. This institution could serve as the national advocate for homeland security professional development activities. It might include all levels of education: entry level, mid-career, and senior education. This institution would be the crown jewel of national professional education.

RECOMMENDATION #23: The federal government should lead a multiagency and multidisciplinary review of education and training.

The fragmented state of professional development could be given direction and a shared set of objectives by a federally led multi-organizational and multidisciplinary council that has expertise in homeland security issues. This professional development review council could help to establish standards for, oversee, and advise this emerging discipline. It could directly implement this advice through input and guidance to the Home Team Academy to improve the scope and efficacy of its developed curriculum. The council could also be responsible for developing a voluntary accreditation process, which would not necessarily be centrally administered, for nongovernmental academic programs so that aspiring professionals would have some means of evaluating the various program offerings. The council should include representatives from federal agencies, much like the Security Professional Development Executive Steering Committee, and representatives from various disciplines, such as safety and security; science, technology, and engineering; and constitutional law and international relations.

RECOMMENDATION #24: The federal government should establish cross-training and cross-experience assignments and programs to recruit and retain highly qualified professionals.

Future homeland security leaders should be required to serve assignments in state and local communities or the private, critical-sector companies that have homeland security responsibilities. Conversely, federal officials should consider drawing from state homeland security organizations and the private sector to fill some of the federal leadership positions. A program of Homeland Security Leadership Fellows should be established, including support for long-term educational opportunities and a rotational assignment system to season these highly qualified and desirable professionals. Candidates for these fellowship positions should include early-career and mid-career leaders from the spectrum of federal, state, and local agencies. Ensuring diversity of experience among professionals and leadership is also vital.

RECOMMENDATION #25: The House of Representatives and the Senate should establish committees with narrow jurisdictions over key education, assignment, and accreditation interagency programs, including homeland security.

Accreditation and congressional involvement are crucial to ensuring that programs are successful and sustainable. Congress should require creation of boards that:

- Establish educational requirements and accredit federal institutions to teach national security and homeland security,
- Screen and approve individuals to attend schools and fill interagency assignments,
- Certify individuals as interagency-qualified, and
- Appoint the professional development review council in concert with the Administration.

Appendix

List of Recommendations

This appendix lists the recommendations made in this report, including the immediate steps that Congress and the Administration should take to strengthen homeland security.

Critical First Tasks

- The Administration should adopt an interagency approach led by a revitalized, reorganized, and integrated National Security Council that treats domestic and international security concerns in a more holistic manner.
- Congress should consolidate jurisdiction over the Department of Homeland Security (DHS) into single committees in each chamber to simplify the challenge of integrating department activities with the other components of the homeland security enterprise.
- Congress should establish committees with narrow jurisdiction over interagency national security professional development (e.g., education, assignment, and accreditation).
- Congress should establish a bipartisan caucus that meets regularly to consider issues affecting the national homeland security enterprise in a holistic manner to inform appropriations and to provide oversight of federal activities.

I. Empowering a National Culture of Preparedness

1. The U.S. should reclaim September 11 as a day of national preparedness.
2. The federal government should develop and implement a national planning capability for preparedness to guide resource allocation and investment across the federal government and to state and local communities.
3. States should take the lead in codifying the Target Capabilities List (TCL), requiring biennial risk and capabilities assessments to identify capability gaps, and ensuring that grant applications do not request any non-TCL capability or an excessive level of a capability.
4. Washington should target the lion's share of financial and other support to public preparedness efforts by state and local government in the areas at greatest risk of catastrophic natural disaster or terrorist attack.
5. Government leaders must provide better warning, notification, and public education.

II. Shifting to a Strategy Focused on Sustaining a Resilient National Infrastructure

6. The federal government should establish a strong regional DHS structure that is focused on preparedness and response and on developing a cooperative state-based regional response network.
7. The federal government should develop stronger national leadership on global and national resiliency issues, especially to deal with national issues (e.g., pandemic influenza, bioterrorism, cybersecurity, electromagnetic pulse attacks, and protection of national infrastructure and systems).
8. The federal government should establish a doctrinal model for government–private sector roles.
9. The federal government needs to recapitalize the nation's aging critical infrastructure, incorporating appropriate homeland security safety and security measures into the construction of any new infrastructure.
10. The international community and the private sector need to focus on increasing the resiliency of key networks of the global economy.

III. Expanding International Cooperation

11. The federal government needs to establish a framework for international homeland security cooperation based on the principles of pragmatism, reciprocity, appropriateness, and free enterprise and private business.
12. The U.S. should expand cooperation with new partners and allies through NATO.
13. The U.S. should establish security assistance sales, lease, and grant programs that allow the DHS to assist countries in obtaining equipment, support, and financing for homeland security functions.
14. The U.S. should facilitate international cooperation on liability concerns.
15. The U.S. should continue to emphasize visa reform and modernization.

IV. Developing a Framework for Domestic Intelligence

16. The President should issue an executive order establishing a national domestic intelligence framework that clearly articulates how intelligence operations at all levels should function to combat terrorism, while keeping citizens safe, free, and prosperous.
17. The U.S. should establish a federal effort to educate the public on domestic intelligence conducted at all levels of government.
18. The Director of National Intelligence must articulate a quick-implementation plan to provide realistic information-sharing capabilities to state and local authorities based on private-sector best practices.
19. The President should issue an executive order establishing a specific timetable for government-wide compliance with the policies, procedures, standards, architecture, systems, and technologies laid out in the Information Sharing Environment Implementation Plan.
20. The President should issue an executive order establishing a national doctrine for applying cutting-edge commercial technology to homeland security and associated activities.

V. Establishing National Programs for Professional Development

21. The professional development curriculum should include a body of common materials to provide the needed high level of understanding of the national enterprise.
22. The federal government should create an academic institution to develop a core curriculum and set guidelines for programs offering specialized degrees.
23. The federal government should lead a multiagency and multidisciplinary review of education and training.
24. The federal government should establish cross-training and cross-experience assignments and programs to recruit and retain highly qualified professionals.
25. The House of Representatives and the Senate should establish committees with narrow jurisdictions over key education, assignment, and accreditation interagency programs, including homeland security.

Task Force Participants

Co-Chairmen

- **David Heyman**
  Director and Senior Fellow, Homeland Security Program
  Center for Strategic and International Studies
- **James Jay Carafano, Ph.D.**
  Assistant Director, Kathryn and Shelby Cullom Davis Institute for International Studies, and Senior Research Fellow for National Security and Homeland Security, Douglas and Sarah Allison Center for Foreign Policy Studies
  The Heritage Foundation

Participants

- **Joseph Augustyn**
  Booz Allen Hamilton
- **William Banks**
  Syracuse University
- **Scott Bates**
  Center for National Policy
- **Jonah Czerwinski**
  IBM
- **James Dean**
  The Heritage Foundation
- **Brian Finch**
  Dickstein Shapiro LLP
- **Susanna Gordon, Ph.D.**
  Sandia National Laboratories
- **Jesper Gronvall**
  Swedish Institute of International Affairs
- **Andrew Grossman**
  The Heritage Foundation
- **Gabriela Herrera**
  The Tauri Group
- **Jan Lane**
  George Washington University
- **Jim Lewis, Ph.D.**
  Center for Strategic and International Studies
- **Ronald Marks**
  Oxford Analytica
- **Matt Mayer**
  The Heritage Foundation
- **Terrill Maynard**
  Homeland Security Intelligence
- **Lt. Col. Joe Myers, Ph.D.**
  Army Adviser to the Commandant of the Air Command and Staff College/Auburn University
- **John Rollins**
  Naval Post Graduate School – Center for Homeland Defense and Security
- **Nathan Sales**
  George Mason University School of Law
- **Seth Stodder**
  Akin Gump Strauss Hauer & Feld LLP
- **Bert Tussing**
  Center for Strategic Leadership, U.S. Army War College
- **Richard Weitz, Ph.D.**
  Hudson Institute
- **Evan Wolff**
  Hunton & Williams
- **Dan Ziegler**
  The Heritage Foundation