Written Testimony Before the

United States Senate
Committee on Homeland Security and Governmental Affairs

"Homeland Security: The Next Five Years"

Daniel B. Prieto

Senior Fellow and Director
Homeland Security Center

dprieto@reforminstitute.org

September 12, 2006

Chairman Collins, Senator Lieberman, and distinguished members of the Committee on Homeland Security and Governmental Affairs, I want to thank you for inviting me to testify before you today. My name is Daniel Prieto. I am Director of the Homeland Security Center at the Reform Institute. Previously, I was Fellow and Research Director of the Homeland Security Partnership Initiative at the Belfer Center for Science and International Affairs at the Harvard University Kennedy School of Government.

My testimony today reflects my own views and analysis and does not reflect the official position of any institution with which I am affiliated.

Introduction

Since 9/11, homeland security in the United States has, in large part, been an attempt to optimize domestic assets and activities to detect, prevent, respond to, and recover from high-consequence events, either terrorist induced or natural. Obviously, there are also a number of related international components, including military action against terrorist groups; overseas intelligence and law-enforcement cooperation; and programs to detect and interdict threats among travelers, emigrants and cargo before they arrive in the United States.

Setting aside military operations and cross-border intelligence sharing efforts, our homeland security efforts in the years since 9/11 have centered on five significant areas of activity: creating new law and policy; creating new organizations; developing new strategies and plans; implementing new "consensus" programs (e.g. C-TPAT, US-VISIT, PCII); and pursuing innovative but controversial programs (e.g. the increasing use of commercial data for terrorism-related analysis, as included in the NSA domestic surveillance program and as seen in TSA's SecureFlight and DoD's TRIA).

To make America more secure in the next five years, we need to:

1. **Adapt to a changing threat environment.**
2. **Engage Society, Educate the Public and Enlist the Private Sector.** To date, we have not done nearly enough to educate the public or to engage the resources and goodwill of the private sector.
3. **Move from Tactics to Doctrine.** Homeland security strategy documents since 2001 have provided tactics, methods and processes, but have failed to articulate strategy and doctrine that provide clear guidance for implementation and goals by which we can measure progress.
4. **Ensure DHS Succeeds**. We can not afford to have a weak DHS that lacks credibility and is challenged to carry out its mandate. One of the major problems DHS has faced is weak management of a complex merger integration process. This needs to change.
5. **Get Technology Right.** While the U.S. is the envy of the world when it comes to technology, the federal government struggles to implement important homeland security technology projects and to transfer important everyday technologies into the homeland security realm.
6. **Catalyze and Govern Information Sharing.**
7. **Develop Rules for the Use of Consumer and Company Data for Counterterrorism.**

The Changing Threat

Looking at the threat environment, the world has not stood still since 9/11. At least two major factors will pose significant new challenges over the next five years.

First, WMD proliferation threats will increase. These growing challenges come from North Korea's pursuit of nuclear weapons and the push by Iran to acquire nuclear weapons capability. The involvement by non-state actors, like the A.Q. Khan supply network, in the proliferation of WMD-related technologies, weapons design, and equipment will continue to grow in seriousness. We will also be challenged by terrorists' efforts to acquire and use WMDs, a situation made more dangerous by potential cooperation between terrorists and rogue or weak states possessing WMD and related technologies.

Second, the terrorist threat is evolving and may look quite different five years from now. Al Qaeda Central is weaker today, but it is stronger as an inspirational movement to cells that are more independent, self-starting and increasingly home-grown. This is exemplified by the perpetrators of the London transit bombings and the thwarted London airline plot. Furthermore, the speed of radicalization has accelerated. Wars in Iraq and in Lebanon provide grievances that make recruitment to radical Islamist groups easier. The proliferation of alternative media outlets and terrorists' use of the internet increase exposure to propaganda and training. Finally, like Afghanistan was for Bin Laden in the 1980s, Iraq provides a theater for the next generation of terrorist leaders to train, make connections, and build reputations.

Engaging Society, Educating the Public and Enlisting the Private Sector

Educating the Public

Faced with the threats of proliferation and global terrorism, one of the most important things we can do as a country is to harness the strength and resolve of our society. The many changes we have made to the organization of the federal government, while essential, will only go so far. The British were renowned for their resolve and determination during the London blitz in World War II. Similarly, the United States will win the war on terrorism, not by force of arms, but by the resolve and resiliency of its citizens.

The inaugural National Strategy for Homeland Security argued that "the Administration's approach to homeland security is based on the principles of shared responsibility and partnership with the Congress, state and local governments, the private sector, and the American people." While the sentiment was and is correct, we have failed to execute on it. I have argued since 9/11 for the need to create a culture of preparedness. For this to happen, we need to view our citizens as the critical backbone of American resolve.

Unfortunately, too many policymakers tend to view the general public not as a source of strength, but as either victims or prone to panic. Given such a view, it is not surprising that the federal government has struggled mightily over how much information to share with the public regarding what to do in the event of terrorist attacks and how to respond depending on the nature of the threat. Too many officials fear that that too much information will frighten the public or aid our enemies.

This discussion should end. The more informed and self-reliant we are when the next attack or disaster strikes, the better off we will be.

The most persuasive recent arguments on this front come from Brian Jenkins of RAND in his new book, *Unconquerable Nation*.[1] According to Jenkins, the federal government's approach to public education and communication has "encouraged dependency" instead of "promoting self-reliance."

> "The best way to increase our ability as a nation to respond to disasters, natural or man-made, is to enlist all citizens through education and engagement, which also happens to be a very good way to reduce the persistent anxieties that afflict us. We have not done this… We need to aggressively educate the public through all media, in the classrooms, at town halls, in civic meetings, through professional organizations, and in volunteer groups. This means more than speeches in front of the American flag. The basic course should include how to deal with the spectrum of threats we face, from "dirty bombs" to natural epidemics, with the emphasis on sound, easy-to-understand science aimed at dispelling mythology and inoculating the community against alarming rumors and panic."

Proposals on Public Education

- Significantly improve the quality of ready.gov so that it contains detailed and deep information on threats, preparedness, and response. To the extent that budgets are limited, ready.gov need not develop information on its own, but should act as a portal that

[1] Brian Michael Jenkins, *Unconquerable Nation: Knowing Our Enemy, Strengthening Ourselves,* RAND Corporation, 2006. For another excellent treatment of the topic see Amanda J. Dory, *Civil Security: Americans and the Challenge of Homeland Security*, Center for Strategic and International Studies, 2003.

organizes and consolidates links and information from sites like those of RAND and the Federation of American Scientists.

- DHS should establish an advisory board, comprising academics and scientists to ensure that materials are accurate and up-to-date, as well as experts on communications, sociology and psychology to ensure that materials are most effective at providing education that empowers our citizenry.
- DHS should increase its efforts to support homeland security education and outreach by trusted public information outlets, including the Red Cross, state and local authorities, and media outlets.

Enlist the Private Sector[2]

Since 2001, the Administration and Congress have repeatedly stressed the critical importance of "public-private partnerships" to make the country safer. Five years after 9/11, such partnership is more hope than reality.

The federal reorganization since 9/11 has raised the difficulty and transaction costs for the private sector to work with the federal government. Information sharing between government and the private sector remains stunted. Overall investment in private sector security initiatives has been modest. The federal government has failed to provide meaningful incentives or standards for securing critical sectors that pose the highest risk and where voluntary efforts have proven to be insufficient. The private sector has not been effectively integrated into response and recovery planning for major disasters, though some promising public-private initiatives have been piloted.

In short, the capabilities, assets, and goodwill of the private sector to bolster our homeland security remain largely untapped. To make America more secure, the federal government urgently needs to provide better leadership on homeland security issues and become a more active partner with the private sector.

When addressing these problems, policymakers should remember that the government is a major market player whose actions can and will affect the ability of the private sector to invest more in security. For its part, the private sector is not just a target, but also an important source for information, assets, and capabilities that the government does not possess.

Policymakers must learn how to harness the deep patriotism and sense of civic duty felt by many American business leaders. American companies are willing to commit their time, expertise, and resources to support the homeland security mission. The federal government must make a concerted effort to recognize and encourage such actions as part of a successful partnership between the federal government and the private sector.

Government engagement of the private sector would preferably be non-regulatory. But, when policymakers and the public feel that voluntary efforts by companies do not achieve adequate security, lawmakers and regulators should make sure to use all of the policy tools at their disposal. Federal standards can provide guidance and help ease industry fears of liability should their security efforts be defeated by a terrorist attack. Tax incentives can make security projects more economically feasible. Finally, Washington must realize that government regulation is not always in conflict with the best interests of the private sector. In many instances, federal action

[2] For a fuller discussion see Steven E. Flynn and Daniel B. Prieto, *Neglected Defense: Mobilizing the Private Sector to Support Homeland Security*, Council on Foreign Relations, March 2006.

can help to bound market uncertainties, making it easier for markets to work and for the private sector to make investment decisions.

Proposals on the Private Sector

- Washington needs to change its policy paradigm regarding the private sector, which, in effect, tells companies to protect themselves. On critical infrastructure issues, Washington needs to provide leadership, not followership.
- Washington must move beyond talking about the need to dramatically improve information sharing with the private sector and hold government officials accountable for actually doing it.
- DHS must strengthen the quality and experience of its personnel. One way to aid in this effort could be to establish a personnel exchange program with the private sector.
- Congress and the administration should work closely with industry to establish security standards and implement and enforce regulations where necessary and, especially, where industry is seeking standards and regulation.
- Congress should establish targeted tax incentives to promote investments in security and resiliency in the highest-risk industries.
- Congress should establish federal liability protections for companies that undertake meaningful security improvements.
- Homeland security officials should substantially increase the number of exercises for responding to catastrophic events. Private sector assets and capabilities should be fully integrated into these exercises, with a view to achieving deeper private sector integration into national and regional emergency response plans.
- Federal response plans should identify specialized supplies/capabilities that will be in short supply following certain types of terrorist incidents or high-consequence events and work with the private sector to ensure the availability of critical supplies and capabilities.
- DHS should establish a federal awards program, modeled after the prestigious Malcolm Baldridge National Quality Awards program, which recognizes private sector achievement and innovation in homeland security.

Move from Tactics to Doctrine

While over a dozen homeland security "strategy" documents have been produced since the 2001, most of them are simply discussions of tactics, methods and processes. This early generation of intended guiding documents generally fails to provide true strategy and doctrine. True strategy documents would clearly set forth priorities, provide definitive guidance for action, and establish goals against which activities and programs can be measured.

In the absence of compelling strategy, too many homeland security programs are ad hoc, reactive, and do not contribute to a coherent vision. In the next five years, tactics and standalone programs must give way to doctrine. This is particularly true in the areas of preparedness and critical infrastructure protection.

Preparedness Doctrine

According to Paul McHale, Assistant Secretary of Defense for Homeland Defense, the United States should assume that we will continue to face traditional military challenges from nation-states and that terrorists will attempt multiple simultaneous mass-casualty CBRNE attacks against the U.S. homeland.

Based on that assumption, the United States should develop a doctrine of homeland security preparedness not unlike prevailing U.S. military doctrine for most of the last 50 years. That doctrine required U.S. military forces to be prepared for two near-simultaneous wars in different theaters. A similar doctrine for homeland security would require the U.S. – DHS, other federal agencies, the National Guard, NORTHCOM and state and local entities – to be prepared to address two to three simultaneous high-consequence events, of the kind envisioned by the fifteen DHS National Planning Scenarios.

Once such a doctrine is established, it would have immediate ramifications for planning.

It would suggest, for example, greater and more specialized training for the National Guard, which has increasingly become the "Swiss-army knife" of homeland security. Creating National Guard "Special Forces" for homeland security would require Guardsmen to receive specific training against certain threat scenarios. Such specialization could occur on a regional basis, depending on event likelihood in a particular geography. For example:

DHS National Planning Scenario	**Geographically Based Training**
Scenario 1: Nuclear Detonation – 10-Kiloton Improvised Nuclear Device	National Capital Region, New York
Scenario 6: Chemical Attack – Toxic Industrial Chemicals	New Jersey
Scenario 9: Natural Disaster – Major Earthquake	California
Scenario 10: Natural Disaster – Major Hurricane	Florida
Scenario 14: Biological Attack – Foreign Animal Disease (Foot and Mouth Disease)	Texas, Missouri, Oklahoma, Nebraska

Improved training, greater specialization, a more sharply defined homeland security mission and free for-credit education at public state universities could provide a powerful incentive and improve recruiting, retention, and morale in the National Guard and Reserve. Training could also leverage existing DHS university centers of excellence.

A second implication of such a homeland security doctrine might be that NORTHCOM would better be able to address multiple simultaneous disaster scenarios if they had their own dedicated resources. They are currently only allocated 1,000 permanent personnel and $70 million. Compare that to DOD's budget in 2004 of approximately $400 Billion and 1.4 million active duty personnel.

In addition, it would be valuable to increase the level of joint training and exercises between National Guard, NORTHCOM, and state and local officials to address specific scenarios.

Proposals on Preparedness

- Establish a homeland security analogue to the military's two-war doctrine.
- Create National Guard Special Forces, providing specialized and regionally-based training against the fifteen DHS National Planning Scenarios.
- Dedicate resources to NORTHCOM.

Critical Infrastructure Doctrine

On critical infrastructure protection, the Homeland Security Act requires DHS to identify priorities, develop a comprehensive national plan, and recommend protective measures.

The latest version of the National Infrastructure Protection Plan (NIPP) fails to meet these requirements. The NIPP identifies obvious, if important tactics – public-private partnership, information sharing, and risk management – but fails to provide the kind of strategic guidance that can coherently guide resource allocation and programmatic activities. We continue to lack a comprehensive strategy for critical infrastructure that meets the requirements of the Homeland Security Act.

Our critical infrastructure efforts suffer from a number of other shortcomings.

First, DHS assumed that the market would provide sufficient incentive for companies to adequately protect critical infrastructure. That has not happened. Washington needs to step up to make sure that we protect critical infrastructure better.

Second, DHS was not granted new authorities, other than what it inherited from legacy offices, for security over vital critical infrastructure sectors. Pending legislation to grant DHS authority over the security of some segments of the chemical industry is a step in the right direction, but more needs to be done. DHS needs to be given authority over security activities at any infrastructure sites that threaten large-scale casualties or are critical to the functioning of the U.S. economy, regardless of sector. So, for example, DHS should have the authority to regulate critical energy infrastructure sites in order to mitigate known vulnerabilities in the electric grid.

Third, Washington has fallen into a kind of "political correctness" over critical infrastructure, as if all sectors pose equal risks. They do not. We must come to consensus on which sectors are more important than others. HSPD-7 started in this direction when it recommended prioritizing critical infrastructure that would have WMD-like effects if attacked. Secretary Chertoff also moved in the right direction when he talked about the importance of risk-based allocations for grant funding. But the failure to definitively establish and articulate clear priorities has been evident in DHS' miscues over the national critical infrastructure database and reductions of grant funding to Washington, DC and New York.

Prioritization of CI sectors should be based on:

- Vulnerability and Consequence. What industries best provide the terrorist trifecta: bodies, symbolism/theater, and economic impact?

- Companies' Ability to Address Vulnerability. Some industries are more capable than others of implementing significant security enhancements on their own and in the near term. The industries least able to protect themselves are those: 1) that exhibit low growth, low profit margins and tight cashflow, all of which limit capital available for investments; 2) whose businesses rely on long-lived capital assets, which are difficult to retrofit or replace easily; and 3) that are not tightly regulated and, therefore, lack a quick mechanism by which the government can simply mandate greater security.

In my judgment, these criteria indicate that the top priorities for critical infrastructure protection are chemical facilities; transportation, including airlines, ports, mass transit, and hazmat transport; and energy, including oil, gas, and the electric grid.

Further critical infrastructure prioritization should also give significant consideration to the geographic location, concentration, and interconnectedness of critical infrastructure.[3]

Fourth, DHS has sharply curtailed its critical infrastructure efforts so that it is now acting largely as a coordinator for the efforts of other agencies. This is a mistake, and in my view fails to carry out the mission Congress and the public expected. In 2004, DHS directed $300 million to critical infrastructure protective actions, including pilot programs, technology applications, bombing prevention, security training and community security planning. In FY07, only $30 million was requested for protective actions, a reduction of 90 percent in three years.

Fifth, the Federal government is failing to use all available policy tools at its disposal to enhance the security of critical infrastructure. It has generally painted a false choice between private sector self-protection and business-harming regulation. The government has failed to creatively use tax policy to promote additional security investments to the extent that it believes that industry, on its own, is not investing enough. Take for example the chemical industry. Often derided as negligent when it comes to security, major chemical manufacturers have spent $3 billion since 9/11 to enhance security, hardly evidence of negligence. If society believes that more security is warranted, the government should catalyze greater investment by providing tax incentives that make security projects more attractive. Had such tax breaks been provided to the chemicals industry soon after 9/11, the legislative debate over "inherently safer technologies" would not have been so protracted, because, I believe, many more companies would have already pursued such projects.

Improving the security of critical infrastructure is essential to the security of the country. Better yet, security investments can benefit the overall health and functioning of critical infrastructures. This helps the U.S. economy and society over the long term. Such "positive externalities" should not be overlooked as the government considers policies to catalyze greater levels of investment in infrastructure security. While our global economic rivals China and India invest scores of billions of dollars into the transportation, energy, and communications infrastructure that will power their economies for a generation, the United States makes due with decades old infrastructure that is brittle and in poor health.

The American Society of Civil Engineers in 2005 provided a national report card on the health of U.S. infrastructure.[4] With an average grade of "D" for aviation, bridges, dams, energy, rail and transit, among others, these infrastructures are more vulnerable to terrorist attack or natural disasters than we can afford, and they will have a harder time recovering after an event.

It is important to remember that the U.S. interstate highway system was built for security reasons and that the Defense Department was responsible for building the precursor network to the internet. Security considerations have always played a significant role in national investments in infrastructure. There is no reason that the same should not be true today.

Proposals on Critical Infrastructure Protection

[3] Paul W. Parfomak, "Vulnerability of Concentrated Critical Infrastructure: Background and Policy Options," Congressional Research Service, December 2005. For an excellent discussion of risk analysis as well as a ranking of the terrorism risks faced by individual U.S. cities see Henry Willis, A. Morral, T. Kelly, and J. Medby, *Estimating Terrorism Risk*, the RAND Corporation, 2005.

[4] American Society of Civil Engineers, *Report Card for America's Infrastructure*, 2005. Available at http://www.asce.org/reportcard/2005/index.cfm.

- Quickly come to consensus on critical infrastructure priorities.
- Use all policy tools available, including a mix of tax incentives, assistance in setting best practices, and smart regulation.
- Grant DHS sufficient authority where it is lacking, not only in chemical security but on facilities that are truly critical at a level of national significance.

Managing DHS for Success

In the next five years, it is critical to stabilize and strengthen new homeland security organizations, especially the DHS. DHS represents a large-scale merger of many agencies in addition to a number of start-up activities. The ability of DHS to manage the integration of these efforts and ensure that the whole of DHS is greater than the sum of the parts relies on a strong and experienced management cadre and the creation of a unified culture. The U.S. Government Accountability Office (GAO) 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. In the private sector, large-scale mergers can take three to five years to work out. Given a much less dynamic government environment, GAO's estimate may be an underestimation.

The birth of DHS has not been easy. For its successes, DHS has suffered significant failures and missteps, which in my view have seriously damaged its credibility. Katrina was its lowest moment, but it has been beset by a number of public missteps on critical infrastructure protection, grant funding, financial management, contract management, and technology; the repeated and frequent missing of Congressional deadlines; high turnover among senior staff; limited expertise among professional staff; difficulty in creating a professional cadre in important areas due to large-scale outsourcing of key strategy and integration tasks to outside contractors and an over-reliance on detailees who maintain loyalty to their home organizations; and general problems of coordination between DHS' disparate parts.

Ineffectiveness or immaturity has led to the subsequent devolution of key functions that DHS inherited only a few years ago. DHS has increasingly diminished, spun off, or shed responsibilities in such areas as intelligence and information fusion, critical infrastructure protection, and post-disaster housing and health. In the most recent federal personnel survey, DHS employees ranked their organization at or near the bottom on nearly every measure of effectiveness. Other departments – Justice, State, DoD – too often do not view DHS as a peer organization.

DHS is falling behind, and the window of opportunity to get things right may be closing. While DHS has made progress in rationalizing many basic operations, too much of DHS lacks strong management and adequate coordination. In the next five years, DHS must resolve key management issues, cease being an umbrella organization, and become a unified enterprise.

If DHS fails to create synergies among the many entities it inherited and to mature into a more effective organization, we will be worse off as a country. If it continues to receive highly critical reviews from its own inspector general and the GAO and unflattering portrayals in the press, if its employees continue to suffer from low morale and confidence in their agency, if it continues to shed key functions with which it was entrusted, and if its fails to improve its reputation among counterpart agencies, then the DHS risks becoming the DMV of the federal government: widely viewed as inefficient and ineffective. Worse yet, criticism of DHS becomes self-fulfilling. The more negatively viewed the organization is, the less effective it becomes.

Presentation of these facts is not meant as an indictment of DHS. Many of the problems were to be expected in a merger integration exercise as large and complex as DHS. My point in raising them is to urge this Committee to do all it can to shepherd the maturation of DHS. It may be necessary to read between the lines when senior DHS officials state that they have all the resources and capabilities they need, rosy scenarios which may be born of political expediency or pride. It also may be necessary to moderate a growing desire to withhold or cut DHS funding as a punitive measure. To the extent that DHS' shortcomings stem from under-resourced or structurally weak management, it is essential to not just use sticks, but to also address the root of the problem by helping strengthen management capability and accountability for the long term.

To improve DHS management, key CxO level positions must be given greater power and more resources. The Chief Financial Officer (CFO), the Chief Information Officer (CIO), and the Chief Procurement Officer continue to lack effective department-wide purview and authority. Some changes implemented by Secretary Chertoff have helped, in particular the creation of a Policy Office and an Office of Strategic Plans, as well as increasing the power of the Deputy Secretary. But an organizational chart that has 22 separate divisions reporting directly to the Deputy Secretary while failing to fully leverage the CxO positions does not make sense. Management control and integration of DHS, in my view, remain far too weak.

Congress plays an important role in DHS management as well, acting in an equivalent capacity to a board of directors. The creation of permanent homeland security committees in both the House and Senate reflect an important step in streamlining Congressional oversight. Katrina provided a galvanizing event that has allowed Congress to be much more assertive on homeland security in this past year. Reports on Katrina as well as bills on ports, borders, chemical security, FEMA, domestic surveillance, and foreign investment in critical infrastructure all demonstrate growing Congressional leadership and assertiveness. Finally, homeland security efforts in this Congressional session appear both more bipartisan and bicameral.

While these are all steps in the right direction, more needs to be done to ensure that Congress provides efficient and effective oversight of DHS' security-related components. For example, the Senate Homeland Security and Governmental Affairs Committee was not given jurisdiction over several key components within DHS, particularly as regards transportation. As advocated by the 9/11 Commission, the Senate and the House homeland security committees should have jurisdiction over all counterterrorism elements of DHS.

Proposals on DHS Management

- Significantly strengthen the DHS management directorate organizationally and with additional resources and deeper experience. Continue to build and strengthen the DHS Policy Office and Office of Strategic Plans.
- Increase coordination between the management directorate, Policy Office, and Office of Strategic Plans, and clearly empower a core "SWAT" team responsible for all integration-related issues and initiatives. Increase working-level interactions between personnel from the offices of Management, Policy, and Strategic Plans with personnel from DHS operating units. More joint interaction on projects and more open dialogue will help build trust, better enable integration-related projects, and establish stronger influence of the DHS Secretariat.
- Continue to streamline Congressional oversight and fully empower Senate and House homeland security committees to have full oversight over all security-related components of DHS.

Getting Technology Right

America is the envy of the world when it comes to technology, but too many homeland security technology projects since 9/11 have faltered, from the FBI's virtual case file and DHS' Homeland Security Information Network to border security systems. We need to better use technology and innovation to protect America. This is true not only on next generation projects like CBRNE detection, but also on migrating mass-market technologies like digital maps and online marketplaces into the homeland security arena.

Outside of the military realm, the federal government is not good at managing technology projects. Too many in government still view IT as obscure work divorced from policymaking and far less important. As a result, government tends to treat the management of technology projects as an afterthought, rather than viewing it as integral to policymaking. In the 1990s, the private sector transformed itself by learning how to deploy advanced technology strategically. The federal government needs to catch up.

While the government in general struggles to implement technology projects successfully,[5] DHS is among the worst performers. According to the GAO, DHS is currently pursuing around 17 high-risk technology projects, of which 15 are suffering performance shortfalls. The 88 percent shortfall rate of DHS high-risk projects is dramatically worse than the average government shortfall rate of 35 percent.

Adding to the homeland security technology problem, the DHS Science and Technology (S&T) directorate faces significant challenges. Weak management and leadership, staffing problems, the absence of coherent long-term strategy, and financial problems have lead to proposed cuts in its budget and calls for its reorganization.

To keep the country safe, we need to make a serious and sustained effort to improve how we deal with homeland security technology. While everyday consumers have benefited significantly from the technology and telecommunications revolution of the late 1990s, the federal government has been left behind. We must recognize the power of technology to solve some of homeland security's most intractable problems.

Take for example, the need to provide better situational awareness to crisis managers, first responders, and the public. A post-Katrina DHS review of state emergency plans, found that most mass evacuation plans remain inadequate and "are an area of profound concern."

The mass market has rapidly adopted digital situational awareness products over the last five to ten years, including online maps with satellite imagery and GPS-based systems in our phones and cars. Think Mapquest, Google Maps, and OnStar. It is not acceptable for the men and women who protect the homeland to be stuck in the dark ages, nor the public they are tasked to help defend.

---

[5] See David Powner, *Information Technology: Improvements Needed to More Accurately Identify and Better Oversee Risky Projects Totaling Billions of Dollars,"* GAO-06-1099T, Government Accountability Office, September 2006. According to the GAO, approximately 300 projects totaling about $12 billion in estimated IT expenditures for fiscal year 2007 have been identified as being either "poorly planned or poorly performing." Specifically, of the 857 major IT projects in the President's budget for fiscal year 2007, OMB placed 263 projects, representing about $10 billion on its Management Watch List. In addition, in response to OMB's memorandum, agencies reported that 79 of 226 high risk projects, collectively totaling about $2.2 billion, had a performance shortfall.

Situational awareness requires a common geographic frame of reference for everyone involved and that can be easily updated as event details become clear. What evacuation and supply routes are open, closed, or destroyed? Where are essential supplies, industrial facilities and oil, gas, electric and communications lines? Where are shelters, hospitals, and churches and are they full? In a real-time terrorist event, such as a dirty bomb or chemical release, knowing whether to go east or west a few blocks can mean the difference between life and death.

To be fair, DHS has realized that good maps are essential to good disaster preparedness and response. Unfortunately, its efforts have fallen short. In 2003/4, DHS launched the Homeland Security Information Network to better communicate with state and local officials. Robust mapping capabilities were to be among its key features. But that functionality ran into trouble and delays almost immediately, and in 2006 the DHS Inspector General found that fewer than ten percent of all users were using the system on a regular basis, in part because it failed to provide useful informational awareness.

It is no surprise then that military resources were called into action by DHS during the response to Katrina. But Homeland Security should not have to beg, borrow and steal from others when it comes to their situational awareness. First-rate digital maps should not be “in case of emergency break glass.” Such capabilities should be in the basic toolkit of homeland security professionals, and they should be readily shared with first responders and state and local officials.

Just as important is empowering the public with geographic situational awareness so they can better plan and make decisions at times of disaster. As we saw in New Orleans, the public is frequently on its own in the immediate aftermath of a disaster, and empowering individuals to create and share response plans with their families or co-workers remains a terribly unmet need.

To ensure that the public benefits from better situational awareness as well, all major print, online and broadcast media should agree on a single map strategy for informing the public before and during an emergency, eliminating duplication of efforts and ensuring as consistent and accurate of an information flow as is possible. Additionally, DHS could establish local “map czars” who are empowered to cut through the bureaucracy to decide what is presented on such maps, including rapidly changing information during a crisis.

Another area where technology could be used much more effectively is in inventorying and coordinating the supply and delivery of disaster response assets. According to a recent report commissioned by the White House after Katrina, the "Achilles' heel" of our national preparedness is the ability, among all those players, to identify critical supplies and resources before a disaster strikes and finding and delivering them quickly afterward.

Everyday technology, properly harnessed, can help address some of the most glaring deficiencies identified by the White House study.

Future disasters envisioned by the Department of Homeland Security will all require specialized response resources, many of which the government will not be in apposition to supply. Federal, state and local governments should identify critical supplies and capabilities – vaccines, ventilators, generators, electric transformers, laboratory capacity, decontamination equipment, logistics, transport, warehousing – that they will need ahead of time.

Building an eBay-like online market mechanism to match regional and national-level disaster-response needs with companies that can pledge assistance ahead of time or help out in real time

would save dollars and lives. Properly built and maintained, it would ensure that the vast majority of private pledges and donations are put to good use, instead of going unused, as happened in Katrina. It would allow state, local and federal governments to inventory available critical assets rapidly and would be much faster than relying on government bureaucrats to create a resource database on their own. Such a system would also serve as a focal point for cooperation between government, the private sector and NGOs. It would allow the establishment of significant cooperation, trust, and interaction in advance of the next disaster so that we are better prepared when the next disaster hits.

Proposals on Technology

- Make it an urgent priority to stabilize and strengthen DHS technology efforts and the S&T directorate. Recruit and build a strong technology management team with a multiyear commitment, and better align S&T activities with the strategic priorities of the DHS.
- Establish a panel of experts, primarily from industry, to advise the Secretary of Homeland Security on technology issues and ongoing technology projects.
- Improve situational awareness by greatly expanding the availability of digital imaging and map capabilities to homeland security professionals as well as to the public directly and via media outlets.
- Drive preparedness with internet based market mechanisms that make it easier to inventory and secure critical response assets from non-governmental actors.

Information Sharing and Counterterrorism Use of Commercial Data

Information Sharing

The President and the Congress have taken bold policy, legal and institutional steps to improve information sharing. Congress enacted the Intelligenec Reform and Terrorism Prevention Act, the President issued Executive Orders to create an Information Sharing Environment (ISE), and new organizations have been created, including the ISE Program Manager within the Directorate of National Intelligence as well as offices and boards focused on privacy and civil liberties.

The ongoing debate over intelligence collection within the United States signifies the challenge to simultaneously protect civil liberties and achieve increased security in an age when governments need more and better information in the face of dynamic and often asymmetric national security threats, as well as communications technologies and globalization which blur traditional notions of national boundaries.

While the information sharing reforms undertaken in the first five years since 9/11 are impressive, they are only a first step. On their own, they are sufficient neither to bring about the needed changes in behavior nor to build the technology systems that are needed to enable better information sharing. To move forward effectively, the government must implement policies to overcome the significant cultural and bureaucratic hurdles that impede information sharing. Better policies, clearer rules, and more robust oversight for sharing intelligence information make us more secure both in our Constitutional rights and against terrorist threats.

To ensure that policy reforms fully translate into changed behavior within critical agencies and departments, leadership from the highest levels of government is necessary. These leaders, including the President and the Director of National Intelligence, need to identify the policies,

rules, procedures, and incentives/disincentives that will promote information sharing and foster the creation of an environment of policies, business rules and technologies that will support it.

Sharing information must become part of the DNA of our intelligence, national and homeland security, and defense communities. It must be woven into the fabric of department and agency cultures, bureaucratic behavior, and standard operating procedures for intelligence and law enforcement, into the education and training of government officials, and into the technology systems that these stakeholders use every day.

Proposals on Information Sharing

I strongly recommend that the U.S. implement the many recommendations of the Markle Foundation Task Force regarding information sharing, including the innovative recommendations of the most recent report.[6]

- Adopt an authorized use standard to protect civil liberties in the sharing and accessing of information the government has lawfully collected; this standard would replace existing outdated standards based on nationality and place of collection.
- Take a "risk management" approach to classified information that better balances the risks of disclosure with the risks of failing to share information.
- Create a government-wide dispute resolution mechanism to facilitate responsible, consistent, and lawful information sharing.
- Develop tools, training, and procedures to enhance the use of the information sharing environment and its technological capabilities by line analysts and by senior officials.
- Expand community-wide training, modern analytic methods, and new tools to enhance the quality of information sharing and analysis.
- Encourage the use of new technologies such as anonymization, and the use of expert and data directories.
- Employ immutable audit systems to facilitate both accountability and better coordination of analytical activities.

Reaching Consensus on the Use of Consumer and Company Data for Counterterrorism

In May 2006, it was revealed that the NSA was augmenting domestic surveillance with large-scale data analysis of consumer telephone toll records. That revelation was only the latest instance of government efforts to use data mining and other technology techniques in the war on terror. A 2004 survey by the U.S. Government Accountability Office found 199 non-classified federal data mining projects, a number that would grow if classified projects were included.

Many of these programs have raised little controversy. Cargo security programs analyze volumes of shipper and cargo manifest data. Companies as diverse as FedEx, Western Union and AOL have been helping the federal authorities and law enforcement by allowing them to look at portions of their customer and subscriber data. Other experiments – including the Defense Department's Total Information Awareness (TIA) program and TSA efforts to use commercially-

[6] *Mobilizing Information to Prevent Terrorism: Accelerating Development of a Trusted Information Sharing Environment*, Third Report of the Markle Foundation Task Force, June 2006. *Creating a Trusted Information Network for Homeland Security*, Second Report of the Markle Foundation Task Force, December 2003. *Protecting America's Freedom in the Information Age*, First Report of the Markle Foundation Task Force, October 2002.

available consumer data in airline passenger screening – raised public outcry and privacy concerns and were shut down by Congress.

There is ongoing controversy over the government's use of private sector and consumer data for counterterrorism purposes. While privacy advocates cry foul, many Americans see little problem. A Washington Post-ABC News poll following the revelations about NSA "data mining" found that 63% of Americans supported the program.

The growth in data analysis efforts marks the recognition of a simple truth: our spies are not well suited to address the jihadist terrorist threat. We are short on Arabic language skills, community ties, and cultural knowledge that would allow our spies to infiltrate increasingly independent and decentralized cells. How, for example, would an American spy ever hope to penetrate a group like the home-grown London subway bombers? Faced with that reality, the growing use of data-analysis techniques to fight terrorism makes sense.

At the same time, government programs that analyze commercial data are imperfect and risk the wrongful entrapment of innocent citizens along with legitimate terrorists. That risk is magnified by the fact that the laws governing these programs are unclear. To the extent data is mishandled, misused or leads to false positives that are difficult to redress or correct, confidence in government is eroded.

Furthermore, the lack of a crystal clear legal framework to govern data analysis and data mining programs puts government intelligence professionals at risk. It makes intelligence officials more likely to mistakenly violate individual civil liberties and privacy laws, making them more vulnerable to lawsuits and accusations of abuse.

We need to move beyond an environment where it seems that different executive-branch agencies are simply experimenting with large-scale data analysis techniques to see what works and what they can get away with. In the next five years, we need to move past experimentation and develop comprehensive legislation, guidelines and rules to govern the growing use of consumer and company data in the fight against terrorism.

Government's use of consumer data is currently governed by a raft of disparate and piecemeal rules. Among many others, these include the Privacy Act and the E-Government Act, the Federal Information Security Management Act, the financial Modernization Act, and Patriot Act amendments to the Fair Credit Reporting Act. Various other bills, including ones on consumer data privacy and data brokers, could add to the confusion.

Similarly, there is a risk of conflicting regimes regarding critical infrastructure information. The recently finalized Protected Critical Infrastructure Information (PCII) could very well come into conflict with the sector-specific data protection regimes contemplated in chemical (S. 2145 and HR. 5695) and port security (S. 2459 and HR. 4954) bills.

Within the next five years, balkanized rules for the government's use of company and consumer data need to be addressed. Any attempt to harmonize or create a unified regime for the use and sharing of industry and consumer data for terrorism-related purposes will need to comprehensively address the government's handling and management of data from "cradle to grave." It should address the full data lifecycle: procurement, receipt, storage, use, ability to combine with other data, sharing within government, sharing with government contractors, encryption, anonymization, dispute, and redress.

The Government's use of consumer and industry data for counterterrorism purposes will continue to grow. Clear and consistent rules to govern this activity are needed so that Americans don't have to feel that the only relationship between civil liberties and security is a zero-sum game.

Conclusion

Are we safer? At the five year anniversary of 9/11, the question is unavoidable.

In many ways the answer is yes. The U.S. has not been attacked again on U.S. soil. We have successfully degraded Al Qaeda Central and are cooperating successfully with allies to detect and thwart additional attacks. Our defenses at home are stronger. We embarked on the largest reorganization of the federal government since 1947. We have sought to improve information sharing with new laws and new institutions. We have sought to make it easier to find terrorists through the innovative use of data analysis technologies while at the same time seeking to protect our values with a the creation of new privacy and civil liberties boards and offices. Airline security has been boosted. Private chemical manufacturers have invested billions on greater security since 9/11. Nuclear plants have raised security at the behest of the Nuclear Regulatory Commission. Add to these measures a higher level of public awareness and vigilance, and in many ways we are safer.

But in many ways, we are not.

The world has not stood still since 9/11. Nuclear proliferation is a growing threat, and global jihadist terrorism is adjusting and evolving. At home, our security efforts are still very much in their infancy. The emblem of our shortcomings is Katrina, with all of the significant gaps it exposed in our leadership, preparedness, coordination, and effectiveness to deal with even widely foreseen homeland security threats. We face other significant challenges going forward. DHS struggles to meet the expectations that came with its creation. Chemical plants and ports are still not secure enough. Transit authorities can't find enough money to implement desired security measures. We lack a national consensus on priorities and our strategies are not robust, leaving us with uncoordinated programs and in a perennial state of reacting to the latest threat. A number of big-ticket homeland security technology projects have faltered. Innovative but controversial "data mining" programs to enhance security are forcing the tradeoff of liberty for security in an unnecessarily zero-sum game.

"Is it safe?" Dustin Hoffman's answer to that question in the famous 1976 movie, *The Marathon Man*, was alternately "yes, "no," and "it depends." For every area of progress, significant gaps and vulnerabilities remain. Over the next five years, we must do more and do better.

In five years time, we should all hope to see:

1. A much better educated and empowered public on homeland security issues.
2. A private sector that works in much fuller partnership with the government in protecting the country.
3. A clear doctrine of national preparedness that requires us to be ready to address multiple simultaneous high-consequence homeland security events.
4. Critical infrastructure is more secure as a result of a mix of government incentives, standards and regulations. Chemical facilities are more secure. The electric grid is less brittle. All forms of transportation, not just airplanes, are less vulnerable and attacks are more resilient. Better investments in security have improved the overall

health of American critical infrastructure. This provides long-term benefits to our overall economy and society.

5. A DHS that is a healthy and respected organization, equal to the task Americans expected of it when it was created.
6. We are doing a better job of using technology to secure the homeland. DHS is able to field top-notch technology executives, professionals, and managers.
7. Information sharing is robust and accountable.
8. The privacy debate over government's use of commercial and consumer data for counterterrorism has reached equilibrium. The federal government has greater ability to look for terrorists, but also has greater accountability for its actions.

Bill Gates, the founder of Microsoft, has said that we always overestimate the change that will occur in five years and underestimate the change that will occur in ten. While we have made progress on homeland security in the first five years, many of us are frustrated by the pace of change and what we have not yet achieved. In the next five years, we have the opportunity – in fact, we have the duty – to make every effort to ensure that America is safer and more secure. Five years from now, I hope we have exceeded our own lofty expectations.

Daniel B. Prieto is Senior Fellow and Director of the Homeland Security Center at the Reform Institute. He is co-author, with Stephen E. Flynn, of *Neglected Defense: Mobilizing the Private Sector to Support Homeland Security*, a Council on Foreign Relations special report. He is also a contributing author to two books, *The Forgotten Homeland* and the forthcoming *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*. Previously, Mr. Prieto was Research Director of the Homeland Security Partnership Initiative and Fellow at the Belfer Center for Science and International Affairs at Harvard University's John F. Kennedy School of Government. He is a former investment banker and technology industry executive and is a past recipient of the International Affairs Fellowship from the Council on Foreign Relations. Mr. Prieto is an associate member of the Markle Foundation Task Force on National Security in the Information Age. He holds and M.A. from the Johns Hopkins University School of Advanced International Studies (SAIS) and a B.A. from Wesleyan University.