America at Risk

A Homeland Security Report Card

About the Progressive Policy Institute

"One person with a belief is a social power equal to ninety-nine who have only interests."
—John Stuart Mill

The mission of the Progressive Policy Institute is to define and promote a new progressive politics for America in the 21st century. Through its research, policies, and perspectives, the Institute is fashioning a new governing philosophy and an agenda for public innovation geared to the Information Age.

This mission arises from the belief that America is ill-served by an obsolete left-right debate that is out of step with the powerful forces re-shaping our society and economy. The Institute advocates a philosophy that adapts the progressive tradition in American politics to the realities of the Information Age and points to a "third way" beyond the liberal impulse to defend the bureaucratic status quo and the conservative bid to simply dismantle government. The Institute envisions government as society's servant, not its master—as a catalyst for a broader civic enterprise controlled by and responsive to the needs of citizens and the communities where they live and work.

The Institute's work rests on three ideals: equal opportunity, mutual responsibility, and self-governing citizens and communities. Building on these cornerstone principles, our work advances five key strategies to equip Americans to confront the challenges of the Information Age:

Restoring the American Dream by accelerating economic growth, expanding opportunity, and enhancing security.

Reconstructing our social order by strengthening families, attacking crime, and empowering the urban poor.

Renewing our democracy by challenging the special interests and returning power to citizens and local institutions.

Defending our common civic ground by affirming the spirit of tolerance and the shared principles that unite us as Americans.

Confronting global disorder by building enduring new international structures of economic and political freedom.

The Progressive Policy Institute is a project of the Progressive Foundation. For further information about the Institute or to order publications, please call or write:

600 Pennsylvania Avenue, SE, Suite 400 Washington, DC 20003
E-mail: ppiinfo@dlcppi.org × WWW: http://www.ppionline.org/
Phone (202) 547-0001 × Fax (202) 544-5014

America at Risk

A Homeland Security Report Card

July 2003

Contents

Introduction

"The U.S. government has no more important mission than protecting the homeland from future terrorist attacks."—President George W. Bush, July 16, 2002[1]

On September 11, 2001, Americans learned a bitter lesson: Our unparalleled military power may prevent other nations from threatening us, but it cannot deter global terror networks. Catastrophic terrorism is a means by which the weak can inflict horrendous damage on the strong. It demands a two-fold response: destroying terrorist havens abroad, and mobilizing American ingenuity and resources to dramatically heighten our vigilance against attacks in our own homeland.

The Bush administration for the most part rose to the first challenge, destroying al Qaeda bases in Afghanistan and routing their Taliban protectors.[2] But on the equally urgent task of building up America's domestic defenses, it has been a very different story.

In fact, the contrast could not be more striking. While energetic in waging war abroad, the Bush administration has been oddly lethargic in fortifying our defenses at home. Instead of leading the charge to revamp our domestic security agencies, for example, it consistently dragged its feet and brought up the rear. Instead of sparing no expense to make Americans safer, it cut taxes and begrudged our police, firefighters and other front-line defenders the resources they need to secure the home front. Instead of setting strategic priorities for homeland security, it advised Americans to stock up on duct tape and set up a color-coded alert system that has only spread alarm and confusion.

The challenge of defending the homeland against attack by foreign terrorists is unprecedented. Neither the government nor the citizens of the United States had been forced to think about this particular threat before Sept. 11, despite warnings from experts that the country was vulnerable to a major terrorist attack.[3] This new focus on homeland security has brought new social, political, legal, and organizational tensions to the fore. The nation rallied around President Bush when he promised that immediate action to secure the homeland would be his top priority.

It has been nearly two years since the attacks, and it is time to examine the progress that the administration has made toward improving homeland security. To that extent, PPI examined seven major categories and 28 subcategories of homeland security policy and graded the administration's efforts in each to create this report card. Letter grades were given to each subcategory based on analysis by PPI staff and discussion with outside experts and government employees, and were then converted to numbers on a standard four-point scale, with "A" worth four points. The numbers were then weighted to reflect relative importance, and averaged to create the final grades. (See the Appendix for a full explanation of the methodology for determining the grades and averages.)

In spite of satisfactory results in a few areas, taken as a whole, the Bush administration's efforts to protect the homeland have been surprisingly lax and inadequate, earning an average grade of "D." We find that the Bush administration has not brought the same energy and attention to homeland security that it has brought to overseas military efforts. The administration has failed to adequately fund a number of essential homeland security functions. In the absence of presenting a compelling vision of the changes necessary to protect the homeland, the Bush administration has failed to push back on the government bureaucracies that have resisted meaningful change. In short, President Bush has failed to

fulfill his promise to make homeland security his top priority. Meeting the new challenge of homeland security requires strong leadership, creativity, and vision; President Bush has demonstrated few of these qualities on the home front.

Some may argue that the Bush administration should be given more time to make progress on homeland security, that expecting significant improvements in our safety would be too much to expect since the Department of Homeland Security (DHS) has only been in existence for half a year. It is important to remember, however, that legislation creating DHS would have been enacted long before if it had not been for the many months of opposition by President Bush and now-Secretary Tom Ridge (who said he would recommend that the president veto any bill creating DHS).[4] Moreover, the agencies with responsibility for homeland security, many now folded into DHS, existed even before the creation of the new department. Therefore, it is entirely appropriate to judge the president's efforts dating back to that fateful day in September. Taken together, these grades present a comprehensive picture of the administration's homeland security efforts, highlighting successes where they exist and pointing to areas where improvement is needed to keep the nation safe.

Bush Administration Homeland Security Report Card

1. Improving Intelligence Gathering and Analysis ..... D
- *Coordinating Inter-Agency Intelligence ..... C-*
- *Integrating Terrorist Watch Lists ..... F*
- *Developing Counterterrorism Database Systems ..... D+*

2. Improving Security at the State and Local Level ..... D-
- *Completing a National Threat Assessment ..... F*
- *Sharing Information with State and Local Governments ..... D*
- *Defining the Role of State and Local Officials ..... D*
- *Providing Financial Support for State and Local Governments ..... D-*
- *Boosting Citizen Preparedness ..... D+*

3. Controlling the National Borders ..... D
- *Tracking Entry and Exit of Foreign Visitors and Students ..... D*
- *Improving the Identification System ..... F*
- *Improving Visa Issuance and Consular Services ..... D*
- *Securing Ports of Entry ..... C*

4. Protecting Critical Facilities ..... D+
- *Enhancing Aviation Security ..... C-*
  - Passenger Security ..... B-
  - Baggage Security ..... C+
  - Personnel Security ..... D
  - Air Cargo Security ..... D-
- *Securing Nuclear Plants and Materials ..... C+*
  - Nuclear Power Plant Security ..... A
  - Nuclear Material Security ..... D
- *Securing Chemical Production and Storage Facilities ..... D-*
- *Boosting Cybersecurity ..... D+*

5. Protecting Against Bioterror Attacks C
- *Developing Bioterrorism Countermeasures ..... C-*
- *Expanding Health Care Surge Capacity ..... C*
- *Updating Public Health Laws ..... C*

6. Defending Civil Liberties and Privacy ..... C-
- *Detaining Suspected Terrorists ..... C-*
- *Protecting Privacy ..... C*

7. Managing the Improvement of Homeland Security ..... D+
- *Reorganizing the Federal Government ..... C-*
- *Launching the Department of Homeland Security ..... C*
- *Learning Lessons from Previous Attacks ..... F*

OVERALL ..... D

1. Improving Intelligence Gathering and Analysis
Final Grade: D

Of all the functions and capabilities encompassed in the term "homeland security," none is more important than intelligence. The ability to respond to a terrorist attack and minimize the loss of life is critical, but it is far better to disrupt terrorist plots before the attacks occur. Stopping terrorists requires the ability to gather intelligence on potential terrorists, analyze that information to see how the pieces of the puzzle fit together, and share the information with those who can thwart the attacks. This section examines the Bush administration's efforts to improve intelligence capabilities.

Coordinating Inter-Agency Intelligence C-

The Sept. 11 attacks exposed a deep problem with the federal government's capabilities for domestic intelligence gathering and analysis. The Central Intelligence Agency (CIA) is forbidden from engaging in domestic intelligence, and the Federal Bureau of Investigation (FBI) has traditionally been focused far more on criminal investigations than counterterrorism. This case-driven law enforcement mission is far different from the counterterrorism mission, which is focused on intelligence gathering and analysis—"connecting the dots"—rather than throwing people in jail. It is fair to say that before Sept. 11 the FBI had fairly limited domestic counterterrorism capabilities.[5] These structural flaws were exacerbated by incompatible and outdated information technology systems, hoarding of intelligence from other intelligence agencies, lack of priorities on counterterrorism, and institutional rivalries that hamstrung what little cooperation existed.

In response, Congress mandated that the Department of Homeland Security (DHS) create an Office of Information Analysis that would serve as a central clearinghouse for intelligence gathered by the agencies. The Bush administration has not followed through on that mandate, but rather created the Terrorist Threat Integration Center (TTIC). This new organization falls under the Director of Central Intelligence and gives the FBI, DHS, and other agencies varying degrees of responsibility. Thus far, TTIC has not fulfilled its promise. The turf battles fueled by this arrangement were evident even before the May 1, 2003, launch, when the FBI frustrated the CIA by failing to appoint a representative.[6] Further, instead of vesting threat assessment, vulnerability analysis, and public advisory responsibilities in a single entity as the law requires, TTIC carries out threat assessment, while vulnerability analysis and communications are DHS's responsibility. Indeed, the cultures of the CIA and FBI lean toward limited information sharing, especially outside of federal agencies. Additionally, on May 13, DHS ceded authority over terrorist financing investigations to the FBI, further dispersing terrorism intelligence responsibilities.[7] And while TTIC has access to all of the government's raw intelligence data, DHS has access only through its representatives at TTIC and has thus far been stymied in obtaining CIA intelligence reports.[8] Other top secret or higher levels of intelligence are unavailable because the DHS Office of Information Analysis lacks the proper secure technology.[9] Moreover, House Select Committee on Homeland Security Chairman Christopher Cox (R-Calif.) recently noted that the development of TTIC does not nullify DHS's responsibility to create a similar analysis center, a position affirmed by Secretary Ridge.[10]

The administration has made some progress in coordinating with state and local officials through the creation of 66 Joint Terrorism Task Forces. FBI Director Robert Mueller has pledged to beef up

the FBI's counterterrorism capabilities.[11] Though it is impossible to know what is happening inside the agency, some experts are skeptical that the FBI is capable of transforming into a domestic counterterrorism intelligence agency. The limitations of the agency's ability to communicate across jurisdictions was revealed during the Beltway sniper investigation in October 2002, where a lack of information technology and a confused command structure hindered the effort to capture the perpetrators.[12] Moreover, without strong leadership from the top, it will be extremely difficult to change the culture within the FBI that disdains counterterrorism work. According to Greg Treverton, former vice chairman of the National Intelligence Council, "In the pecking order of the FBI, if you don't carry a gun, [or] if you're not a special agent in charge, you're a second-class citizen."[13] Federal efforts at information sharing generally involve lateral communication between federal agencies, with information only sometimes shared with states and localities; moreover, states and localities are by and large ignored as a source of intelligence.

Unfortunately, the White House has been timid about standing up to the various agencies to do the one thing that can bypass these problems: create an entity that can perform the essentially new function of domestic intelligence gathering and analysis. Such an agency (perhaps modeled on the British MI-5) would cut across institutional rivalries and legal barriers to detect and disrupt terrorist plots before they occur, rather than investigating them after the fact. The congressional Joint Inquiry into the Terrorist Attacks of September 11, 2001, recommended the creation of a cabinet-level Director of National Intelligence, with "the full range of management, budgetary and personnel responsibilities needed to make the entire U.S. Intelligence Community operate as a coherent whole."[14] (Some experts believe that the problems exhibited with the launch of DHS indicate that intelligence capabilities should be developed within existing agencies before splitting into a separate agency, to avoid a "vulnerability gap" in the time it takes to create the new entity.) Whatever the preferred solution, it is clear that fundamental change in the intelligence bureaucracy is necessary. Until the administration acts aggressively to remake our domestic intelligence capabilities, improvements in existing agencies will be only minor steps in the right direction.

Integrating Terrorist Watch Lists F

Terrorist watch lists provide a clear and simple way for front-line public safety officers to identify potential known terrorists. Eighteen months after Sept. 11, the General Accounting Office noted that among nine different federal agencies there exist 12 different lists, which vary widely in their scope, content, and availability.[15] It is widely agreed that integrating these lists and ensuring proper access is a very important step in securing the nation.

While integrating terrorist watch lists is not technologically difficult, the administration has failed to do so despite congressional funding for the task. This is largely because it has been unwilling to exert the leadership necessary to overcome the bureaucratic morass that holds up this simple and vital element of securing the homeland. While some effort was initially made to populate the Transportation Security Administration's (TSA) watch lists with names from other agencies, Secretary Ridge still identifies watch-list integration as one of the department's great, unmet tasks.[16]

To accomplish this task, it is not enough to simply deploy technology; rather, the Bush administration needs to undertake a serious examination of the rules by which names are added to an integrated watch list (to prevent agencies from hoarding information during their investigations) and the rules under which the names on the watch list will be disseminated. The National Crime Information Center (NCIC), the national database of wanted criminals, is currently tasked with distributing terrorist watch list information to local law enforcement, and changes in visa application procedures will require consular offices to check the lists. For an integrated watch list to be effective, the administration needs to resolve the questions of who will get watch list information and how. In particular, if an intelligence agency is reluctant to

name a terrorist to state and local law enforcement for fear of jeopardizing an ongoing investigation, they should still be able to track watch-listed suspects with a "silent hit" system that notifies the intelligence agency when a law enforcement officer has queried a database about the suspect. Thus, when a potential terrorist is pulled over for something like a traffic violation (as at least two of the Sept. 11 pilots were in the weeks before the attacks), the investigating agency will be told of the location and time of the stop.[17]

Developing Counterterrorism Database Systems D+

The investigation into the Sept. 11 attacks shows, albeit with 20/20 hindsight, that the information necessary to disrupt the hijacking plot was available before the attacks, but there was no way to assemble the data to form a picture of the plot.[18] The biggest barrier to putting together those pieces is bureaucratic "stovepiping" of information, a system where information travels only up and down the chain of command and not across a network of law enforcement agents who might be able to put the pieces together.[19] Effective counterterrorism requires effective communication both within and between the agencies fighting the war on terrorism, and the best way to facilitate that communication is through a database system for storing and retrieving information on terrorist investigations and an ability to access data routinely collected by federal agencies charged with homeland security functions (e.g., data on entry and exit of foreign visitors). Indeed, efficiently exploiting the great U.S. strengths in information technology will be a critical component in defending the nation, but so far the Bush administration has done little in this regard.

The Bush administration has chosen not to create a comprehensive interagency database, electing instead to invest money in badly managed upgrades to existing systems. The federal government spends a total of $50 billion per year on information technology, but as the Markle Foundation Task Force on Information Security in the Digital Age pointed out, "almost none of this is being spent on how to solve the problem of how to *share* this information and intelligence among these federal agencies."[20] The FBI, for example, was granted an additional $78 million to hasten the deployment of its hardware, software, and network modernization project, Trilogy. However, real progress has been made only on deployment of desktop hardware and network elements—the actual software used to share information will not be ready until 2004. The Department of Justice's own inspector general determined that slipshod management delayed the program 10 months and caused a $60 million cost overrun.[21] This may be due to lack of overall leadership, as the administration has not yet compiled a plan for government-wide intelligence integration, while the FBI and other agencies have expanded individual programs without effectively integrating them across agency lines. Even DHS has been investing with an eye toward DHS-wide "meta data," not government-wide standards.[22] It is not just that the administration has failed to focus on creating a homeland security information network, but that the basic IT tools the agencies need to fight terrorism are in many cases years behind the best practices in the private sector. For example, a recent report by Hoover Institution fellow Bruce Berkowitz underscores the woeful condition of information technology at the CIA.[23]

The newly renamed Terrorism Information Awareness project, or TIA, (formerly Total Information Awareness) is aimed at developing a "data-mining" system that can use computers to help assemble the puzzle pieces, but it is far from functional, and an effort to defund the program is currently underway in the Senate.[24] (The TIA project has also raised serious privacy concerns, discussed in Section 6.) But at the same time, technologies such as NCIC lack the physical capacity to store the information required by the homeland security mission. The essential test of the Bush administration's commitment to efficient intelligence processing will be the effort to deploy technology for a homeland security mission, an effort that is so far lacking.[25]

2. Improving Security at the State and Local Level
Final Grade: D-

National security is a federal responsibility, and in times of war it is the federal government that takes control on the front lines. In the war on terrorism, though, the front lines are frequently within our borders. In the Sept. 11 attacks, it was local police and firemen who responded to help the victims, and it is state and local governments that are patrolling our streets on the lookout for further threats. Improving homeland security, then, cannot be done simply by reshuffling bureaucracies in Washington. The federal government needs to support state and local governments in their homeland security functions. This section analyzes the Bush administration's efforts to provide that support.

Completing a National Threat Assessment F

A comprehensive National Threat Assessment is a key component of a homeland security plan. The assessment should determine the relative risk and vulnerability presented by major targets in each state. While some locations within the United States face the real risk of imminent attack, other areas face little or no risk of imminent danger. Completing this threat assessment and disseminating specific threat-related information to the jurisdictions specifically at risk should be a top priority of the federal government. Congress has mandated that DHS "identify and assess the nature and scope of terrorist threats to the homeland … and understand such threats in light of actual and potential vulnerabilities of the homeland." The DHS is to do so by conducting "comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States, including the performance of risk assessments to determine the risks posed by particular types of terrorist attacks within the United States."[26]

Unfortunately, the Bush administration is nowhere near completion of a comprehensive national threat and vulnerability assessment.[27] In the absence of a unified assessment, the federal government is operating under the de facto assumption that every facility in every state is equally at risk of being attacked. As a result, the national threat level is elevated based on non-specific chatter; the allocation of funding to state and local entities is decided in some cases using population-based formulas; and training scenarios are often simply based on the imagination of the planners rather than the actual dangers likely to be faced by agents in a particular location. This is an inefficient and dangerous way to conduct the business of homeland security.

The Bush administration's failure to direct and assist the states in the development of a comprehensive threat assessment in the nearly two years since the Sept. 11 attacks is baffling, particularly since much of the relevant data is readily available.[28] Without this information, the administration and the state and local governments who rely on Washington for threat evaluation have been flying blind. Many of the administration's other failures on the homeland security front can be tied to this failure.

Sharing Information With State and Local Governments D

In the months immediately following the attacks of Sept. 11, the Bush administration took a number of steps to improve the sharing of homeland security-related information with state and local governments. These included expanding state and local representation on Federal Joint Terrorism Task Forces and establishing Anti-Terrorism Task Forces in each state (though it is still in doubt whether many of these task forces are truly "joint" or are operated at the pleasure of the FBI). Additionally,

DHS established a five-color Homeland Security Advisory System intended to allow the federal government to notify state and local entities when increased vigilance is necessary without compromising the sources and methods used to obtain the information.

Despite a great deal of rhetoric, many state and local officials believe that the administration's efforts have not led to significant improvements in information sharing between federal, state, and local entities since the Sept. 11 attacks. The terror alert system in particular has been a disaster, forcing states to spend millions of dollars for increased security during times of heightened alert with no specific information as to the viability of the threat. Instead the system just rotates between two levels: an "elevated" and "high" risk of terrorist attack. The color-coded terror alert system is ineffective and should be scrapped completely.[29]

With no national leadership and little funding, most states still have not linked key law enforcement information systems so that they can better "connect the dots," and no effective system exists to help counterterrorist agents gather the information collected by state and local agencies and law enforcement officials. To the extent that the federal government has agreed to share information through the Joint Terrorism Task Forces, the administration has been slow to complete the necessary background checks so key state and local personnel can be provided with specific information relevant to their jurisdictions.

In response to this lack of federal effort, some states are developing bilateral and multilateral sharing arrangements.[30] This is a reasonable response to the failure of the Bush administration to provide federal leadership (as opposed to mere funding) on information sharing, but is not the best way to accomplish the goal. More effort is needed from the administration to address this issue.

Defining the Role of State and Local Officials D

For the most part, Washington has recognized the vital role state and local governments play in serving as our nation's "first responders." But Washington is just beginning to circulate a draft National Response Plan that identifies how federal, state, and local entities would work together to respond to a terrorist attack.[31] The DHS is just beginning to develop standards to provide consistent incident management processes nationwide. And, despite a great deal of rhetoric, the independent radio systems used by the vast majority of our nation's first responders still are not interoperable.

Furthermore, **the Bush administration has virtually ignored the fact that state and local authorities also play a critical role in detecting and preventing future terrorist attacks.** The fact that a terrorist cell is operating in this country may be first uncovered by a local police officer or a member of the community. Counterterrorism and crime control efforts must be linked; we know that terrorists work with crime organizations and often use traditional crimes such as drug and illegal weapons trafficking, money laundering, and bank robbery to offset costs and further support their political/terrorist objectives.

Exclusively defining counterterrorism as a domestic intelligence issue and crime-fighting as a law enforcement issue creates artificial barriers that are unnecessary and even dangerous, yet today that is the approach the federal government is taking. There is a growing consensus among local police chiefs that the same information-driven, community-based efforts that have proven effective in preventing crime may be our best hope for preventing future terrorist attacks, and improving these capabilities will give a dual benefit of reduced crime and terrorism prevention.

Providing Financial Support for D-State and Local Governments

The Bush administration and the Republican-led Congress have made homeland security an unfunded mandate. Nearly the entire burden of heightened security falls upon state and local governments, who must pay overtime to the first responders who go on alert. A recent study by the U.S. Conference of Mayors projected that the weekly cost to the nation's cities for operating at heightened security under the code orange alert exceeds $70 million. During the May 2003 elevation to level orange, some localities did not have the resources to increase security operations. This would

be unfair in the best of times, with healthy state budgets and police forces that are not shrinking (and further depleted by reserve deployments to Iraq[32]). However, in these times of economic crisis and war, the economic costs caused by the Bush administration's inaction is even worse.

The Bush administration's funding for emergency responders is woefully inadequate. In a report entitled *Emergency Responders: Drastically Underfunded, Dangerously Unprepared*, the Council on Foreign Relations estimates that the White House has budgeted only one-third of the amount necessary to prepare for the next terrorist attack, with an unmet need of up to $98 billion.[33] What little support the states have received from the federal government is distributed through inefficient funding allocation formulas that were developed by DHS with no regard for actual risks and threats because no threat assessment has been done. This lack of federal support is even more troubling because the administration is missing an excellent opportunity to reduce crime overall by modernizing the law enforcement infrastructure, particularly their information technology systems, an important side benefit of well-planned homeland security spending.

This problem cannot be dismissed, as Bush has dismissed so many other complaints by governors and mayors, as state and local officials come looking for federal handouts to relieve their budget woes. National security is fundamentally a federal responsibility, and while Bush has been aggressive overseas, he has abdicated that responsibility on the home front without providing the funds necessary for states and localities to pick up his slack. The administration's refusal to fund state and local governments in a sufficient and efficient manner has left the nation more vulnerable to terrorist attack.

Boosting Citizen Preparedness D+

In any terrorist attack, the preparedness of first responders is important, but equally important is a prepared citizenry. Instructing the public on how to react is a key factor in mitigating natural disasters and other emergencies; Americans are taught starting in elementary school how to react to everything from a house fire to an earthquake. This preparedness is key to reducing panic and saving lives, and it needs to be applied to terrorist attacks as well.

Unfortunately, the administration's main effort, the *Ready.gov* website, which purports to give advice in the event of terrorist attack, is lacking in detail and is at times contradictory. The site has been used more as a source of humor than as a source of preparedness information; duct tape is now a well-known punchline. The website itself discourages citizens from using it as a source of information; the Terms of Use declare that the DHS "[is] not responsible if information that we make available on this site is not accurate, complete or current . . . any reliance upon the material found on this site will be at your own risk."[34]

A proper citizen preparedness program would include a threat warning system that gives specific information about the reasons the government has decided to increase the threat level (i.e., intelligence that indicates an attack on airports is in the works). The threat level should never be raised merely to cover bureaucratic bases in the event of an attack. The *Ready.gov* website should include region-specific information (such as highway escape routes, local radio stations for information, and so on) that citizens can access by entering their zip code on the front page. The website should also include additional expert advice on how to deal not only with the effects of various kinds of attacks, but with the confusion and panic that will inevitably follow.

The administration has also failed in its responsibility to create effective volunteer organizations to deal with attacks. President Bush announced his intention to triple the number of volunteers in Community Emergency Response Teams (CERT) that could respond in the event of an attack to help save lives.[35] The CERT program is an excellent idea that was in place before the Sept. 11 attacks, and it should be expanded just as President Bush promised. **However, the administration has not pressed Congress for adequate funding to meet this promise to support volunteer efforts in the war on terrorism.**[36]

3. Controlling the National Borders
Final Grade: D

The best way to prevent terrorist attacks on U.S. soil is to stop terrorists and their weapons from entering the country in the first place. Unfortunately, our borders are extremely porous and our methods of keeping track of foreign visitors extremely weak. Gaining control of the borders is a long-term project made more urgent by the war on terrorism. This section examines the Bush administration's efforts to close our borders to terrorists.

Tracking Entry and Exit of Foreign Visitors and Students — D

In the wake of the Sept. 11 attacks, Congress passed the Enhanced Border Security and Visa Entry Reform Act.[37] Among other provisions, the Act requires the Immigration and Naturalization Service (now reorganized as a part of DHS) to issue "smart visas" with biometric identifiers, check visitors against integrated lookout lists, and track the entry and exit of foreign visitors. The Act also directs the administration to accelerate implementation of the Student and Exchange Visitor Information System (SEVIS), the database used to ensure that visitors who enter the country on student visas do in fact attend their stated institutions.

The student tracking program was initiated in 1996 as a reaction to the first bombing of the World Trade Center, but final implementation had been intentionally delayed by some players within the Bush administration who are ideologically opposed to the system because of a belief in open borders and limited government.[38] The SEVIS system went online in early 2003 and since then has been plagued by technical difficulties—a vexing situation given that the pilot program had been extremely successful but was radically changed by the Bush administration in an effort to kill the system entirely.[39] Given the similar task of tracking entry and exit of foreign visitors, the Department of Justice rolled out a pilot program called the National Security Entry-Exit Registration System (NSEERS), which was widely criticized for the discretion granted to border agents that led to accusations of discrimination.[40]

The various visitor tracking systems and visa issuance systems are slated to be integrated in a new program announced by DHS called the U.S. Visitor and Immigrant Status Indication Technology system (US-VISIT). The DHS plans to implement the first phase by the end of this year, with full implementation scheduled for October 2004 to meet the deadline set by the Enhanced Border Security and Visa Entry Reform Act. **However, agency officials are skeptical that the deadline can be met, and earlier implementation of SEVIS does not inspire confidence that it can be.** A recent GAO report details many problems with the ongoing implementation.[41]

Though Congress correctly identified the weaknesses in the immigration system and took action to correct them, efficient and effective implementation of the law is the responsibility of the executive branch. Even though Sept. 11 may have broken through some of the stonewalling that plagued the implementation of SEVIS, the White House still refuses to make it a priority. The administration needs to stop making excuses and devote itself to implementing the US-VISIT program by the October 2004 deadline.

Improving the Identification System — F

The most sophisticated biometric visa system is useless if a terrorist can simply toss the visa into an airport trashcan and head to the nearest Department of Motor Vehicles to get a driver's license or

identification card (DL/ID) under a false identity. Unfortunately, the current identification system in the United States makes that scenario all too likely. False identification is so easy to obtain that it is considered a rite of passage for teenagers. Moreover, the states do not have their systems integrated, making it possible for criminals and terrorists to move from state to state acquiring different identities.[42] Though the driver's license was not intended to serve as an identification card, it has become the de facto identity document—it can be used in any state to open a bank account, rent an apartment, enroll in college, or obtain a passport.

Under political pressure from privacy advocates and immigration groups, President Bush has refused to take steps to close the holes in the DL/ID system. The *National Strategy for Homeland Security* calls only for the federal government to "support" a state-led effort to develop minimum standards for issuance of DL/IDs.[43] The states, facing intense budget pressure, have worked through the American Association of Motor Vehicle Administrators (AAMVA) to improve both card technology and communication between state agencies, but have resisted wholesale changes that can both fully integrate and thoroughly modernize the DL/ID system.[44]

Upgrading standards for issuing DL/IDs is an important first step, but it is not enough. A better solution would be to convert all state-issued driver's licenses and identification cards into "smart cards" containing an encrypted biometric device that resides on the card only. This can ensure that only the holder of a card can use it in a biometric reader. At the same time, the states should implement an integrated database, linked to all other states and the US-VISIT system, containing a facial recognition capability that works from the digital photos taken for the cards.[45] This system would ensure that anyone who has already been issued a DL/ID or smart visa will be identified before a new card is issued, and eliminate identity switching and many other forms of identity theft.

Improving Visa Issuance and Consular Services — D

Often the first line of defense against terrorism is ensuring that known or suspected terrorists are not granted visas to enter the country in the first place. Prior to Sept. 11, overseas consular services focused on efficiency (granting visas as quickly and inexpensively as possible) over security, obviously a mistake since known terrorists were able to enter the country legally, despite being on watch lists.

In mid-2002, lawmakers pushed to strip the visa adjudication function from the State Department and transfer it to the new DHS. The White House and Secretary of State Collin Powell, however, managed to convince Congress that the visa function was best left in the hands of the State Department. In November 2002, Secretary Powell selected a new Assistant Secretary for Consular Affairs who pledged to "respond vigorously and creatively to the challenge of strengthening America's national security." During this period, Congress, via several pieces of legislation, did mandate changes in visa policies, including requiring the intelligence and law enforcement agencies to expand information sharing with State. This has doubled the number of suspected terrorists listed in the visa lookout database.

While acknowledging recent reforms, a December 2002 report by the State Department's inspector general found that the Bureau of Consular Affairs' focus on terrorism and visa control had been sidetracked by pressure to secure U.S. embassies and consulates overseas. It also found that it had not made any big changes in the visa-issuing process. "The NIV [nonimmigrant visa] issuance process as it existed before Sept.11 was inadequate to meet that threat. Since Sept. 11, steps have been taken to address this problem, though existing policies and resources still aren't secure enough."[46] The inspector general's report concluded that visa-issuing posts make up their own rules about waiving an interview with little regard for security, and that Consular Affairs' use of foreign travel agencies to help process visa applications is haphazard and reckless. The report also found that fraud prevention efforts, databases, and personnel are not integrated into the visa-issuing process. A recent GAO study also pointed to serious defects in the procedures for revoking the visas of suspected terrorists or criminals.[47]

In addition, the disconnect between mission and

resources is great. While the president's FY 2004 budget seeks a substantial boost in consular funding, even more resources will be needed in light of additional duties mandated by Congress, such as requiring personal interviews of a larger proportion of visa applicants and capturing biometric identifiers from all visa applicants. Moreover, the administration has done nothing to create links between consular offices and an integrated terrorist watch list.

Securing Ports of Entry C

Before Sept. 11, most security measures at ports of entry (both seaports and land border crossing points) were focused primarily on preventing trafficking in drugs and humans. The Department of Homeland Security now recognizes that border security is an important part of the anti-terrorism effort, and realizes the difficult balance that must be struck between preventing terrorists and weapons from entering the country and continuing to allow the free flow of goods—worth over $3 billion daily—from our trading partners.[48]

The administration moved relatively quickly to improve security at ports of entry along the Canadian border. In December 2001, the United States and Canada announced the Smart Border Initiative to facilitate the free flow of cargo across the border. The primary components of the plan were efforts to improve security at shipping facilities before cargo reaches the border, identify high-risk cargo, and upgrade the technology used to check and track cargo as it crosses the border.[49] Progress on the Mexican border has been somewhat slower, but the administration has secured agreement with the Mexican government to implement a similar smart border initiative.[50] These initiatives will be successful only to the extent that an ongoing process for auditing the results and ensuring the cooperation of the freight shippers is in place.

Unfortunately, the effort to secure seaports is more of a mixed bag. The DHS has implemented a number of measures to improve security at seaports, including the Container Security Initiative (CSI), which seeks the cooperation of foreign governments to begin security procedures in foreign ports on cargo bound for the United States. The CSI program has been agreed to by governments of 19 of the 20 largest foreign ports (though not yet underway at all of them), and DHS intends to expand the program further.[51] However, from a budgetary perspective, DHS has given port security short shrift. Vulnerability assessments of the 55 largest seaports required by the Maritime Transportation Security Act of 2002 have not received adequate funding, and at the current rate will not be completed for another five years.[52] The DHS also tried to divert $28 million from Operation Safe Commerce (a pilot program to identify and implement systemic port security initiatives) in order to cover a budget shortfall in airport security.[53] Also lacking is a comprehensive program to improve security and speed of border crossings by deploying detectors that can identify potentially dangerous cargo such as radioactive material.[54] **The Bush administration has made an admirable effort to brainstorm ideas and programs to secure the ports of entry, but needs to back up that effort with sufficient funds to acquire the staff and technology to implement the ideas.**

4. Protecting Critical Facilities
Final Grade: D+

Given limited resources, it is obviously impossible to maintain a high level of security at every single public facility in the United States. However, special attention should be given to certain critical facilities based on their value to terrorists. Experience teaches us that terrorists prefer certain targets over others for a number of reasons: soft security, high publicity value, and especially, the ability to "leverage" an attack with additional secondary deaths. Just as the Sept. 11 hijackers leveraged their breach of airport security into thousands of deaths on the ground, future terrorists are likely to go after targets that will cause massive destruction, panic, and chaos. Those facilities, therefore, represent the highest priority and need to be secured first. This section will examine the progress President Bush has made in protecting those critical facilities, including aviation, nuclear facilities, chemical facilities, and the information infrastructure.

Enhancing Aviation Security C-

Passenger Security B-

The top priority for aviation security was improvement of passenger screening and security, and the Bush administration has done reasonably well in a short period of time. The creation of the Transportation Security Administration (TSA), an agency tasked with securing all modes of transportation, was an excellent first step. The TSA removed all private contractors from airport screening and replaced them with 55,000 federal employees with better training and better pay. The equipment and procedures for screening passengers also improved, and though there was anecdotal evidence that security screeners were going overboard in the immediate wake of the Sept. 11 attacks, TSA has done an admirable job of balancing passenger safety and convenience. It has also made significant upgrades to physical security on the planes themselves, including deployment of air marshals, fortified cockpit doors, and a program to arm pilots.

However, the process has not been without problems. The TSA hired too many full-time screeners and failed to audit its contractors, leading to a $3.3 billion budget deficit and forcing cuts in research and development and other areas.[55] Efforts to develop a Registered Traveler program, which would encourage individuals to submit to comprehensive background checks in exchange for convenience at the airport, are on hold, even though they show great promise for boosting both security and convenience.[56] The TSA also hopes that their forthcoming Computer Assisted Passenger Prescreening System (CAPPS II) will address the background check side of the passenger security equation, though concerns about privacy and effectiveness have put the program in limbo.[57] **Also troubling is the lack of an administration plan to deploy next-generation passenger screening machines that will better check for explosives;** coupled with a Registered Traveler program that identifies low-risk passengers in advance, these machines would greatly reduce the risk of a terrorist carrying a bomb aboard an airplane.

The administration should also focus on efforts to arm aircraft with defenses against shoulder-fired surface-to-air missiles and to improve security for flights arriving in the United States from foreign terminals. These are not theoretical risks. Last November, two missiles were fired at an Israeli airliner and in December 2001 the "Shoe Bomber" Richard Reid tried to destroy a plane bound for the United States from Paris. These vulnerabilities—particularly the fact that individuals (as opposed to their carry-on luggage and shoes) are not screened for explosives—represent a major ongoing risk.

Baggage Security C+

The TSA purports to screen all baggage for

explosives and hazardous material, but this "screening" may take several forms, including canine inspections, hand searches, swabbing, or even passenger-bag matching, a technique that does not guard against suicide bombers. When TSA announced in December 2002 that it has achieved "100% baggage screening," it had installed just 239 of the 1,100 explosives detection machines and 1,951 of the 6,000 trace detection machines that it had estimated were needed.[58] The baggage screening goal was actually accomplished by combining machine screening with the less-effective methods of hand searches and bag matching. Moreover, because the lack of machines requires a high number of hand searches, a rash of luggage thefts has occurred, which could lead to a public backlash against the entire baggage security process.[59] There is also no system in place to identify high-risk luggage, which could greatly improve the efficiency of the screening process; of course, identifying high-risk luggage would not be necessary if all luggage was screened with explosives-detection machines, but until that happens, high-risk identification is a prudent step.[60]

Personnel Security **D**

The Aviation and Transportation Security Act of 2001 required that airport employees with access to secure areas submit to screening procedures similar to those for passengers, and TSA began that process by implementing background checks. Initial background checks, however, failed to disqualify dozens of workers with histories of certain crimes at Los Angeles and LaGuardia airports alone.[61] At the same time, TSA has taken no steps to physically screen employees, and security procedures at employees' access points to secure areas remain non-standard and often lax. The TSA argues that all of these problems will be solved when the Transportation Worker Identification Credential (TWIC) program is up and running, but that program is only now entering early test phases.[62]

Air Cargo Security **D-**

Although physical screening mechanisms have been mandated for passenger baggage carried aboard airplanes, the freight which composes the other half of passenger airplane cargo undergoes no such procedure. Freight security is governed by TSA's "known shipper" program, by which shippers of cargo carried on passenger planes must either have a lengthy shipping history with the carrier or be verified by the carrier as a legitimate business. There are no defined criteria to verify carriers, TSA does not carry out the task themselves, and the only change to the program since Sept. 11 has been to ask carriers to share their "known shipper" lists with one another.[63] The Department of Transportation's inspector general found in 2002 that the program was "easily circumvented" by terrorists seeking to place explosives on an airplane, while simple precautions, such as requiring airlines to verify the credentials of freight forwarders physically delivering the cargo to them, remain absent.[64] And while TSA maintains that comprehensive security procedures would be overly burdensome, only $10 million dollars has been allocated to address the problem.

An internal TSA "Cargo Security Discussion" document said that "cargo is likely to become—and may already be—the primary threat vector in the short term" and that the agency needs to "improve [cargo] security and reduce risk as soon as possible."[65] **Yet, as recently as June 2003, DHS Assistant Secretary for Information Analysis Paul J. Redmond testified that he has "not considered" the potential threat from unscreened passenger airline cargo.**[66]

Securing Nuclear Plants and Materials *C+*

Nuclear Power Plant Security **A**

Nuclear power plants represent about 20 percent of our nation's electrical generation capacity. As long as nuclear reactors are operating, a substantial amount of radioactive waste will have to be stored near them. The United States has 104 commercial nuclear reactors in 31 states. The Nuclear Regulatory Commission (NRC), in reaction to the Sept. 11 attacks, quickly issued heightened security regulations for all nuclear power plants. Overall, the nuclear power industry has spent nearly $400 million on additional security since the attacks. If anything, the NRC could be faulted for overkill, as nuclear power plants have always been extremely secure and additional security measures may not be the best use of resources; worst-case scenarios of terrorist

attacks on plants or nuclear waste under transport indicate a very low likelihood of collateral injury.

Nuclear Material Security **D**

Power plants are not the only sources of radioactive material. Hospitals, research universities, and other facilities use radioactive material in a variety of medical and scientific equipment. All told, there are over two million licensed sources of radioactive material in the United States. Though under the jurisdiction of the NRC, security at these facilities can be lax; each year, there are approximately 250 reports of lost or stolen radioactive material, the majority of which is not recovered.[67] Because this material can be used to make a so-called "dirty bomb" that uses conventional explosives to spread radioactive material, great attention is needed to secure these sources of material.

Securing Chemical Production and Storage Facilities *D-*

Approximately 15,000 facilities in the United States house chemicals that could threaten the population and the environment if they were released as the result of a terrorist attack.[68] But, unlike the nuclear industry, which is strictly governed by federal mandate, security at chemical facilities is unregulated and currently organized largely through what appears to be a relatively effective voluntary code that applies to most of the largest facilities.[69] Though there is a certain amount of disagreement among the chemical industry, environmental activists, and security specialists as to the degree of federal regulation necessary to keep these facilities secure, there is general agreement that the federal government needs to take action.

Unfortunately, the Bush administration has done almost nothing to address this problem. Though a number of facilities will be partially covered by new maritime security regulations—many chemical plants are built on navigable waters and have docks that fall under the jurisdiction of the U.S. Coast Guard—the administration has not submitted a legislative proposal for chemical plant security. **This lack of action is particularly troubling because Secretary Ridge has stated that voluntary efforts alone are not sufficient to assure the public of the industry's preparedness.**[70] Two competing chemical facility security bills, introduced by Sen. James Inhofe (R-Okla.) and Sen. Jon Corzine (D-N.J.), are currently under consideration, but the White House has refused either to take a position on the bills or to negotiate agreement between the parties.[71]

Boosting Cybersecurity *D+*

Securing the nation's "cyberspace" is important not only because the nation's economy is fully dependent on computer communications, but also because the nation's physical infrastructure is managed largely over electronic networks. While research and development in this area is essential, front-line defense comes from gathering and sharing information between government and the private entities which compose 80 percent of the nation's cyber-reliant infrastructure.

Though the National Infrastructure Protection Center exists to promote cybersecurity (among other things), the administration's efforts to secure cyberspace and the physical infrastructure on which it depends have been badly coordinated and underfunded.[72] Nearly a year and a half after Sept. 11, the administration released its *National Strategy to Secure Cyberspace* and *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. These reports addressed essentially two halves of the same problem—securing critical infrastructure physically and electronically—but as the General Accounting Office discovered, "neither strategy (1) clearly indicates how the physical and cyber efforts will be coordinated; (2) defines the roles, responsibilities, and relationships among the key CIP [critical infrastructure protection] organizations, including state and local governments and the private sector; (3) indicates time frames or milestones for their overall implementation or for accomplishing specific actions or initiatives; nor (4) establishes performance measures for which entities can be held responsible."[73]

Additionally, the cybersecurity strategy did little more than encourage private companies and individuals to secure their own hardware and software, stopping short of regulating even the most vital pieces of infrastructure.[74] At the same time,

the administration has balked at appointing an official to oversee cybersecurity efforts. After federal cybersecurity chief Richard Clarke resigned in January 2003, the Bush administration in June moved the position to DHS, where the authority was vested three levels of leadership beneath the secretary. This will only contribute to the lack of coordination in cybersecurity efforts.

Beyond helping to secure the network infrastructure of the nation, the Bush administration has also failed to make significant improvements in the security of federal government computer networks. Rep. Adam Putnam (R-Fla.), chairman of the House Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, held a hearing on June 24, 2003, in which he excoriated administration's efforts at cybersecurity, calling the lack of progress "no longer acceptable."[75] Citing a report from the Office of Management and Budget, Rep. Putnam listed a number of weaknesses in federal cybersecurity, including the lack of system-level security plans, required cybersecurity reviews, and coordination in IT spending.[76] As Rep. Putnam pointed out at the hearing, government networks are tempting targets for cyberterrorists because an attack could do serious damage both to the economy and to the government's ability to operate. The Bush administration needs to make a much more serious effort to improve network security within federal departments and agencies.

5. Protecting Against Bioterror Attacks
Final Grade: C

As the nation was reeling from the shock of the Sept. 11 attacks, another vulnerability was exposed. The threat of bioterrorism became all too real when the anthrax attacks sickened or killed both the intended recipients and the postal workers who unwittingly transmitted the deadly microbes. Though those attacks were relatively limited in scope, their impact was dramatic in terms of fear and panic, and the perpetrator has yet to be caught. This makes future attacks with biological and chemical weapons a very real concern.[77] This section examines the Bush administration's efforts to defend against such attacks. (It should also be noted that many of the same efforts to protect against bioterrorist attacks will also be effective responses to chemical and radiological attacks.)

Developing Bioterrorism Countermeasures C-

The Centers for Disease Control and Prevention (CDC) estimates that there are 57 diseases which are likely vectors for bioterrorism, but for which no countermeasures exist. A significant national effort is urgently needed to give biomedical researchers incentive to aggressively pursue treatments for these pathogens.

The president's proposed BioShield program intends to entice pharmaceutical companies to develop such countermeasures, at a purported cost of $5.6 billion over the next five years. The program would position the federal government as a guaranteed customer for treatments to bioterrorism, thereby encouraging private pharmaceutical companies to invest resources in development of those treatments.

BioShield's effects are likely to be limited though, as certain constraints make it unlikely that pharmaceutical companies will fully participate. For example, BioShield requires that countermeasures be developed, tested, and mass-produced within five years, an unreasonable timetable for combating rare and therefore largely unresearched diseases. At the same time, countermeasures in development that happen to have commercially viable applications, such as treating plant diseases or more common infectious agents, are disqualified from the program even if the commercial application translates into a usable countermeasure. Further, companies using expedited testing procedures are granted no indemnity for unanticipated side-effects, and there is no guarantee that millions of dollars of research will actually yield a government contract. Finally, the president's plan does not provide incentive for researching the tools and diagnostics necessary to deal with new and unanticipated diseases.[78]

To counter these shortcomings in the Bush administration's approach, Sen. Joseph Lieberman (D-Conn.) introduced the Biological, Chemical, and Radiological Weapons Countermeasures Research Act of 2003.[79] The bill provides companies with more secure market guarantees, liability protections, and incentives for raising venture capital, which make it far more likely that private companies will actually participate. It also does not restrict companies to an unreasonable and arbitrary five-year timeframe for research, development, manufacture, and delivery, and includes not only drugs and vaccines, but research tools and facilities necessary to deal with an outbreak of an unanticipated or substantially modified agent. The Lieberman approach is much more likely to produce needed countermeasures than the Bush administration's BioShield program, and should be adopted instead.[80]

The Bush administration also needs to pay more attention to the risks of bioterrorism targeted against agriculture and the food supply in the United States. As the outbreak of so-called Mad Cow Disease in the United Kingdom shows, aggressive steps are sometimes necessary to control potentially devastating epidemics of diseases in livestock and crops. Terrorists could wreak economic havoc by

infecting the food supply, and the diseases could even spread to humans. Though the issue is addressed briefly in the president's *National Strategy for Homeland Security*, little is being done to address this specific threat.[81] (In fact, the Department of Agriculture recently announced that it is reducing the amount of imported meat it inspects from 17 percent to 6 percent, despite bioterrorism fears.[82])

Expanding Health Care Surge Capacity C

Mass casualties resulting from any terrorist attack still threaten to overwhelm hospitals. Casualties from a biological, chemical, and radiological attack are all the more difficult to treat as they require specific equipment and expertise. Programs such as regional medical mutual aid plans can help hospitals expand their capacity when needed and, coupled with special supply stockpiles, can provide essential countermeasures to specific threats.

The administration has successfully expanded the national pharmaceutical stockpile, and has deployed additional "push packs" of supplies throughout the country. But although the president's FY 2003 budget called for $225 million for the development of regional medical mutual aid plans, implementation has been spotty, and the item was dropped in the 2004 budget. More of an effort must be made to help states and municipalities plan for the mass medical casualties that can accompany a terror attack.

According to the GAO, the efforts of state and local health agencies to prepare for a bioterror attack have improved the nation's capacity to respond to infectious disease outbreaks, but gaps in preparedness remain. The GAO found that many hospitals lack the capacity to respond to such outbreaks on a large scale. They lack adequate equipment, isolation facilities, and staff to treat a large increase in the number of patients that may result.[83] Moreover, upgrades in communications between public health agencies can facilitate faster response to an attack.[84]

Updating Public Health Laws C

The virulence of many bioterror agents does not cease after the initial attack, as infected people continue to spread contagious diseases if they are not quarantined during and after treatment. In some extreme cases, it may be necessary to restrict freedom of movement for attack victims, or for their families who are not victims, to prevent further contamination (as we have seen in Canada and China with SARS). Public safety officials generally have limited authority to constrain movement (such as evacuations during natural disasters), and U.S. laws are neither uniform nor sufficient to give authorities adequate power to contain an outbreak.

To address this, the Bush administration drafted model legislation that would allow health officials to impose legally enforced quarantines, and would also permit individuals to appeal a quarantine order. To date, however, 22 states and the District of Columbia have passed different parts of the bill, and others have passed none. This patchwork of laws would make it difficult to react to an outbreak that could easily cross state borders.[85] **The administration needs to do more to create a unified federal program to quickly contain the damage caused by biological or chemical terrorism.**

6. Defending Civil Liberties and Privacy
Final Grade: C-

In the days and weeks after the Sept. 11 attack, the Bush administration and Congress rushed to find ways to make it easier for law enforcement and intelligence agencies to combine efforts against terrorists operating in the United States. This section examines the extent to which those new efforts impacted civil liberties and privacy.

Detaining Suspected Terrorists C-

In the immediate aftermath of the World Trade Center and Pentagon attacks, the Bush administration engaged in an unprecedented round-up of potential terrorist suspects, both in the United States and abroad in Afghanistan, without the benefit of well-defined rules on how the detentions would work. An internal investigation into the Justice Department's detention of hundreds of people after Sept. 11 (most for suspected immigration violations) found significant problems in how the cases were handled. More than 700 foreign nationals were held for routine visa violations, many under a regulation allowing the Immigration and Naturalization Service to hold individuals for an extended period without charge. Many were denied prompt access to attorneys and some remained in custody for months pending "clearance" by the government, even after immigration judges had granted them bail or issued deportation or "voluntary departure orders." There were also reports of ill treatment of detainees, including verbal and physical abuse and prolonged solitary confinement. Appearing before Congress in June, Attorney General John Ashcroft said that the Justice Department's civil rights division was investigating four instances of alleged abuse of detainees identified by the inspector general. For another 14 incidents noted by the inspector general, evidence was deemed insufficient to bring criminal charges.[86]

In the war on terror, the Bush administration has engaged in a disturbing pattern of making up the law as they go along. Zacarias Moussaoui, for instance, faced charges in federal court for the Sept. 11 attacks, but was denied access to a key defense witness because the witness was being detained at the U.S. military base at Guantanamo Bay, Cuba. After a judge ruled that Moussaoui could not be denied access to an exculpatory witness on national security grounds, the government instead is considering simply dismissing the charges and trying Moussaoui in a military tribunal, where defendants are not given the same civil liberties.[87] Though the Bush administration may feel they erred by not trying Moussaoui in a military tribunal in the first place, they should not be able to simply move defendants between the civil justice system and military tribunals, as predictability of legal process is key to our commitment to rule of law.

The issue of terrorist detainees raises other troubling civil rights questions. Foremost among them is the fact that two of detainees, Jose Padilla and Yaser Esam Hamdi, are U.S. citizens who have had their due process rights revoked simply by being declared enemy combatants.[88] Even for non-citizen enemy combatants, however, the failure to adjudicate as quickly and transparently as possible is troubling.

All evidence indicates that they have been treated well, and there is widespread agreement that they should not be treated as prisoners of war as defined by the Geneva Convention because they were not acting as uniformed military under the direction of a state. At the same time, it is not right for the United States to be able to seize and indefinitely detain individuals, even suspected terrorists, with no clear path to their eventual disposition, be it criminal charges in the United States or release back to their home country. The Bush administration should work with other nations to create a protocol for dealing with terrorists and other non-state actors.

In the meantime, a firm set of rules is needed to give the detainee a defined and transparent adjudication process that will rule on their status in a timely manner, consistent with American standards of justice.

Protecting Privacy C

With regard to privacy issues, the Bush administration has not so much violated privacy as ignored the issue entirely. The DHS waited until April 2003 to appoint a chief privacy officer and a director to the Office of Civil Rights and Civil Liberties (a position mandated by Congress). The administration's initial effort to implement CAPPS II, the airline passenger screening system, did not take citizen privacy into account despite the fact that the system would check the credit reports of airline passengers; it was up to Democrats in Congress, including Sen. Ron Wyden (R-Ore.) to demand that DHS account for the privacy implications of the system before testing it.[89] Similarly, the administration was tone-deaf to the privacy implications of the experimental data-mining Terrorist Information Awareness project, despite the fact that the plan included accessing an unprecedented number of public, private, and commercial databases. While these systems have not yet been implemented, and therefore no privacy violations have occurred, **the Bush administration has here again shown a troubling disregard for the need to have clear privacy rules in place before developing these new systems.** As the Markle Foundation Task Force put it, "To succeed, the system must have the confidence of the American people it serves, while the analysts and operatives involved must feel confident that they know what they are expected and allowed to do, and that their work is lawful and appropriate."[90]

Privacy concerns have also been raised by the 342-page USA Patriot Act, approved by overwhelming majorities in both the U.S. Senate and House of Representatives.[91] The Act gives law enforcement officials broader authority to conduct electronic surveillance and wiretaps, and gives the president the authority—when the nation is under attack—to confiscate any property of anyone within U.S. jurisdiction believed to be engaging in such attacks. The measure also tightens oversight of financial activities to prevent money laundering and diminishes bank secrecy in an effort to disrupt terrorist finances. The act also changed provisions of the Foreign Intelligence Surveillance Act (FISA), which was passed in 1978 during the Cold War. The FISA established a different standard of government oversight and judicial review for "foreign intelligence" surveillance than that applied to traditional domestic law enforcement surveillance. The Patriot Act now permits surveillance under the less rigid standard whenever foreign intelligence is a "significant purpose" rather than the "primary purpose" of an investigation.[92]

These are reasonable steps to take, particularly since the powers granted in the act could prove to be instrumental in thwarting future terrorist attacks. The legislation has improved communications between law enforcement and intelligence agencies, helped seize millions of dollars that would have been funneled to terrorist groups, and assisted the FBI in monitoring cellular phone and email communication by terrorist groups. However, given the general lack of concern for privacy expressed by the Bush team, vigorous oversight of the administration of the USA Patriot Act by Congress and the courts will be necessary to ensure that serious privacy violations do not occur. (The administration leaked a draft of a more expansive, and worrisome, proposal dubbed PATRIOT II, but because that draft does not appear to be moving forward, we are not grading it in this report card.)

In general, the Bush administration has not committed the kinds of wholesale civil liberties and privacy violations that some advocacy groups warned against in the wake of the attacks. Nevertheless, the administration's obvious disregard for the importance of these issues is cause for concern and continued attention.

7. Managing the Improvement of Homeland Security
Final Grade: D+

In addition to assessing the individual elements of the homeland security strategy, it is also important to evaluate the overall management of the homeland security project. This evaluation particularly applies to President Bush himself, because improving homeland security is at base an exercise in management and leadership, and because the president frequently touts his management skills above his mastery of public policy. This section examines how the administration has managed the improvement of homeland security since the Sept. 11 attacks.

Reorganizing the Federal Government C-

It did not take long after the attacks to realize that the federal government as structured on Sept. 11 was not fully up to the task of protecting American citizens from terrorists. In response to this challenge, Sen. Lieberman, then chairman of the Senate Governmental Affairs Committee, introduced the Department of National Homeland Security Act of 2001 on October 11, 2001.[93] Unfortunately, President Bush opposed this legislation for eight months, before finally reversing course in June 2002 and putting forth a plan to create DHS that was substantially similar to Sen. Lieberman's long-standing proposal.[94]

It is important that President Bush changed his mind and, at long last, did the right thing by reorganizing the agencies responsible for homeland security. More than mere bureaucratic reshuffling, the new department is poised to take advantage of new efficiencies in budgeting and resource allocation and, just as important, able to break through some of the organizational problems that had plagued some agencies. (One example is the Immigration and Naturalization Service, which has now been split into functional bureaus under DHS.[95]) However, to the extent that DHS is having trouble getting up to speed with operations at this late date, the blame must lie with President Bush for delaying the reorganization for eight months through his opposition to the Lieberman proposal. Moreover, the administration has not pushed to give the House Select Committee on Homeland Security a permanent role with defined jurisdiction to perform appropriate oversight of DHS.[96]

Launching the Department of Homeland Security C

Once President Bush embraced the creation of DHS and Congress passed the law doing so, it fell to the administration to facilitate one of the largest government reorganizations in U.S. history. This is, without question, a difficult task that requires strong leadership to set priorities, overcome bureaucratic resistance, and ensure that tasks are completed. President Bush, who frequently boasted of his management expertise during his election campaign, ought to be well suited to this task.

Unfortunately, the launch of DHS has been a mixed bag. Many of the existing agencies transferred to the new department have continued to work as they always have, and some have begun to improve under reorganization. Many of the most important functions of DHS, however, have languished. The TSA, which was created shortly after the Sept. 11 attacks under the Department of Transportation, has yet to complete 60 percent of the background checks on its workers, a failure that recently led to the departure of two of the agency's personnel officials.[97] The department's intelligence analysis capabilities are also severely limited due to a lack of analysts, office space, and secure equipment; this failure also led to the resignation of a high-ranking

DHS official.[98] There is a widespread sense that the agency is not moving as quickly as it could to meet the reorganization challenge, despite generally adequate funding.[99]

Of course, it is not the president's place to micromanage a bureaucratic reorganization. Considering that President Bush declared homeland security to be his top priority, however, it is troubling that he has not given this major undertaking more of his attention and leadership.

Learning Lessons from Previous Attacks F

One of the most important responsibilities of any government after any disaster is to evaluate how the disaster happened to determine how to prevent or better respond to the next one. These independent examinations—such as the investigations into plane crashes—are less about assigning blame for a disaster than they are about learning lessons from it. When it is as horrific as the Sept. 11 attacks, it is even more important to learn the lessons that can prevent the next attack, or save lives if it cannot be stopped.

This is why it is disturbing that the Bush administration fought so hard against an independent inquiry into the Sept. 11 attacks. (President Bush did support a limited congressional inquiry into the attacks.[100]) After months of opposition to the independent inquiry, which gained support in Congress in the wake of revelations regarding intelligence failures leading to the attacks, President Bush finally changed his mind and publicly supported the inquiry in September 2002.[101] He then slowed the progress of the inquiry by appointing Henry Kissinger to chair the panel, a move that resulted in weeks of controversy over Kissinger's alleged conflicts of interest, ultimately resulting in his resignation in December 2002.[102] Next, Bush tried to strangle the commission by withholding the funds necessary for a thorough investigation, another move on which he was forced to retreat.[103] In recent days, the co-chairs of the commission have complained that agencies within the administration have been withholding documents vital to the inquiry.[104]

There is no doubt that this investigation could carry significant political risk for the president. The commission is scheduled to finish its inquiry in March 2004, though it will likely be delayed by the lack of White House cooperation. Many of the president's political allies feel that the commission will place some blame on the White House for failing to do more to stop the Sept. 11 attacks.[105] Despite this risk, however, the president has a greater responsibility to the safety of the American people, and should fulfill that responsibility by fully examining the failures that led to the attacks.

Conclusion

Careful examination of the Bush administration's record on homeland security invites the inescapable conclusion that President Bush has given homeland security more lip service than action. While some progress has been made, not nearly as much has been done as might be expected given that Bush has declared homeland security to be his highest priority.

There are several reasons why the president has not followed through on his promises to make the nation more secure. First, the administration has put far more energy into overseas operations, believing that assertive overseas military action trumps efforts to strengthen the defense of the homeland. Second, in line with this administration's overarching effort to cut the size of the federal government and devolve governmental functions to the state and local level, the Bush administration has simply not devoted the resources—financial, political, and administrative—to ensuring a strong and effective federal role. Along these lines, the president's overriding commitment to slashing taxes has led him to underfund efforts to improve intelligence coordination, communication, and border control.[106] Most significant, however, is that the president and his key advisors are ideologically constrained when it comes to dedicating themselves to homeland security. His administration's anti-government stance led them to reject comprehensive overhauls of the identification system and to oppose instituting a student visa tracking system. The president's belief that homeland security, like crime fighting in general, is a state and local responsibility has led him to limit federal support to state and local governments, putting much of the burden of homeland security on cash-strapped states.

Most disturbingly, President Bush's inattention to domestic security has led us into a war on terror without the benefit of America's secret weapon: entrepreneurial spirit and overwhelming technological superiority. Though the terrorists have the advantage of stealth, secrecy, and suicidal fervor, we should be fighting back with our own strengths, including our adaptability to changing circumstances, our creative drive, and our ability to quickly develop and implement new technologies through both private and public funding. **President Bush has devoted much rhetoric to bringing our entrepreneurial spirit to other elements of government, but on homeland security he has consistently sided with the ponderous, underfunded status quo over fostering the kinds of innovations that will help keep our citizens safe.**

President Bush's strong words and dramatic settings for speeches have helped make Americans feel safer. It is time for Bush to move beyond mere words, however, and implement the policies that will thwart terrorists and make Americans safer not in theory, but in reality.

Appendix
Complete Grades and Methodology

		Grade	Weight (out of 35)	Score	Percent contribution toward total grade (rounded to nearest %)
1. Improving Intelligence Gathering and Analysis		**D**	**8**	**1.13**	**23%**
	Coordinating Inter-Agency Intelligence	C-	3	1.67	9%
	Integrating Terrorist Watch Lists	F	2	0	6%
	Developing Counterterrorism Database Systems	D+	3	1.33	9%
2. Improving Security at the State & Local Level		**D-**	**5.5**	**0.68**	**16%**
	Completing a National Threat Assessment	F	1.25	0	4%
	Sharing Information with State & Local Governments	D	1.25	1	4%
	Defining Role of State & Local Officials	D	0.5	1	1%
	Providing Financial Support for State & Local Governments	D-	2	0.67	6%
	Boosting Citizen Preparedness	D+	0.5	1.33	1%
3. Controlling the National Borders		**D**	**6**	**1.13**	**17%**
	Tracking Entry & Exit of Foreign Visitors & Students	D	1.5	1	4%
	Improving the Identification System	F	1	0	3%
	Improving Visa Issuance & Consular Services	D	1.75	1	5%
	Securing Ports of Entry	C	1.75	2	5%
4. Protecting Critical Facilities		**D+**	**5**	**1.61**	**14%**
	Enhancing Aviation Security	C-	3	1.67	9%
	Passenger Security	B-	0.75	2.67	2%
	Baggage Security	C+	0.75	2.33	2%
	Personnel Security	D	0.75	1	2%

	Air Cargo Security	D-	0.75	0.67	2%
	Securing Nuclear Plants & Materials	C+	0.75	2.5	2%
	Nuclear Power Plant Security	A	0.375	4	1%
	Nuclear Material Security	D	0.375	1	1%
	Securing Chemical Production & Storage Facilities	D-	0.75	0.67	2%
	Boosting Cybersecurity	D+	0.5	1.33	1%
5. Protecting Against Bioterror Attacks		**C**	**3**	**2.11**	**9%**
	Developing Bioterrorism Countermeasures	C-	2	1.67	6%
	Expanding Health Care Surge Capacity	C	1	2	3%
	Updating Public Health Laws	C	0.5	2	1%
6. Defending Civil Liberties & Privacy		**C-**	**2.5**	**1.87**	**7%**
	Detaining Suspected Terrorists	C-	1	1.67	3%
	Protecting Privacy	C	1.5	2	4%
7. Managing the Improvement of Homeland Security		**D+**	**5**	**1.5**	**14%**
	Reorganizing the Federal Government	C-	1.5	1.67	4%
	Launching the Department of Homeland Security	C	2.5	2	7%
	Learning Lessons from Previous Attacks	F	1	0	3%
OVERALL		**D**	**35**	**1.32**	**100%**

Methodology

Letter grades were assigned to the most specific sub-areas within general sections and topic areas, corresponding to the numbers of a standard four-point academic grading scale. (A=4, B=3, C=2, D=1, F=0). Plusses and minuses added or subtracted one-third of a grade—e.g., a B- is awarded for a range between 2.67 and 2.99, a B is awarded for a range between 3.0 and 3.32, and a B+ is awarded for a range between 3.33 and 3.66.

Sections, topic areas, and sub-areas were weighted to reflect their relative importance in PPI's view, with 35 points overall being allocated between seven main topic areas and 28 sub-areas.

Grades were then assigned to sections and general topic areas by multiplying grades of sub-areas by their weights, adding these together, and then dividing by the total number of points for the section or general topic area to determine that area's weighted average grade. These numerical average grades were then used to assign letter grades according to the number-letter grade rubric above. The overall grade was determined similarly. Percent contribution of topics and subtopics is listed for reference purposes.

Endnotes

[1] http://www.whitehouse.gov/homeland/book/letterfromthepresident.pdf.
[2] One serious mistake was letting Osama bin Laden escape, due in part to an insufficient commitment to troops on the ground. The administration also seems to be failing in the important task of rebuilding Afghanistan. Unfortunately, these mistakes may also be repeated in Iraq.
[3] The United States Commission for National Security/21st Century (the Hart-Rudman Commission) had warned of our vulnerabilities years before the attacks. http://www.nssg.gov/Reports/NWC.pdf.
[4] Ridge was recommending a veto as late as one week before President Bush changed his mind and threw his support behind the creation of the new department. http://www.govexec.com/dailyfed/0502/053002cd1.htm.
[5] Joshua Micah Marshall details the FBI's limitations in "A Failure to Communicate," *Blueprint*, July 2002, http://www.ndol.org/ndol_ci.cfm?contentid=250675&kaid=124&subid=900019.
[6] http://www.fcw.com/fcw/articles/2003/0428/news-threat-04-28-03.asp.
[7] Katz, Rita and Josh Devon, "Perilous Power Play: FBI vs. Homeland Security," *National Review Online*, May 27, 2003.
[8] House Select Committee on Homeland Security Hearing on Homeland Security Progress, May 20, 2003.
[9] Rep. Jim Turner letter to Pres. Bush, June 9, 2003. Relying on testimony of Paul J. Redmond, Assistant Secretary of Homeland Security, June 5, 2003.
[10] *Ibid.*, New, William, "Cox Plans Substantive Revision of Homeland Security Act," *National Journal's Technology Daily*, May 2, 2003.
[11] For GAO's assessment, see GAO-03-759T "FBI Reorganization: Progress Made in Efforts to Transform, but Major Challenges Continue," June 18, 2003, http://www.gao.gov/new.items/d03759t.pdf.
[12] Becker, Jo and Phuong Ly,"Probe Less Cohesive Than Advertised; Parts of Cross-Boundary Effort Fraught With Politics, Leaks, Confusion," *The Washington Post*, October 10, 2002.
[13] Marshall, *op cit.*
[14] http://intelligence.house.gov/jis_recommendations.htm.
[15] GAO-03-322 "Terrorist Watch Lists Should be Consolidated to Promote Better Integration and Sharing," April 15, 2003. http://www.gao.gov/new.items/d03322.pdf.
[16] Testimony of Secretary Tom Ridge before the House Select Committee on Homeland Security, May 20 and 22, 2003.
[17] It is unclear to what extent the intelligence agencies currently use a silent hit system linked to the national crime databases.
[18] This is discussed in more detail in the PPI policy brief "Using Technology to Detect and Prevent Terrorism," by Shane Ham and Robert D. Atkinson, January 2002, http://www.ppionline.org/documents/IT_terrorism.pdf.
[19] This was the main complaint of FBI whistleblower Colleen Rowley. An edited copy of her memo on the subject can be found at http://www.time.com/time/nation/printout/0,8816,249997,00.html.
[20] Markle Foundation Task Force on National Security in the Information Age, "Protecting America's Freedom in the Information Age," October 7, 2003, p. 10, http://www.markletaskforce.org.
[21] Department of Justice Office of the Inspector General, "FBI's Management Of Information Technology Investments," Report No. 03-09, December 2002, http://www.justice.gov/oig/audit/0309/index.htm.
[22] Statement of Steven I. Cooper before the Committee on Government Reform, May 8, 2003.
[23] http://www.cia.gov/csi/studies/vol47no1/article07.html.
[24] http://www.wired.com/news/politics/0,1283,59606,00.html.
[25] http://www.gcn.com/vol1_no1/homeland-security/22601-1.html.
[26] P.L. 107-296.
[27] http://www.hillnews.com/news/040903/homeland.aspx.
[28] A *Washington Post* story on July 8, 2003, detailed the work of doctoral candidate Sean Gorman, who has completed a nationwide map of critical infrastructure vulnerabilities using data gathered from the Internet. http://www.washingtonpost.com/wp-dyn/articles/A23689-2003Jul7.html.
[29] Cohen, John D., "Coded Alert System Should Go," *The Hill*, June 4, 2003, http://www.thehill.com/news/060403/ss_cohen.aspx.
[30] One such project is the Multistate Anti-Terrorism Information Exchange (MATRIX), a pilot program of the Institute for Intergovernmental Research. http://www.iir.com/matrix/.
[31] http://www.nemaweb.org/docs/National_Response_Plan.pdf.
[32] For more information on reductions in law enforcement, see "Cop Crunch" by Jose Cerda III in *Blueprint* Magazine, April 2003, http://www.ndol.org/ndol_ci.cfm?kaid=119&subid=156&contentid=251453.
[33] http://www.cfr.org/publication.php?id=6085.

[34] For more examples of the questionable advice contained at Ready.gov, see http://www.ndol.org/ndol_ci.cfm?contentid=251312&kaid=131&subid=207.
[35] http://www.whitehouse.gov/news/releases/2002/01/20020130.html.
[36] President Bush allowed his budget request to be cut from $200 million to $25 million. "Bush's volunteer plan takes a hit," by Mimi Hall, *USA Today*, January 27, 2003, p. A8.
[37] P.L 107-173.
[38] For details on how the Bush administration interfered with the development of the student tracking system, see "Borderline Insanity," Nicholas Confessore, *Washington Monthly*, May 2002, http://www.washingtonmonthly.com/features/2001/0205.confessore.html.
[39] *Ibid.*
[40] The NSEERS system applies mainly to young men from Muslim countries. For details, see http://www.immigration.gov/graphics/shared/lawenfor/specialreg/index.htm.
[41] GAO Report 03-563, "Homeland Security Needs to Improve Entry Exit System Expenditure Planning," http://www.gao.gov/new.items/d03563.pdf.
[42] For a comprehensive look at problems with the identification system, see "Modernizing the State Identification System: An Action Agenda," by Shane Ham and Robert D. Atkinson, http://www.ppionline.org/ppi_ci.cfm?contentid=250175&knlgAreaID=140&subsecid=900017.
[43] http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf.
[44] For more on AAMVA's efforts, see http://www.aamva.org/IDSecurity/.
[45] This would match with State Department efforts to create a passport with facial recognition technology. http://www.gcn.com/vol1_no1/daily-updates/22765-1.html.
[46] http://oig.state.gov/documents/organization/16215.pdf.
[47] GAO Report 03-798, "Border Security: New Policies and Procedures Are Needed to Fill Gaps in the Visa Revocation Process," June 18, 2003, http://www.gao.gov/new.items/d03798.pdf.
[48] http://www.census.gov/foreign-trade/Press-Release/2002pr/Final_Revisions_2002/exh4.pdf.
[49] http://www.canadianembassy.org/border/declaration-en.asp.
[50] http://www.whitehouse.gov/infocus/usmxborder/22points.html.
[51] http://www.dhs.gov/interweb/assetlibrary/Port_Security_Press_Kit_DHS.pdf.
[52] http://www.miami.com/mld/miamiherald/news/opinion/5972538.htm.
[53] http://www.govexec.com/dailyfed/0603/060403p1.htm.
[54] For an overview of the current status, see "Pushing out the Borders," by Alan M. Field, *Journal of Commerce*, April 28, 2003.
[55] Testimony of Kenneth M. Mead, Inspector General, U.S. Department of Transportation before the Committee on Senate Commerce, Science, and Transportation.
[56] For a comprehensive look at potential technology improvements to airport security, see "How Technology Can Help Make Air Travel Safe Again," by Robert D. Atkinson, Progressive Policy Institute, September 2001, http://www.ppionline.org/ppi_ci.cfm?knlgAreaID=124&subsecID=900018&contentID=3807.
[57] http://washingtontimes.com/national/20030619-010106-3427r.htm.
[58] Dillingham, Gerald L., "Post-Sept. 11 Initiatives and Long-Term Challenges," testimony before the National Commission on Terrorist Attacks upon the United States, April 1, 2003, http://www.gao.gov/new.items/d03616t.pdf.
[59] http://www.washingtonpost.com/wp-dyn/articles/A45823-2003Jun28.html.
[60] The Reason Foundation "Rethinking Checked-Baggage Screening" gives an excellent overview of this topic. http://www.rppi.org/ps297.pdf.
[61] Goo, Sara Kehaulani, "Airport Finds That More Screeners Are Questionable," *The Washington Post*, June 12, 2003, A03. Initial checks were carried out by private contractors, and at least one has been penalized for poor performance. Employees are also subject to a more comprehensive round of OMB-administered background checks, though TSA could not report on the progress of that program.
[62] http://www.fcw.com/fcw/articles/2003/0714/web-twic-07-16-03.asp.
[63] Carrier is shorthand for the group of freight forwarders who consolidate shipments at facilities near the airport and then place such cargo on passenger planes, and the minority of airline companies who perform this task themselves.
[64] Schneider, Greg, "Terror Risk Cited for Cargo Carried on Passenger Jets," *The Washington Post*, June 10, 2002, A01.
[65] *Ibid.*
[66] Letter from Rep. Jim Turner to President Bush, June 9, 2003. Relying on testimony of Paul J. Redmond, Assistant Secretary of Homeland Security, June 5, 2003.
[67] http://www.gao.gov/new.items/d03638.pdf.
[68] This estimate is based on the number of facilities currently required by the Environmental Protection Agency to maintain a Risk Management Plan (RMP). Some of these facilities store relatively benign chemical compounds that would not pose an immediate health hazard if released. However, in the absence of a more comprehensive threat analysis, the RMP facilities are

a good starting point for evaluation.

[69] For more information on the American Chemistry Council's Responsible Care program and chemical plant security, see http://www.accnewsmedia.com/site/page_date_pr.asp?TRACKID=&VID=13&CID=36&DID=76.

[70] GAO 03-439, "Homeland Security: Voluntary Initiatives Are Under Way at Chemical Facilities, but the Extent of Security Preparedness Is Unknown," http://www.gao.gov/new.items/d03439.pdf.

[71] The Corzine bill is S. 157, and the Inhofe bill is S. 994 in the 108th Congress.

[72] The functions of the NIPC as it was originally created have been split, with the analysis and warning functions now a part of DHS.

[73] Dacey, Robert F. and Randolph C. Hite, "Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues," testimony before the U.S. House of Representatives Committee on Government Reform, May 8, 2003, http://www.gao.gov/new.items/d03715t.pdf.

[74] See Sarah D. Scalet, "CSO's Cyberdraft Suggestions," *CSO Magazine*, for an informed (if sarcastic) appraisal, http://www.csoonline.com/read/110802/briefing_draft.html.

[75] Rep. Putnam also expressed dismay that the data on security improvements, delivered in a mandatory report under the Government Information Security Reform Act, was seriously out of date.

[76] The OMB report is analyzed by GAO in 03-852T, "Information Security: Continued Efforts Needed to Fully Implement Statutory Requirements," http://www.gao.gov/new.items/d03852t.pdf.

[77] The full scope of the threat remains unknown. According to Rep. Jim Turner (D-Texas), who questioned the DHS Office of Information Analysis in a June 2003 hearing on the bioterrorist threat, DHS "was completely unprepared to provide the Committee with a current assessment of the threat from bioterrorism and appeared ill-equipped to provide a comprehensive assessment of threats to the homeland generally."

[78] Brownlee, Shannon, "A Shot in the Arm," *The New Republic*, May 12, 2003, http://www.tnr.com/doc.mhtml?i=20030512&s=brownlee051203.

[79] S.666 in the 108th Congress.

[80] The House of Representatives approved the Bush proposal 422-2, http://www.washingtonpost.com/wp-dyn/articles/A3506-2003Jul16.html.

[81] http://story.news.yahoo.com/news?tmpl=story&cid=679&ncid=742&e=14&u=/usatoday/20030618/cm_usatoday/5252320.

[82] Elizabeth Becker, "Meat Inspections Declining; Impact of Policy Is Contested," *New York Times*, July 10, 2003, p. A21.

[83] GAO-03-373, "Bioterrorism: Preparedness Varied Across State and Local Jurisdictions," April 2003, http://www.gao.gov/new.items/d03373.pdf.

[84] For more information on systemic upgrades to the public health system, see "Reforming Public Health for Bioterrorism," by Tara O'Toole M.D., http://www.ndol.org/ndol_ci.cfm?contentid=250032&kaid=124&subid=160.

[85] Connolly, Ceci, "Laws not up to SARS Epidemic," *The Washington Post*, April 26, 2003, A01.

[86] http://www.justice.gov/oig/special/0603/index.htm.

[87] http://www.washingtonpost.com/wp-dyn/articles/A34808-2003Jun26.html.

[88] The American Bar Association Task Force on the Treatment of Enemy Combatants set a series of guidelines for the treatment of U.S. citizens that are declared enemy combatants. http://www.abanet.org/leadership/enemy_combatants.pdf.

[89] S. Amend. 59 to H. J. Res. 2 in the 107th Congress.

[90] Markle Foundation Task Force, *op cit.*, p. 31.

[91] P.L. 107-56.

[92] One of the potential roadblocks to thwarting the Sept. 11 attacks was the FBI's failure to further investigate Zacarias Moussaoui because they did not believe they could qualify for a FISA warrant.

[93] S. 1534 in the 107th Congress. A similar proposal, based on the Hart-Rudman report, was introduced by Rep. Mac Thornberry (R-Texas) before the Sept. 11 attacks (H.R. 1158 in the 107th Congress).

[94] Chen, Edwin and Janet Hook, "A Pragmatic Bush Claims Cause as His Own Strategy," *Los Angeles Times*, June 7, 2002, p. A-21.

[95] For a summary of the new organization of the former INS, see http://www.bakerdaniels.com/newsstand/article.cfm?articleID=1545.

[96] Nichols, Hans, "House Security Panel May Not Survive," *The Hill*, July 1, 2003.

[97] Goo, Sara Kehaulani, "2 Transportation Security Officials Quit," *The Washington Post*, July 3, 2003, p. A4.

[98] See the testimony of Paul J. Redmond, Assistant Secretary for Information Analysis, before the House Subcommittee on Intelligence and Counterterrorism, June 5, 2003. Redmond resigned, citing health reasons, less than one month after his controversy-generating testimony.

[99] *Ibid.* For discussion of TSA efforts to reprogram funds to cover for shortfalls in airport screening.

[100] The joint inquiry by the House and Senate Intelligence committees issued a report in December 2002, which can be found at http://intelligence.senate.gov/pubs107.htm.

[101] "Bush drops opposition to 9/11 commission," Reuters News, September 20, 2002.
[102] Harding, James, "Kissinger Second Take," *Financial Time*s, December 14, 2002.
[103] The change in the White House's funding position may have resulted from inquiries by a journalist. For the full story see http://www.time.com/time/nation/article/0,8599,437267,00.html.
[104] Shenon, Philip, "9/11 Commission Says U.S. Agencies Slow Its Inquiry," *The New York Times*, July 2, 2002.
[105] A *New York Post* op-ed said that the commission was looking for a "scapegoat." http://news.yahoo.com/news?tmpl=story2&cid=106&u=/nypost/20030711/cm_nypost/seekinga911scapegoat&printer=1.
[106] For an overview of the effort to shrink the federal government by increasing budget deficits, see "Starving the Beast," by Ed Kilgore, *Blueprint*, June 2003, http://www.ndol.org/ndol_ci.cfm?kaid=127&subid=170&contentid=251788.

Acknowledgements

This report card represents a combined effort of Progressive Policy Institute scholars and researchers, including Robert D. Atkinson, John Cohen, Shane Ham, Will Marshall, Brian Newkirk, Steven J. Nider, and Sarah West. A special thanks goes to Shane Ham for pulling together disparate material into a coordinated report. PPI would like to thank the many individuals who shared their expertise during the development of this report card, including Jeffrey H. Smith, former general counsel of the Central Intelligence Agency, and Randy Beers, former senior director for combatting terrorism and special assistant to the president.

PPI also gratefully acknowledges the contributions of Congresswoman Jane Harman of California, the ranking Democratic member of the House Intelligence Committee. The work of Congresswoman Harman and her staff in investigating the administration's homeland security efforts served as crucial guidance in the development of this report card.

We would also like to thank Rep. Jim Turner of Texas, ranking Democrat on the House Select Committee on Homeland Security, and the committee staff for their invaluable help in the creation of this report card.