

**THE STATE OF HOMELAND SECURITY:
ASSESSING PROGRESS IN SECURING
THE UNITED STATES
AGAINST THE THREAT OF TERRORISM**

September 2003

Executive Summary

When the terrorists struck on September 11, 2001 it fell to the Bush Administration to take the nation to war. This is a war fought on many fronts and in distant lands from Iraq and Afghanistan to Yemen and Indonesia. Most significant was the addition of a new front, the U.S. homeland. For the first time in more than half a century, the threat was not only distant, posing dangers to America's allies and overseas interests; it had come to this country's shores.

As was the case the previous times the homeland was attacked, the United States was ill prepared for war. There had been a number of studies, some commissioned by the federal government, that warned of the possibility of major terrorist attacks on the United States and proposed plans to prevent or mitigate such dangers. A few tentative steps had been taken to develop policies and procedures relevant to terrorism and homeland security. However, there was no national strategy for homeland security, no dedicated agency or department and no priority assigned to the terrorism threat by law enforcement or the Intelligence Community.

The Bush Administration can claim an impressive list of accomplishments over the past two years. The Transportation Security Administration (TSA), in a unique partnership with private industry, deployed tens of thousands of screeners and hundreds of screening machines to more than 440 airports nationwide in less than a year. A new Cabinet department, the Department of Homeland Security (DHS), was created, merging some 22 agencies and offices into a single organization dedicated to securing the homeland. The Patriot Act permitted domestic and foreign intelligence information to be more readily shared. The Terrorist Threat Integration Center (TTIC) was established as a clearinghouse for intelligence. A new combatant command, Northern Command (NORTHCOM), oversees the protection of the North American continent and ensures adequate military support to civil authorities in the event of a terrorist attack. Billions of dollars have been invested in improving the nation's biodefenses, in the security of ports and waterways and in enhancing the capabilities of first responders.

These are all important first steps. Some major vulnerabilities have been addressed. If we are to express judgment of the administration's performance with a grade, it is clear that they warrant an overall grade of "A-." An explanation of the grading system used can be found in the section of the main report that addresses assessment methodology.

Assessing how well the Bush Administration has positioned itself for the long-term task of securing the homeland against the full range of potential threats is more problematic. Many of the steps taken by the administration, while significant, have been obvious responses to the most flagrant problems and to previously identified gaps. In some instances, such as the effort to improve emergency response capabilities, the administration has simply thrown money at the problem. Appropriate in the short term, these techniques will not work in the long term.

Two years removed from the fear that energized and spurred the government's actions, it is necessary to take stock. Complete security is impossible to achieve. Resources are finite. Hard choices need to be made and the administration requires a strategy to make those choices. However, no clearly defined long-term strategy has been put forth to replace this approach. Its title notwithstanding, the *National Strategy for Homeland Security* contains no strategy. It sets no priorities. It defines no useful measures of performance by which to judge progress.

It is difficult to determine whether the myriad long-term initiatives to secure the borders, counter bioterrorism or protect critical infrastructure will truly make the nation safer. Money and resources are being spent, but without a strategy and a good set of metrics or performance measures, it is not hard to draw the erroneous conclusion that the only way of enhancing homeland security is to spend and do more in every area and against all possible threats.

Furthermore, contrary to popular belief, it is not the administration alone that bears the onus of formulating a strategy. There is a need to resolve the issue of which areas of homeland security fall under the responsibility of the government to implement and pay for and which fall under the responsibility of the private sector.

Absent a strategy, clear metrics and resolution of the public-private issue, it is clear that the administration has a long way to go in taking on the hard tasks of long-term homeland security. Great vulnerabilities remain in areas such as airport security, border security and particularly in our emergency response and consequence management abilities.

On a sector-by-sector basis, this study's assessment of the long-term prospects for the security of the homeland is not entirely negative. Measures to enhance intelligence collection and information sharing, the physical security of ports and waterways, critical infrastructure protection, cyber security and military support to civil authorities, if continued, should yield significant improvements to the nation's security situation.

After what must be judged a good initial response to September 11, the Bush Administration merits no better than a "C+" for its efforts to develop a long-term strategy and program for the enhancement of homeland security. It remains to be seen whether the nation is going to invest the sustained effort necessary to deal with the real and possibly growing threat of terrorism or whether the nation is going to treat September 11 as a "one-shot" deal, and remain content with improved, but not comprehensive, homeland security.

Homeland Security Report Card

1.	Border Security	
	<i>Initial Actions</i>	A
	<i>Long-Term Prospects</i>	B
2.	Air Transportation Security	
	<i>Initial Actions</i>	A
	<i>Long-Term Prospects</i>	B
3.	Surface Transportation Security	
	<i>Initial Actions</i>	B
	<i>Long-Term Prospects</i>	C
4.	Chemical/Biological Defense	
	<i>Initial Actions</i>	B+
	<i>Long-Term Prospects</i>	C-
5.	Defense Against Nuclear Terrorism	
	<i>Initial Actions</i>	C
	<i>Long-Term Prospects</i>	D
6.	Emergency Response & Consequence Management	
	<i>Initial Actions</i>	B
	<i>Long-Term Prospects</i>	D
7.	Critical Infrastructure Protection	
	<i>Initial Actions</i>	B+
	<i>Long-Term Prospects</i>	A-
8.	Cyber Security	
	<i>Initial Actions</i>	B
	<i>Long-Term Prospects</i>	A
9.	Domestic Intelligence	
	<i>Initial Actions</i>	A-
	<i>Long-Term Prospects</i>	B
10.	Foreign Intelligence	
	<i>Initial Actions</i>	B+
	<i>Long-Term Prospects</i>	B+
11.	Military Support to Homeland Security	
	<i>Initial Actions</i>	A
	<i>Long-Term Prospects</i>	A
12.	Public Awareness and Crisis Communications	
	<i>Initial Actions</i>	B+
	<i>Long-Term Prospects</i>	C+
Overall		
	<i>Initial Actions</i>	<u>A-</u>
	<i>Long-Term Prospects</i>	<u>C+</u>

THE STATE OF HOMELAND SECURITY: ASSESSING PROGRESS IN SECURING THE UNITED STATES AGAINST THE THREAT OF TERRORISM

Assessing the state of homeland security nearly two years after the attacks of September 11 is a complex and challenging task. Anyone familiar with the workings of government knows that activity or expenditure is not the same as progress. There has been much activity in the area of homeland security since September 11 and a great deal of money has been spent. But the fundamental question remains: Are we safer now than we were on September 11, 2001?

At one level this is an existential question to which no concrete answer is possible. At another level it is an eminently practical question that demands detailed response. The Bush Administration is spending tens of billions of dollars on homeland security. It has created a new Cabinet department specifically devoted to homeland security. An inter-agency Terrorist Threat Integration Center has been created. Congress has passed laws, most notably the Patriot Act, to enable intelligence and law enforcement agencies to more readily detect and intercept terrorist attacks. While there have been numerous warnings of possible terrorist attacks, to date the United States homeland has not suffered another terrorist incident.

Yet some observers believe that progress in securing the homeland has been inadequate. Among the deficiencies they cite are inadequate or nonexistent screening of air cargo, the lack of funds for first responders or the slow rate at which available funds are disbursed, the limited protection available for U.S. ports and waterways and the lack of security for critical infrastructure. Responsibility for critical areas such as the defense against biological attack is fragmented among a number of government departments and agencies. There is a growing concern in the states and communities about the burdens and costs that heightened homeland security imposes. There are complaints, alternatively, either that the role of the private sector is not receiving sufficient attention or that too much weight and responsibility is being placed on the backs of private corporations.

As Secretary Tom Ridge acknowledges, there will never be enough money, people or equipment to make the United States absolutely secure. But it is precisely because preclusive security is a mirage that the American people need to know how much security they can expect not only in the near-term but once the Department of Homeland Security (DHS) and other federal state and local entities responsible for this task are fully stood up. They also need to know if their money is being well spent and if the government's actions are well advised.

Assessment Methodology

It is important to assess progress in securing the homeland not only from the perspective of security experts, but also from the point-of-view of the American people. The subject of homeland security is exceedingly complex and difficult to appreciate in its entirety. Simply understanding the workings of the new Department of Homeland Security, itself an amalgamation of some 22 agencies and offices with more than 170,000 workers, is a daunting task. So too, many have found, is an understanding and awareness of how to respond to the color-coded alert system created by the DHS. These two examples are important, for while they can be taken as signs of progress from the vantage point of expert knowledge, to many in the general public they appear to be process behaviors without identifiable outcomes.

When asked to consider the current state of their security, the average American is unlikely to have a comprehensive sense of what the term means, despite its common use. They may conjure images of the President making declarations, military personnel patrolling airports, or perhaps Tom Ridge being sworn in to the Office of Homeland Security. But, since the term “homeland security” describes a wide spectrum of functions, casual consideration of whether we are any safer than we were on September 11 yields little in the way of concrete answers. Faced with a blizzard of data on both government and private sector activities to enhance homeland security, the American people need help in understanding the answer to the question: Are you safer now than you were on September 11?

Providing that answer requires understanding how it might best be couched. Virtually all academic institutions (with the exception of those trendy schools which believe that to judge student performance is to inhibit their creativity and threaten their sense of self worth) express their judgments of individual performance in terms of grades. The most common grading schemes are either letters, typically “A” to “F,” or percentages from 100 to 0. While the basis for a grade can reflect an element of subjectivity, both systems have the twin virtues of simplicity and broad familiarity to the American public. For these reasons, the Lexington Institute chose to summarize its evaluation of the state of homeland security with a letter grade. Values for letter grades were assigned according to the standard four-point system with an “A” receiving 4 points. The grades reflect the difficulty of the challenges the nation confronted in each of the twelve areas as well as the performance of federal, state and local government and the private sector. The grades were then totaled and averaged to arrive at the final score.

In order to provide a valid or at least worthwhile judgment of performance, a grade must reflect the subject’s achievements in relation to the nature or magnitude of the challenge. Furthermore, the weight of a subject’s achievements must be assessed in light of the point from which they started. To employ a simple analogy, demonstrating an ability to write between the lines might earn a first grade student an “A” but not even warrant consideration for a high school senior.

The issue of perspective is also present in any evaluation of the state of homeland security. Experts differ in their judgments and in the grade they assign to efforts to enhance homeland security, depending on how they approach the subject. To some observers it is performance alone that matters, regardless of the magnitude of the challenge. Others emphasize the effort put forth and the extent to which the administration has fulfilled its stated objectives. Still others point to the warnings and assessments that could have set the country on a more rapid path toward enhanced security.

What are we measuring when we assess the state of homeland security and assign a grade? Much of the current literature on homeland security tends to focus on the magnitude of the problem and the administration's slow progress in addressing these many potential threats. These judgments are not entirely fair. Threats appear almost endless and overwhelming. Absent adequate threat assessments and vulnerability studies it is difficult for the new Department to establish sensible priorities for addressing the problem. Without a good set of metrics or performance measures, it is not hard to draw the erroneous conclusion that the only way of enhancing homeland security is to spend and do more in every area and against all possible threats. Without appropriate, commonly understood measures of merit, it is also impossible to know whether the American people are safer today than they were on September 10, 2001.

Yet defining appropriate performance measures for homeland security is a particularly challenging undertaking. Dr. Ruth David, president of the ANSER Corporation, described the challenge in this way:

One of the most difficult questions has to do with defining success. What is the goal of the homeland security mission? Are we defending America – the nation – or protecting every individual American from every conceivable terrorist threat? This question is not part of the national security agenda, but it is at the core of the homeland security debate. If we set the bar too high we face unaffordable resource requirements – a black hole of spending –and untenable loss of personal freedom. If we set it too low, American citizens may lose confidence in their government's ability to protect the nation from terrorism. If we fail to answer the question we have no context for decision making – no way to prioritize investments – and no way to measure progress.¹

Israel, representing the gold standard for security measures, is reported to foil 15 or 20 terrorist attacks or suicide bombings for every one that is successful. But is a failure rate of 5-6.5% acceptable? Perhaps, if each successful attack caused “only” a few casualties; but probably not if casualties were in the hundreds and definitely not if each event resulted in tens of thousands of dead and injured. Reducing the frequency of attacks is very important. But given the high likelihood that some attacks are going to get through, it is more important still to enhance our ability to limit the scope and scale of damage and loss of life to the lowest level possible.

Anthony Cordesman recognizes this reality and argues that the measure of merit for homeland security must reflect the reality that it is impossible to eliminate the threat.

¹ Dr. Ruth David, “Homeland Security: In Pursuit of the Asymmetric Advantage,” paper presented to the Committee on National Security Systems, 2002 Annual Conference, April 9-11, 2002, pp. 2-3.

Victory cannot be defined in terms of eradicating terrorism or eliminating risk. This war must be defined in much more limited terms. It will consist of reducing the threat of terrorism to acceptable levels - levels that allow us to go on with our lives in spite of the fact that new attacks are possible and that we may well see further and more serious tragedies.²

Cordesman's comment begs the question: What is an acceptable level of terrorism? Nominally, this will depend on the kind of attacks the terrorists can undertake, the amount of damage they can achieve and the likelihood of such attacks. But as a number of experts have observed, the standard risk calculus is skewed by the prospect of a terrorist attack involving weapons of mass destruction (WMD).³ It is perhaps better argued that while no terrorism is acceptable, the goal of homeland security should be to seek to prevent all attacks while ensuring that should a successful attack take place, the effects will not be catastrophic in terms of lives and costs.

This said, it is important to develop measures of performance, however imperfect or incomplete. Unfortunately, the federal government has yet to provide credible standards of success in the area of homeland security. In testimony before Congress, the Comptroller General of the United States, David Walker, noted the absence of measures of effectiveness (MOEs) for homeland security programs.

The Congress has long recognized the need to objectively assess the results of federal programs. For the nation's homeland security programs, however, we have not yet seen the development of appropriate performance measures or results-oriented outcomes.⁴

Measures of performance or effectiveness can either be input or output oriented. The majority of measures of performance or metrics that have been proposed are input oriented. These measures focus on the *process* of securing the homeland. Examples of input-oriented measures would be the manpower employed in homeland security, the dollars spent and the plans written. Output-oriented measures focus on results. They reflect the *consequences* of making changes to inputs. Examples of output-oriented metrics would be couched in terms of the ability to deter terrorists, interdict planned attacks or reduce damage in the event an attack is successful.

Input-oriented measures are the more readily definable of the two types. Moreover, it is far easier to chart progress on input-oriented measures. Both the start and end points for assessing progress are self-evident. Government tends to focus on input-oriented measures of merit. The success or failure of programs is often defined in terms

² Anthony Cordesman, *The Lasting Challenge: A Strategy for Counterterrorism and Asymmetric Warfare*, Center for Strategic and International Studies, November 30, 2001, p. 4.

³ Frank Cilluffo, Sharon Cardash and Gordon Lederman, *Combating Chemical, Biological, Radiological and Nuclear Terrorism: A Comprehensive Strategy*, Center for Strategic and International Studies, Washington, D.C., December 2000. On the debate in the United States regarding the threat of WMD attack see Richard A. Falkenrath, "Problems of Preparedness: U.S. Readiness for a Domestic Terrorist Attack," *International Security*, Vol. 25, No. 4, Spring 2001, pp. 149-153.

⁴ David Walker, *Homeland Security: Responsibility and Accountability for Achieving National Goals*, testimony before the Committee on Governmental Affairs, U.S. Senate, GAO – 02-672T, Washington, D.C., April 1, 2002, p. 7.

of the extent to which government achieves the process goals it defined for itself, regardless of the relevance of the attainment of those goals to solving the problem for which they were promulgated.

In an effort to establish output measures, the DHS is looking at identifying collateral benefits of homeland security activities and regulations. It has been suggested that measures to improve defenses against biological threats could have the secondary benefit of producing general increases in the health of the population. Similarly, some in the DHS argue that secondary economic benefits can be provided to companies through improvements in critical infrastructure.

Given the diversity of the potential threat and the great expanse of potential targets, virtually all experts agree that a comprehensive capability is preferred over one that is narrowly focused on a few, albeit highly dangerous, threats or a limited set of potential targets. This means that evaluating progress in homeland security must be done with an eye to the interrelationship between measures. In essence, grades must be based on a comprehensive perspective with respect to the effort to make the homeland more secure. A comprehensive perspective is one that focuses on the employment of all available means by which to address the threat. This view was expressed most directly by the Gilmore Commission:

It is axiomatic that, the better we are prepared, through a broad spectrum of antiterrorist and counterterrorist activities, the more likely we are to reach the ideal situation – the deterrence, prevention or interdiction of any terrorist event before it occurs. Given the nature of the potential threats, it is likely that no amount of preparation will cover all possible threat scenarios, and that adequate measures must be under-taken to respond to an event should it occur, in a way that will – first and foremost – minimize human casualties, and that will also mitigate damage to property and to the environment.⁵

As discussed above, a preclusive defense, one that protects all Americans against every kind of attack, is not possible. This presents a problem in defining appropriate output metrics. Should progress in securing the homeland, particularly in such areas as first response and attack mitigation, be assessed against the standard of the unlikely but highly destructive attack? Or, as argued by the Gilmore Commission, should the standard of assessment be the more likely attacks, those that are localized or less lethal?

What are appropriate output-oriented metrics? If outputs can't be measured in terms of attacks averted or terrorists caught, judgments must be based either on measurable changes in circumstances or conditions that make a terrorist attack possible, or on the existence of capabilities that reduce the consequence of such attacks. This must be done with a reasoned view toward the balance that must exist between different types of attack, the probability of their occurring and the consequences should the attacks actually come to pass.

⁵ Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (The Gilmore Commission), First Annual Report, I. *Assessing the Threat*, U.S. Government Printing Office, Washington, D.C., December 15, 1999, p. 52.

Limiting access by terrorists to the U.S. homeland or to weapons of mass destruction can support the overall capability for damage limitation. But the borders cannot be rendered impenetrable. Nor can access to all forms of WMD be denied with confidence. Therefore, increased security should be measured against the standards of potential lives saved and damage limited across a range of scenarios with an emphasis on potential catastrophic threat. Relatively simple measures can substantially reduce the consequences of low-order terrorism. But to a large degree, the likelihood that this type of terrorism will affect any single individual is statistically equivalent to random chance. Not so for catastrophic terrorism, which can kill thousands and permanently affect millions more. In this era of new threats, the success of homeland security must be measured in terms of the capabilities needed to survive even the worst form of attack.

The most important measures of success for homeland security are not quantitative, but qualitative. It is not the number of attempted acts of terrorism foiled, the mass of people deployed or the amount of resources expended. Rather, it is the existence of a family of capabilities that collectively provides high assurance of damage limitation and casualty reduction under all circumstances, but particularly against the threat of so-called catastrophic terrorism.

Furthermore, the adequacy of the measures taken cannot be judged against a static threat. By its very nature, the terrorist threat is both unknowable and ever-changing. Yesterday the threat was aircraft hijackers armed with knives, today it is man-portable, shoulder-fired anti-aircraft missiles and tomorrow it may be a ballistic missile armed with a weapon of mass destruction. Indeed, many terrorism experts assert that terrorists will naturally gravitate away from areas that are well protected, where the risk of detection is high and the probability of success is low, to less well-defended and easier targets. Hence, grading the administration's performance in securing the homeland must be based on recognition that an "A" in defending against today's threat is not adequate overall, if the grade for anticipating future threats is an "F."

A common issue in many evaluations of the state of homeland security is that how the effort is judged depends on what time frame one uses as measurement. Some analysts (and the administration itself) argue that assessments should be made based on the changes that have occurred since September 11. They feel that recognition should be given to how far the nation has come in two years, viewing that date as the nation's entry into the world of counterterrorism and homeland security. If one is to grade the effort in these early "elementary" years, the overall conclusion must be that enormous progress has been made. The government to this date has moved very rapidly in a wide variety of directions. In some cases, missions have not quite been fulfilled, but major progress has been made.

Homeland security is a long-term endeavor. While it is important to understand how far the nation has come in a very short time, it is perhaps more important to know how much farther the nation has to go and the pace at which it is progressing toward that goal. Thus, grading the nation's accomplishments in securing itself from terrorist attack must recognize both near-term and far-term dimensions. What was an adequate response

in the immediate aftermath of September 11, as the nation reeled from the attack, in terms of the speed, scale and breadth of the actions taken, may not be sufficient in any of these respects two years later. Thus, to continue the school analogy, as one graduates to higher levels of education, expectations rise. At this level, the administration has to show a long-term strategy and competence in how it would deal with the gross terrorist threat – the things that are going to be catastrophic. Here the administration’s performance is, as yet, spotty. It is for this reason that this study provides separate grades for both the initial efforts to secure the homeland and for those activities designed to provide more comprehensive responses to the terrorist threat over a longer time frame.

Progress in Homeland Security: Grading the National Effort

Beginning in January 2003, the Lexington Institute undertook a study to assess rigorously the administration’s homeland security efforts to date. Based upon a review of government proposals and plans, the Institute identified twelve functional areas whose aggregate represents the homeland security effort. A team of twelve nationally recognized scholars was assembled to conduct assessments of the current state of progress in each area. Their papers are published on the Institute website at www.lexingtoninstitute.org/homeland/index.asp. The names of the experts and the areas they addressed are provided below.

Topic	Evaluator
Emergency Response & Consequence Management	Dr. Joseph Barbera Co-Director of the George Washington University Institute for Crisis, Disaster, and Risk Management
Domestic Intelligence	Mr. Robert M. Blitzer Associate Director of SAIC’s Center for Counterterrorism Technology and Analysis Former chief of the Domestic/Counterterrorism Planning Section of the FBI
Air Transportation Security	General Joel Feldschuh, MBA Chairman & CEO, Ganden Security Services Solutions (GS-3) Former CEO of El Al Airlines
Border Security	Lieutenant Colonel (Ret.) Frank Hoffman Consultant, EDO Professional Services Former principal analyst and author for the Hart/Rudman Commission’s homeland security assessments
Ground Transportation Security	Mr. Brian M. Jenkins Research Associate, Mineta Transportation Institute

Nuclear Defense	Dr. David Kay Senior Fellow at the Potomac Institute for Policy Studies Special advisor for strategy to assist the United States in searching for Iraq's weapons of mass destruction Former UN Chief Nuclear Weapons Inspector
Foreign Intelligence	Ms. Ellen Laipson Chief Executive Officer of the Henry L. Stimson Center Former Vice Chairwoman of the National Intelligence Council
Cyber Security	Dr. Martin C. Libicki Senior Policy Analyst, RAND Corporation
Military Support to Homeland Security	Dr. Steven Metz Director of Research and Chairman of the Regional Strategy and Planning Department at the U.S. Army War College
Chemical/Biological Defense	Mr. Michael L. Moodie President of the Chemical and Biological Arms Control Institute
Critical Infrastructure Protection	Mr. Michael Scardaville Policy Analyst, The Heritage Foundation
Public Education & Media	Dr. Loren B. Thompson Chief Operating Officer of the Lexington Institute and adjunct professor at Georgetown University

Efforts by the Hart-Rudman and Gilmore Commissions, Richard Clarke of the National Security Council Staff and organizations such as the Center for Strategic and International Studies and the Council on Foreign Relations to address the potential terrorist threat to the homeland, had been underway in the years and months prior to the attack. Nevertheless, September 11 was a wake-up call. A new Cabinet department, the Department of Homeland Security, was quickly created. As one observer noted, “with the stroke of a pen the President initiated the largest reorganization of our government since World War II.” The creation of the DHS, in conjunction with the signing of the Patriot Act, served to greatly dilute the barriers in sharing intelligence between domestic and foreign agencies. Likewise, the establishment of the DHS and the issuing of the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* and the *National Cyber Security Plan* resolved many of the interagency coordination efforts of the past and clearly established the Department as the central figure in the federal government’s program. The Freedom of Information Act and anti-trust exemptions in the Homeland Security Act of 2002 should open the door to increased public-private communication, and further bolster critical infrastructure efforts.

The Bush Administration moved rapidly to address the most obvious national vulnerabilities, those that would make it all but inevitable that the homeland would be

struck not once, but many times, and not with small attacks, but catastrophic ones. In creating the Department of Homeland Security, Washington sought to close obvious gaps in homeland security caused by the distribution of responsibilities among dozens of Cabinet departments and government agencies. The Transportation Security Administration, in a unique partnership with private industry, was able to deploy tens of thousands of screeners and hundreds of screening machines to more than 440 airports nationwide in less than a year. A new combatant command was created, Northern Command, to oversee the protection of the North American continent and to ensure adequate military support to civil authorities in the event of a terrorist attack. These are important first steps.

Border Security

A major effort was initiated shortly after September 11 to improve security at U.S. borders and ports. Fear that terrorists might clandestinely deliver weapons of mass destruction in cargo containers led to new security measures on U.S. ports and borders and, on February 2, 2003, new shipping procedures. Within the Department of Homeland Security, virtually all the federal agencies with responsibility for securing U.S. borders (Border Patrol, Customs Service, Immigration and Naturalization Service [INS] and Coast Guard) were united in a single directorate. Operation *Liberty Shield* was initiated to provide, inter alia, enhanced land and maritime patrolling of the nation's borders.

One of the first steps taken by the U.S. Customs Service to enhance maritime trade and border security has been its Container Security Initiative (CSI). The Customs Service is negotiating agreements with the customs agencies of America's major trading partners to establish uniform procedures for screening and inspecting cargo before loading aboard U.S.-bound vessels. As part of these agreements, U.S. customs officials are being "forward deployed" to major overseas shipping ports, and being granted access to shipping manifests and to observe loading procedures. Currently, 18 of the world's top 20 seaports, representing nearly 70 percent of all of the containers shipped to U.S. seaports, have signed agreements with American customs officials to help secure international trade from terrorism.

Under the 2002 Maritime Transportation Safety Act, ports, vessels and facilities are required to conduct vulnerability assessments and develop security. Implementation of those plans will require their review by the DHS and a determination of who will pay for security improvements. The U.S. Customs and Border Protection directorate has recently published proposed regulations to obtain advance information concerning shipments of goods to the U.S.

A corollary with CSI is the Customs-Trade Partnership Against Terrorism (C-TPAT), a public-private endeavor between the U.S. Customs Service and the trading industries to develop and maintain effective security processes throughout the global supply chain. Within a little more than a year, the C-TPAT program has been

implemented extensively throughout the trade community with more than 1,600 carriers, brokers, shippers and freight forwarders voluntarily participating.

Another positive step is the initiation of Operation Safe Commerce (OSC) under the auspices of the Department of Transportation and U.S. Customs Service. This initiative provides a live experimental test-bed for a series of new security techniques to increase the security of container shipments. Congress, in the 2002 Supplemental Appropriations Act, provided \$28 million for OSC to improve the security of container shipments through pilot projects involving the United States' three largest container ports of entry (Los Angeles/Long Beach, New York/New Jersey and Seattle/Tacoma).

One of the more important initiatives underway has been the increased awareness of the need for a recapitalization of the Coast Guard. The Coast Guard has an increasingly important role to play in homeland security. But its ships and aircraft are aging and technologically obsolete. As a result, it has excessive operating and maintenance costs, and lacks essential capabilities in speed, sensors and interoperability. The administration belatedly recognized this and, in response, increased funds for the Coast Guard's primary modernization program, known as Deepwater. This program will replace the Coast Guard major cutter fleet and upgrade its helicopter assets. At a cost of \$17 billion, the program will materially enhance the Coast Guard's ability to secure U.S. trade and ports, conduct navigation and public safety missions, and enforce U.S. laws. In particular, a new suite of Command, Control, Communications and Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems will extend the Coast Guard's capacity to detect and identify all activity in the maritime arena. This capability, known as "maritime domain awareness," is needed to improve the nation's ability to intercept and engage those activities that pose a direct threat to U.S. sovereignty and security.

In addition to reorganizing the operation of agencies responsible for border security, the DHS has taken steps to make it more difficult for terrorists to enter the United States. The U.S. Visitor and Immigrant Status Indication Technology system (U.S. VISIT) is designed to make entering the U.S. easier for legitimate tourists, students and business travelers, while making it more difficult to enter the U.S. illegally through the implementation of biometrically authenticated documents.

Positive initial steps could be undermined by a lack of investment in the next few years. Observers have noted that border security, which seeks to prevent attacks, is receiving relatively fewer resources than other areas, principally those intended to deal with the consequences of an attack. Many opportunities to exploit technology may be missed if the DHS is unable to invest in long-term research and development.

Initial Actions: Grade A. The administration has taken a number of very important steps over the past two years to enhance border security. It has closed a number of security gaps involving the movement of both people and material across U.S. borders. In particular, steps have been taken to improve maritime intelligence, secure international shipping and enhance the security of U.S. ports.

Long-term Prospects: Grade B. There is still an ingenuity/technology gap that needs to be closed. Complacency and lack of investment are significant dangers that could prevent the closing of this gap.

Air Transportation Security

On November 19, 2001 President Bush signed into law the Aviation and Transportation Security Act (ATSA), which among other things created a new Transportation Security Administration (TSA) within the Department of Transportation. The ATSA legislation put airport security under federal responsibility for the first time. It also set deadlines for achieving a better-secured travel system, including a November 19, 2002 deadline for hiring, training and deploying a federalized screeners force, and a December 31, 2002 deadline for deploying Explosive Detection Systems (EDS) machines at all of the nation's 429 commercial airports. These quick actions by the government were important, not only in providing deterrence to potential terrorists who might seek to mimic Al Qaeda's September 11 feat, but also in lowering public anxiety.

The creation of the TSA and the deployment of tens of thousands of screeners and hundreds of machines to the nation's airports all within a year stands as a singular demonstration of what government can accomplish. Yet critics of the administration's aviation transportation security program point out that cargo shipments are not adequately screened. In addition, the administration has yet to formulate an approach for dealing with the problem of man-portable surface-to-air missiles.

Initial Actions: Grade A. In terms of meeting ATSA near-term legislation deadlines and restoring public trust in aviation security, there should not be any doubt: the TSA has done an excellent job. Ninety-five percent of TSA resources went toward meeting the two deadlines in the public spotlight – the November 19, 2002 deadline for hiring, training and deploying a federalized screeners force, and the December 31, 2002 deadline for deploying the EDS/ETD screening system in airports.

Long-term Prospects: Grade B. There are still many loopholes in the overall security system in various areas of cargo, mail, perimeter, onboard security, etc. Moreover, September 11 can be attributed in part to the intelligence agencies' failure to divert sufficient resources to study those threats thoroughly, evaluate them and communicate with each other in order to share valuable information at the opportune time. Therefore, long-term homeland security strategies need to focus as much upon intelligence as upon air security.

Surface Transportation Security

The creation of the TSA also represented an opportunity to build security into the nation's ground transportation sector, and the Department of Transportation's Federal Transit Administration was proactive in reviewing security measures and discussing improvements with industry associations and state governments. It quickly followed by

aggressively implementing the easy measures first, including increased presence of uniformed and plainclothes security staff, more frequent security patrols, and well-publicized announcements about remaining vigilant for suspicious activity and abandoned packages. The administration's focus on airline security, as opposed to ground transportation security, has been appropriate because attacks to airliners can produce orders of magnitude more casualties than even the bloodiest incidents of non-airline sabotage or truck bombs. They also can result in far more economic disruption. Even so, a review of events on and immediately after September 11 showed that local surface transportation systems played a vital role in evacuation, rescue, communications and recovery.

It is clear that relatively less attention has been focused on protecting surface transportation. In part this is because the consequences of an incident are likely to be less severe than those generally associated with a terrorist incident involving aircraft. It also reflects the more fragmented nature of the nation's surface transportation systems. Inherent vulnerabilities and high ridership make surface transportation systems both attractive targets and difficult to protect.

Following September 11, the Department of Transportation's Federal Transit Administration reviewed security measures and discussed improvements with industry associations and state governments. Systems operators and local police implemented the easy measures first. They increased the presence of uniformed and plainclothes security staff and conducted more frequent patrols. The public was asked to remain vigilant for suspicious activity and abandoned packages. Doors leading to vital systems were locked and stations were tidied to reduce hiding spaces. Crisis plans were reviewed and responses exercised.

Current plans focus largely on encouraging state and localities as well as private operators to maintain enhanced security. Although the Transportation Security Administration within the DHS will have authority over surface transportation, its role to date has been largely advisory. DHS's science and technology directorate is supporting research in the area of surface transportation safety and security.

Initial Actions: Grade B. Understandably, the administration's initial focus has been on commercial aviation, followed by cargo containers. The federal government has not attempted to extend to surface transportation the same authority it has for aviation security. In the short term, the Department of Transportation's Federal Transit Administration was proactive in reviewing security measures and discussing improvements with industry associations and state governments. This was followed up by aggressively implementing "the easy measures first." Responsibility for the security of surface transportation remains with state and local law enforcement authorities and the public and private entities that own and operate the transportation infrastructure and assets. The creation of the TSA represents an opportunity to build security into the nation's transportation sector in a more systematic way.

Long-term Prospects: Grade C. Much progress had been made since September 11, but most of the improvements have addressed the easy issues. Further significant improvements, such as detecting chemical or biological attacks, remain a challenge – and would cost billions. Insufficient funding is the most significant challenge in making transit systems as safe and secure as possible. There is some lack of clarity regarding the responsibility of government vs. the private sector in this area. Ground transportation security should have two strategic objectives in the long-term; prevent casualties and minimize disruption/rapidly restore operations.

Chemical/Biological Defense

Defense against catastrophic threats was one of the critical mission areas listed in the *National Strategy on Homeland Security*. The strategy identifies a number of major initiatives, several of which relate directly to the chemical or biological weapons threat. This document also requires that extra attention and targeted federal funding be directed to several areas, notably defense against bioterrorism. An important aspect of biodefense is the strengthening of the nation's public health and emergency medical system.

The administration has programs underway across the critical functions necessary to ensure an effective response to a chemical or biological attack. An effective response capability can be assessed in terms of capacities to handle a major incident, including one involving pathogens for which no current prophylactic measures exist. Programs in this area involve surveillance and reporting, epidemiology, laboratory analysis, preparedness planning, training and education, communication and information, medical research and development, and consequence management and mitigation.

The administration identifies surveillance and reporting as critical functions in an overall response architecture. It recognizes, however, that any system based only on responding to bioterrorism is not sustainable, either financially or functionally. For that reason its efforts to improve surveillance capacities are grounded in public health surveillance and reporting systems that seek to exploit a variety of different information sources. For this approach to be successful, it requires a high degree of cooperation from local medical services and practitioners. The extent of cooperation should be viewed as an important output-oriented metric for assessing progress in this area.

Another function to which the administration has given considerable priority is enhancing laboratory capacity. This involves, first, building overall capacity, which is being promoted primarily by federal funding of state and local preparedness efforts, particularly through the Centers for Disease Control and Prevention (CDC). The goal is to expand the number of bioterrorism agents that state and local labs can identify, expand their ability to handle dangerous pathogens and implement appropriate protocols. In the FY 2003 budget, the President requested \$200 million to improve state and local laboratory capacity. Enhancing lab capabilities also focuses on improving linkages between state and local public health laboratories and private sector and clinical laboratories. The major initiative in this regard is the Laboratory Response Network

(LRN), which establishes connections between laboratories with different safety and containment levels, as well as different proficiencies in identifying agents.

A third priority area for the administration has been medical research. The National Institute for Allergies and Infectious Diseases (NIAID) at the National Institutes of Health (NIH) spearheads this effort. The Bush Administration requested more than a six-fold increase in bioterrorism research totaling \$1.748 billion. As part of Project Bioshield, the President called for an additional \$6 billion over 10 years to ensure that resources are available for developing “next generation” medical countermeasures.

Another important priority has been to build capacity and bolster capabilities at the state and local level to improve consequence management and mitigation. The administration has focused on three programs: the Metropolitan Medical Response System (MMRS), the Public Health Preparedness and Response for Bioterrorism Initiative, and the Bioterrorism Hospital Preparedness Program. The primary focus of the MMRS is to develop or enhance existing emergency preparedness systems at the local level. Over the past five years, MMRS has achieved its goal of getting the participation of the 122 most populous U.S. cities. The Public Health Preparedness and Response Initiative focuses specifically on the public health dimension of local response capabilities. The Bioterrorism Hospital Preparedness Program, run by the Health Resources Services administration (HRSA) of the Department of Health and Human Services is intended to enable states and municipalities to upgrade hospitals and other health care facilities, develop a multi-tiered system in which local health care facilities are prepared to triage, treat, stabilize and refer multiple casualties to identified centers of excellence, or develop multi-state or regional consortia to pool limited funding to accomplish these goals.

The administration must be commended for the breadth of the initiatives it has taken in the area of defense against biological/chemical attack. This is an ambitious agenda. In some instances, it may be too ambitious. One need only point to the smallpox vaccination plan, intended to inoculate some 500,000 first responders. As of August 2003 barely 40,000 first responders had agreed to be inoculated. In addition, there are reports of disparities in how federal funds are being employed at the state and local levels.

Initial Actions: Grade B+. The complexity and multidimensionality of the challenge demands a response that is equally complex and multidimensional if it is to be effective. Defense against chemical/biological attack requires investment in plans, policies, procedures, training, technology and science. It requires a focus not only on emergency response and first responders but also on the nation’s medical service system. Initial efforts have strengthened emergency response capabilities. Most of the administration’s major initiatives will take years of focused effort and continuous investment in order to bear fruit. The failure of the voluntary smallpox inoculation program must be viewed as a serious setback for the administration.

Long-term Prospects: Grade C-. The administration’s short-term efforts to address chemical and biological threats to U.S. homeland security have produced

progress, but have still not achieved the goal of providing the necessary level of preparedness. In the long-term, the reality is that there is neither a single measure that will “solve” the problem nor one set of activities that can be pursued to accomplish the goal. Rather, incremental improvements across a wide range of response measures are required, and they are the only means by which progress can be made in the face of limited resources. Many medical professionals and facilities and military personnel have not participated in the President’s vaccination program because of uncertainty about the likelihood of attack and concern over adverse effects of vaccination. This reaction highlights the fact that the public is not necessarily comfortable with the current national policy. In addition, the entire U.S. system for developing and producing vaccines needs attention – vaccines for smallpox and anthrax are prioritized, but there are marked shortages of vaccines for many other serious agents. A national strategy for developing, producing, stockpiling and distributing vaccines needs to be elaborated.

Defense Against Nuclear Terrorism

Some of the measures taken to improve homeland security against chemical/biological attacks will also contribute to mitigation of a nuclear attack. This is particularly true for a radiological dispersal device (RDD) that would affect, at most, a few square blocks. In the event a nuclear device is detected, elements of the DHS such as the Domestic Emergency Support Teams and Nuclear Incident Response Teams could help locate and neutralize the device. However, the sheer scale of destruction associated with a nuclear detonation would overwhelm virtually any local response capability. Such an event would require a swift, massive, national response involving thousands or even tens of thousands of rescue and medical personnel, as well as massive amounts of equipment and supplies.

A nuclear detonation on U.S. soil is considered by most experts to be a low probability event. Maintaining a ready capability to respond to such an event is an extremely expensive proposition. At best, it may be possible to augment planned efforts in the areas of emergency response training and material stockpiles. Therefore, the success of the administration’s actions to combat nuclear terrorism must be judged largely from the perspective of preventing such weapons from reaching U.S. shores.

The United States has intensified its counterproliferation efforts in the aftermath of September 11. It is working with like-minded nations to stem the traffic in WMD technology and materials. After some hesitation, it is continuing with the Nunn-Lugar programs to secure the nuclear stockpile and know-how that is resident in the states of the former Soviet Union. It is pursuing multilateral negotiations to eliminate the WMD threat posed by North Korea.

At the same time, the United States has promulgated a National Security Strategy that addresses in new ways the WMD threat to the homeland. The new Strategy argues that the ability to deter attacks on the U.S. homeland is less certain in the 21st Century than was the case during the Cold War. For this reason, the threat of retaliation alone is insufficient as a response to proliferation of WMD. The Bush Administration concluded

that new capabilities and doctrines were required. It announced the creation of a new strategic Triad consisting of air and missile defenses, nuclear and conventional strike capabilities and a healthy nuclear weapons development capability. The administration also declared that it would, under certain circumstances, act in anticipation of the emergence of a WMD threat. Finally, the administration continued its commitment to maintaining a robust and flexible strategic nuclear capability. These measures, it is thought, might dissuade some potential proliferators from pursuing a WMD program. If not, the United States would now have a broad array of options for dealing with the emerging threat.

With the end of the Cold War, U.S. intelligence capabilities to track nuclear developments were allowed to seriously decay. A serious investment is needed in the full range of intelligence means focused on nuclear enterprises worldwide.

Initial Actions: Grade C. The topic of assessing preparedness for nuclear attack has a longer history in popular literature than most other functional areas of homeland security. However, nearly two years beyond September 11, and more than eight months beyond the point where the Homeland Security Department started to emerge as a real possibility, it is difficult to give this area more than an “incomplete.” Overseas measures to restrict proliferation of nuclear weapons may be bearing fruit. So, too, may steps to enhance the military’s capability to interdict or intercept a nuclear attack.

Long-term Prospects: Grade D. The nuclear club is growing. More countries may develop and even deploy nuclear weapons in the next several decades. It is therefore irresponsible not to consider measures in anticipation of the possibility, however remote, that a nuclear weapon may be detonated in the United States. An extensive national effort over a number of years will be required if the United States is to develop the capabilities to mitigate the consequences of a nuclear attack. At present, little is being done to even develop the plans for such an effort.

Emergency Response/Consequence Management

Improving the nation’s capacity to respond to emergencies, principally by enhancing the capabilities of first responders, is the administration’s number one priority in homeland security. In fiscal year 2004, the administration plans to spend a little over \$7 billion on federal, state and local capabilities. An honest assessment of all the unfunded needs of a national emergency response system might well result in resource requirements close to triple that amount.

To improve on-site management of federal assets in the immediate aftermath of an incident, the Federal Emergency Management Agency (FEMA) initiated plans for the rapid deployment of DHS Incident Management Teams. To significantly strengthen the DHS emergency response capabilities, FEMA began incorporating Domestic Emergency Support Teams, Nuclear Incident Response Teams, the National Disaster Medical System and the Strategic National Stockpile into its planning and response capabilities.

Money is being spent and the DHS is attempting to provide direction to the first responder communities. However, the nation still lacks a framework to spend the money smartly. The administration needs to set a strategy for guiding its investments. Most grant money is distributed on a per capita basis with fixed base amounts for each state. The result is spending a little money on everything and not a lot of money on the most important things.

It is clear that homeland security at the state and local levels cannot be a “one size fits all” proposition. Nevertheless, there needs to be a set of basic standards. Also, the states and localities need guidance based on experience and best practices. The DHS has taken the important step of developing a template for state-level security plans. At the time of this report, response of the states has varied widely, with some yet to produce plans and others providing only an outline of what must follow.

In light of the scale and scope of the problem, emergency response may be the most difficult area under the rubric of homeland security. The federal government needs to ensure that first responders get the necessary equipment and basic training and, at the same time, ensure that federal funds are spent appropriately.

National standards for emergency response need to be established. Without real standards there is no way to realistically determine the nation’s most important unfunded needs. In addition, standards are essential for determining levels of readiness and how much spending is enough.

Initial Actions: Grade B. The administration has made progress in terms of programs in surveillance and reporting, epidemiology, laboratory analysis, preparedness planning, training and education, communication and information, medical research and development, and consequence management and mitigation.

Long-term Prospects: Grade D. This is one of the weakest areas of preparation, primarily because it is an area that depends upon coordinated actions of everyday medical and public health personnel who have never faced the magnitude of threat for which they need to be prepared. Public health and acute-care medicine encompass very diverse resources, which are widely separated in management methods, goals, and funding and preparedness. Many of the current threats have not been widely experienced during the modern medical era. While there must be an urgency to prepare for terrorism at the national level, successful response and incident management requires effective local capability and capacity in the affected jurisdictions.

Critical Infrastructure Protection

The task of protecting the nation’s critical infrastructure is one of the most daunting challenges facing governments at all levels. Critical infrastructure encompasses the complex systems that have developed over many years to manage the production and distribution of critical commodities such as energy, food and water, and to manage vital functions such as banking, telecommunications, transportation, health care and the

production of major commodities essential to a modern post-industrial state. Further complicating the task of protecting this infrastructure is the fact that most of it is privately owned.

The Clinton Administration undertook the first nationwide effort to deal with the problem of critical infrastructure protection. It created a series of information sharing and analysis centers (ISACs) for critical industries, each one led by a specific federal department or agency. Lead federal agencies worked with specific sectors of industry to identify vulnerabilities and develop contingency and response plans.

Since September 11, the Bush Administration's efforts in this area have focused on two objectives. The first is creating overarching national policy and a unified capability in the DHS to deal with the task of critical infrastructure protection. The second is working with industry to identify and evaluate potential targets and their vulnerabilities on an industry-by-industry basis.

The administration has published a number of important policy documents in this field including the *National Strategy for Homeland Security* in July of 2002, the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* in February 2003, and the *National Strategy to Secure Cyberspace* also in February 2003. These documents expanded the definitions of critical industries and proposed goals and standards for the development of critical infrastructure protection programs and plans.

The Homeland Security Act of 2002 transferred the National Infrastructure Protection Center (NIPC), the Critical Infrastructure Assurance Office (CIAO), the energy security and assurance programs of the Department of Energy, the National Infrastructure Simulation and Analysis Center (NISAC), the Federal Computer Incident Response Center (FedCIRC) and the National Communication System (NCS) to the Department's Information Analysis and Infrastructure Protection Directorate (IAIP). This concentration of responsibilities for threat assessment, vulnerability analyses and response planning into a single directorate was an important first step in enhancing the security of critical industries. It may also contribute to the ability to address cyber security issues.

The administration also addressed the role of the private sector in the protection of critical industries. The Homeland Security Act provided legal protection to private industry in order to facilitate closer cooperation with the government. First, anti-trust protections allowed businesses to share information related to infrastructure vulnerabilities or protection measures either directly or through an ISAC. Second, the Act expressly exempted information related to critical infrastructure protection efforts voluntarily shared by industry with government from release under the Freedom of Information Act.

One of the most important issues in critical infrastructure protection is an industry-by-industry threat and vulnerability assessment. In November 2002, the NIPC recommended a five-step risk management tool to industry. While this is a necessary first

step, almost a year later it is unclear how far this process has moved or, whether having done these assessments, anything has changed on the ground to improve the security of critical infrastructure.

Initial Actions: Grade B+. The administration has taken a number of important steps to build on the efforts of its predecessor and expand the area of critical infrastructure protection. Efforts are beginning to perform the necessary threat and vulnerability assessments, with some sectors well advanced. As yet, little has been done, as suggested by a recent study by the Council on Foreign Relations, to actually enhance the physical security of critical industries. Action must follow analysis.

Long-term Prospects: A-. Continuing progress in this area should enhance security over the long-term. In particular, government and industry will be able to establish standards and identify requirements for enhanced protection of the truly critical elements or “nodes” in each infrastructure sector.

Cyber Security

The effort to improve cyber security is challenged by the lack of clarity with respect to the threat and disagreements as to the best approach for providing protection for the nation’s computer networks. There are constant reports of attempts to hack private and government systems. While virus, worms and the like do cause problems, these tend to be relatively small-scale and of short duration. Data theft may be the most significant danger in cyber space from both national and private security perspectives. At the same time, it is important to note that the evidence of significant successes against critical systems is almost nonexistent.

One of the greatest advantages the United States possesses in the area of cyber security is the dynamism of the private sector. Cyber security is a robust and growing industry. The so-called “white hacker” community is constantly testing commercially available software and proposing fixes for security problems. There is a strong push to establish common metrics for cyber security. The use of common criteria and best practices to measure software quality is increasing. This effort is being aided by the adoption of ISO 17799 that attempts to measure the quality of an organization’s information security process.

Cyber security is largely a matter for the private sector. Most cyber security problems could be addressed simply by good practices, such as updating virus software and password-protecting systems. One way of creating incentives for the private sector to take cyber security more seriously would be to develop a robust insurance business to cover damage from cyber-attacks.

Initial steps: Grade B. Efforts to monitor cyber space and continually reassess threats are important tasks for the DHS and other relevant branches of government. At the same time, the government needs to avoid over-investing in this area.

Long-term Prospects: Grade A. The nation may be much less vulnerable to cyber attack than has been suggested in most public analyses, and may over-exaggerate the threat. The fear of cyber attacks may outstrip the realities of the damage such attacks can incur, and the tools for protecting computers may already be readily available to those who wish to use them.

Domestic Intelligence

The initial response of the Federal Bureau of Investigation (FBI) to September 11 was, simply put, remarkable. Director Robert Mueller immediately set out to transform the FBI. The Bureau's counterterrorism program was reorganized. Fifty-six Joint Terrorism Task Forces (JTTFs) were established, one in each of the FBI's field offices. Resources have been and are being moved from traditional criminal investigative programs into the counterterrorism program, so that domestic intelligence operations, including the development of human sources and the lawful employment of electronic collection, can be implemented quickly and effectively. A multi-year effort is underway to upgrade the FBI's antiquated computer systems and to allow for the integration of databases resident in other government departments and agencies.

The enactment of the still-controversial Patriot Act was extremely important as a means of enhancing domestic intelligence capabilities. The Patriot Act permits the dissemination of intelligence collected domestically or through testimony at Federal Grand Jury sessions to other elements of the Intelligence Community. The Patriot Act also improves processes to secure subpoenas for the records of electronic communications, permits Foreign Intelligence Surveillance Act (FISA) court orders for business and other records, provides for a more flexible method of securing telephone toll records and allows for streamlined procedures for securing FISA court orders.

The sharing and analysis of intelligence information was further enhanced by the creation of the Terrorist Threat Integration Center (TTIC). The TTIC is not intended to replace the existing Intelligence Community. Rather, its purpose is to be a "clearing house" for terrorist threat information. As yet, it is too early to tell whether the TTIC will serve as a major improvement in the fight against terrorism.

Another major issue is the creation of an information architecture to permit the rapid exchange of information among domestic and foreign intelligence agencies. At present, many of the relevant agencies and departments have antiquated and incompatible information-storage systems. Solving this problem will require a major sustained investment of resources.

Initial actions: Grade A- The creation of the DHS and signing of the Patriot Act have served to greatly dilute the barriers in sharing intelligence between domestic and foreign agencies. The creation of the TTIC was also a significant step forward.

Long-term prospects: Grade B. In the future, massive work remains to be done in all of these areas given the fact that most of the federal agencies with these responsibilities have been under-funded and generally not supported in their core

missions over many years. The DHS must be given the authority and funding it needs to succeed.

Foreign Intelligence

In the war on terrorism, the Intelligence Community has been working hard for nearly a decade to develop a capacity to collect and interpret a vast quantity and variety of data. To support this effort, the Central Intelligence Agency (CIA) created the Counterterrorism Center (CTC). Prior to September 11, the CTC had a modest analytic team. The CIA and other intelligence agencies have redirected assets to the problem of counterterrorism. But, as is the case with domestic intelligence, recruiting regional experts and those with relevant linguistic skills remains a serious challenge.

Collection and analysis of information are two continuing issues of concern for the Intelligence Community. Another is the timely dissemination of information. It is by now clear that one of the causes of September 11 was the failure to make sure that a new piece of information was not just stored in a database but also conveyed, with a proper sense of urgency, to people in other parts of the federal system. Intelligence and law enforcement, intelligence and immigration, law enforcement and visas, borders and law enforcement: all these critical interfaces were under-developed. The creation of the TTIC is an attempt to solve this problem.

Initial Actions: Grade B+. The Freedom of Information Act and anti-trust exemptions in the Homeland Security Act of 2002 should open the door to increased public-private communication. In addition, the fusion of information analysis with vulnerability assessments and closer cooperation offers the prospect of dramatically increasing the synchronization and comprehensiveness of the infrastructure protection efforts at all levels of government and in the private sector.

Long-term Prospects: Grade B+. Much will hinge on how quickly the myriad of federal agencies transferred to the DHS are consolidated into a focused effort. Likewise, since so much of the administration's effort hinges on information analysis, reforms in how intelligence is shared will be crucial to the success of the Department's efforts. If the Terrorist Threat Integration Center fails to overcome the stovepiping of the pre-September 11 era, it will likely create a major obstacle for the administration's critical infrastructure protection efforts.

Military Support to Homeland Security

The military has been able to effectively shift its focus from exclusively external enemies to a balance between external and homeland security, largely because mechanisms for shifting to greater emphasis on homeland security were already in place. The Department of Defense (DoD) has been institutionalizing robust procedures for transformation over the past decade. Dealing with asymmetric threats, including terrorism, was one of the foci for transformation.

The Services were already working on capabilities and concepts for homeland security before the September 11 attacks. Military efforts to support homeland security activities were generally handled under the Joint Task Force Civil Support. Following the September 11 attacks, the Office of the Secretary of Defense (OSD) and the Services created a range of new organizations to deal with military involvement in homeland security.

Post-September 11, the military performed well. The DoD provided increased air defense patrols and physical security at airports, ports, and critical infrastructure sites, increased support to the Coast Guard, and temporarily increased support to other federal agencies and first responders in what became known as Operation *Noble Eagle*.

Over the past two years, DoD has taken major steps to develop policies, doctrine and organizational capabilities to more actively support homeland security. DoD created the position of Assistant Secretary of Defense for Homeland Security. The Services created a range of organizations to support better homeland security.

The most important action to enhance military support to homeland security was the creation of a new unified combatant command, U.S. Northern Command (NORTHCOM) to consolidate homeland security missions previously dispersed among other military organizations. Its mission was “defending the United States and supporting the full range of military assistance to civil authorities.” NORTHCOM’s role is still ill-defined. It did not assume new missions but simply took over some already being performed by the U.S. military, in part to avoid criticism over an increased military role in domestic security. NORTHCOM plans, organizes and executes homeland security missions, but has few assigned forces.

The future contribution of the military to homeland security depends on how aggressively DoD, the Services and NORTHCOM take their charter to support the overall national effort. DoD needs to examine the future role of the National Guard in homeland security. NORTHCOM has not moved very aggressively to define its role and identify its requirements for capabilities.

Initial steps: Grade A. Important steps toward augmenting the effectiveness of the military in homeland security were underway before September 11. DoD and the military have continued, escalated and expanded this process. In general, the military is significantly better prepared for homeland security today than it was on September 10, 2001. DoD has been able to shift its focus from exclusively external enemies to a balance between external and homeland security.

Long-term Prospects: Grade A. Shifting the focus of DoD and the U.S. military is difficult in that the military is by nature cautious and cumbersome. Since September 11, 2001 it has been heavily engaged in the war on terrorism, other external missions and internal transformation. Given this, expectations for how much DoD and the military could have shifted over the past year and a half must be kept in check.

Public Awareness and Crisis Communications

September 11 and the anthrax attacks of that same year proved to be important learning experiences for all levels of government with respect to crisis communications. From those experiences came recognition of the need not only for continuous public education on homeland security issues, but also for clear and continuous public communications during a crisis. Governments also learned that if they were going to communicate with the public they required the means for rapid situation assessment, information sharing and decision making.

Over the past two years, the administration has made great strides in its public education efforts and its handling of crisis communications. Responsibilities were assigned within the federal government for communications and public awareness. Governor Ridge played a lead role, first as the Director of the Office of Homeland Security at the White House, and second as Secretary of the Department of Homeland Security. The other leading spokesman was Attorney General John Ashcroft. These improvements have been well demonstrated in recent crises such as the Northeastern power failure.

Six months after the attacks, the administration created its Homeland Security Advisory System. This system was intended “to create a common vocabulary, context and structure for an ongoing national discussion about the nature of the threats that confront the homeland and the appropriate measures that should be taken in response.” The administration’s oft-maligned color-code system to indicate the level of terrorist threat facing the homeland, while imperfect, does provide a simple way of communicating basic information.

Over time, as the demands of homeland security become more complex, an intensified public awareness and education campaign will be necessary in order to make the public more conversant with the measures that they can take to make themselves and their nation more secure. In addition, the administration must consider how it will provide the necessary crisis communication should a major terrorist incident occur. Experts argue that only a carefully planned and constructed system, one that is well exercised, will surmount the inevitable confusion of a major terrorist attack.

Initial steps: Grade B+. Despite frequent ridicule, the color-coded threat conditions of the Homeland Security Advisory System are an effective way of communicating the prevailing degree of danger to mass audiences.

Long-term Prospects: Grade C+. The Bush Administration may have underestimated the difficulty of getting the process and product right. Aside from the obvious difficulty of explaining danger without reinforcing fear, fragmented authority, bureaucratic rivalries and legitimate differences of opinion among policymakers impeded the administration’s early efforts. The administration has not sought the active participation of most citizens in counter-terror efforts.

The Way Forward

If one were to assign grades for the administration's initial efforts to secure the homeland, it would be an "A-." Overall, across all functional areas, there was consensus among the experts that the Bush Administration has taken a proactive approach to try and make this nation safer since September 11. That news is encouraging. Unfortunately, the administration has shown spottier competence and preparation for the long-term.

In assessing the way forward and developing an action agenda to support long-term progress in homeland security, this report draws on ideas from many sources, but particularly from the subject experts who contributed to this Lexington Institute study. More detailed discussions of many of these recommendations can be found in the published versions of these special studies available on the Lexington Institute website.

Directly after September 11, the administration had the "advantage" of a set of known deficiencies, where it was possible to react with knee-jerk speed without having a real strategy. There are still more holes to fill. Further significant improvements to ground transportation, including detecting chemical and biological attacks, would likely cost billions. In terms of border security, there is still a major ingenuity/technology gap that needs to be closed. The Intelligence Community needs more money, training and personnel in the future. In addition to the need to hire more language-capable officers, the issue of who is responsible for warning needs to be resolved, and authority needs to be further streamlined and centralized.

After what must be judged a good initial response to September 11, the Bush Administration merits no better than a "C+" for its efforts to develop a long-term strategy and program for the enhancement of homeland security. It remains to be seen whether the nation is going to invest the sustained effort necessary to deal with the real and possibly growing threat of terrorism or whether the nation is going to treat September 11 as a "one-shot" deal, and remain content with improved, but not comprehensive, homeland security.

One oft-heard criticism of the DHS and NORTHCOM is that they both have a short-term perspective. This is of particular concern when it comes to planning the long-term investments in capabilities and science and technology necessary to address the more difficult aspects of the homeland security problem. Although it is beset with a myriad of near-term demands and challenges, the DHS and the administration as a whole must focus serious attention on the long-term plan for homeland security.

A long-term strategy for homeland security has not been clearly defined. Creating a strategy for homeland security beyond filling obvious holes is complicated by the fact that homeland security does not consist of one single program. Homeland security is a loosely-defined concept, representing a wide spectrum of functional areas such as border security, air transportation security, cyber security, etc. Each functional area, in turn, is comprised of numerous, sometimes competing behaviors and activities. However, months removed from the fear that energized and spurred the government's

actions, it is necessary to take stock of the allocation of finite resources – money, people, technology, etc. Hard choices need to be made and the administration requires a strategy to make those choices.

Furthermore, contrary to popular belief, it is not the administration alone that bears the onus of formulating a strategy. There is a need to resolve the issue of which areas of homeland security fall under the responsibility of the government to implement (and pay for), and which fall under the responsibility of the private sector. In his evaluation of public education and the media, an often-overlooked area of homeland security, Dr. Loren Thompson, Chief Operating Officer of the Lexington Institute, notes that in general, the administration has not sought the active participation of most citizens in counter-terror efforts. Instead, it has asked for public support and patience while specialists carry out the various missions associated with securing the homeland. Until the issues of strategy and public-private responsibility are firmly resolved, the public will be left as passive observers, with an uncertain illusion of progress.

The public-private responsibility issue permeates many functional areas. In addition to making the case that the nation may be much less vulnerable to cyber attack than has been suggested in most public analyses, Dr. Martin Libicki, senior policy analyst for RAND, suggests that a set of limited measures, largely in the hands of the private sector, could be sufficient to provide robust protection. Dr. Joseph Barbera, Co-Director of the George Washington University Institute for Crisis, Disaster, and Risk Management, emphasizes the importance of preparing to manage those incidents of catastrophic terrorism that cannot be prevented (including attacks by weapons of mass destruction), and states that while there must be an urgency to prepare for terrorism at the national level, successful response and incident management requires effective local capability and capacity in the affected jurisdictions. Similarly, responsibility for the security of surface transportation rests with state and local law enforcement authorities and the public and private entities that own and operate the transportation infrastructure and assets. Private industry owns between 85-90% of the assets vital to national operations and well-being. Michael Scardaville, Policy Analyst with The Heritage Foundation, concludes that robust critical infrastructure security programs involve “actors both in and out of government.” “The extent to which business and industry are able to assist each others’ infrastructure protection policies,” he states, “is likely to prove one of the most central determinants of whether or not critical infrastructure protection efforts are succeeding.”

Americans need to accept the fact that there is no such thing as invulnerability to attack. Long-term strategies for homeland security must reflect that sober reality. Frank Hoffman, Consultant with EDO Professional Services, notes that even with increased screening efforts, our borders cannot be made impenetrable. With some 90,000 miles of coastline, 5,000 miles of intercoastal waterways, and 9,000 miles of land borders designed to facilitate travel and trade, access into America is almost limitless. Ground transportation suffers from twin inherent vulnerabilities of easy access to facilities and high passenger volume. Similarly, given the hundreds of airports, thousands of planes, tens of thousands of daily flights and limitless ways terrorists can attack, loopholes

remain in cargo, mail, onboard and perimeter security. As former Chief Executive Officer of El Al Joel Feldschuh stated, “the only way to completely prevent aviation terror is by banning air transportation altogether.” Feldschuh points to intelligence failures, not failures in air security, as the ultimate precursors to September 11, while Dr. Ellen Laipson, Chief Executive Officer of the Henry L. Stimson Center, stated that “even with maximum information flow, intelligence sharing and smart interagency coordination, highly motivated and well-trained operatives would have been able, and are still able, to conduct attacks on the United States.”

The theme reflects a simple reality. That is, even with the best intelligence, whether across the borders, in the air or on the ground, the public needs to realize that some attacks are going to get through. Such analyses indicate that as we struggle to define good metrics for success in homeland security, we cannot limit ourselves to deterrence and prevention of attacks as the only measures of success. Even the Israelis, who represent the gold standard for extent of security measures, cannot foil all attacks. Analysis of our own security efforts must therefore be tempered with lowered expectations in terms of prevention. Instead, the measure of success needs to be in the ability to minimize both casualties and disruption in operations following instances of catastrophic terrorism.

Unfortunately, the ability to minimize casualties and disruption was found to be one of the weakest areas of homeland security. This is in part because most threats of major concern, such as chemicals, radiation and biological agents are complex and have not been currently experienced during the modern medical era; but mostly because adequate preparation depends upon coordinated actions of everyday medical and public health personnel. Public health and acute-care medicine encompass very diverse resources, which are widely separated in management methods, goals, funding and preparedness. While there must be an urgency to prepare for terrorism at the national level, successful response and incident management requires effective local capability and capacity in the affected jurisdictions. “What is needed,” Dr. Barbera states, “is truly interdisciplinary, all-hazard, one-system planning and preparedness, which will only happen through effective federal guidance, with accompanying, carefully presented templates and funding initially proffered by the federal government.” It is not clear that such organization, a strong national guide overseeing local public efforts, is in place.

Dr. Barbera argues that this is not an area that can be improved simply by throwing money at the problem or hiring more personnel. In his analysis, he notes the fact that this nation is not yet adequately prepared for the catastrophic impact of more common hazards (i.e., a massive earthquake in a densely populated area of California), let alone WMD. Recent events such as the anthrax dissemination attack in 2001 and attempts to implement a national smallpox preparedness program are further examples of the inadequate state of public health preparedness. “One cannot fault the earnestness of the health and medical preparedness effort, or the intensity of both the federal and overall national effort itself,” he states. “But much in the past has been misguided, redundant, and has left very large preparedness gaps uncovered.”

The need for strong federal leadership was echoed in critiques of several other functional areas. In creating the DHS, Washington sought to close obvious gaps in homeland security caused by the distribution of responsibilities among dozens of Cabinet departments and government agencies. However, the historically fragmented nature of the U.S. government's organizational capabilities, combined with the reluctance of the private sector to participate, has made it difficult to focus on cohesive strategies. Dr. David Kay, former U.N. Special Commission chief nuclear weapons inspector, was pessimistic in his assessment of defense against nuclear attack, stating "...in the area of the preparation of the medical response, and post-attack decontamination, don't ask who in government is responsible for it (because) you're going to have a hard time finding anyone who will step up and take that." Dr. Laipson echoed that theme in her assessment of foreign intelligence, stating that "the tendency to compromise or to partly empower many different agencies to manage a piece of the terrorism problem will undermine the goal of achieving more synergy and smarter integration of the great human and technical power we possess."

Michael Moodie, President of the Chemical and Biological Arms Control Institute, offered a more positive assessment of the government's efforts in preparing for chemical or biological defense. "The use of the nerve gas Sarin by the Aum Shinrikyo in the Tokyo subway in March 1995 had awakened some policy makers to the potential interest of non-state actors in obtaining and using such capabilities," he stated. "But it was only after the tragic events of September 11 and the subsequent anthrax experience that fighting violence at home that could exploit chemical and biological weapons became a national priority." However, he acknowledged the inherent difficulties in adequately addressing prevention, preparedness, consequence management and mitigation. Ultimately, he concluded, "the major issue for the future will be whether the Congress and the administration will sustain the commitment to meet critical requirements and express that commitment in adequate levels of funding to get the job done."

An Action Agenda

One thing on which virtually all experts in this area can agree is that the level of funding for homeland security is grossly inadequate. But simply increasing the amount of money for homeland security is not a solution. The task is so vast that virtually any amount would be insufficient to address the myriad of problems, at least not in the near-term. It is difficult for the federal government to conduct adequate oversight over existing problems and disbursements.

More important in the long-term than increasing the amount of money available for homeland security is for the government to define a clear rationale for how it will allocate available resources. Such a rationale must be based on a comprehensive strategy and this strategy requires a system for setting priorities. As yet, neither the DHS nor any part of the federal government has developed such a system. In order to avoid wasteful expenditures and ensure continuing public support for the homeland security enterprise, it

is imperative that the DHS move rapidly to complete the various assessments and analyses that will lead to a system for prioritizing resource expenditures.

As part of a national strategy, the DHS must aggressively pursue its current efforts to create an effective and efficient regional structure that harnesses the potential synergies of adjoining states. In addition, it is appropriate to contemplate a national transportation security strategy. Creating one would require identifying and ranking overall objectives: preventing the loss of life; minimizing long-term risks to health; limiting social upheaval, environmental catastrophe, and economic disruption.

In the area of border security the DHS should expand current efforts to push the security perimeter outward from U.S. shores. Frank Hoffman argued that the United States should and is encouraging its partners, trading partners and industry, via tools such as tax credits and “fast pass” benefits, to a) enhance security at overseas loading docks, ports and warehouses, b) conduct background checks on shipping personnel and crews, and c) establish an automated database to identify and track shipping throughout the entire transit pipeline and provide updated manifests before entry.

There are still several issues to be addressed in aviation security. Screening of cargo and mail needs to be as thorough as passenger screening has become. The TSA should develop a comprehensive air cargo security program that includes identity checks of individuals making cargo deliveries, a computerized cargo profiling system and cargo-screening facilities. A program for appropriate basic and recurrent training for screeners and flight attendants needs to be initiated. Sufficient funds need to be allocated to provide air marshals on more flights. Airport and airline employees need to be screened.

Funding for public health and medical preparedness, training, equipment purchases and other activities must be refocused so that it is dispensed only for resources that fit within the defined systems. The current “training” glut has been relatively useless. Templates are possibly the only viable way to rapidly move local and state preparedness and response capability forward in appropriate directions, and so should be carefully considered by federal health and medical authorities. MMRS is an excellent start on templates, and has promoted the beginnings of integration between acute medical care, public health and public safety agencies.

Mass casualty terrorism will be an enduring threat. Preparing to meet that threat must become and remain real, and be assimilated into the all-hazard funding for disaster preparedness at the local level. Federal, state, and local authorities need to share expenses for mass terrorism health and medical consequence management. Such investments should be based on the idea that there is now a permanently expanded public safety requirement for protecting American families.

The Bush Administration needs to take seriously the dangers from the potential misuses of biosciences. Clearly, first among these is the potential for bioterrorism. But there are additional problems such as the inadvertent development of dangerous pathogens or the unregulated intermixing of genetically-modified with non-modified

foodstuffs. The technology to modify organisms is decades-old and has proliferated to every corner of the globe. The ability to manipulate DNA is rapidly spreading around the world. It is important to assess the potential dangers and take steps to address them while, at the same time, not stifling the innovation in the biological and life sciences that has produced so much benefit for humanity. The administration needs to mount a national effort involving the Intelligence Community, the pharmaceutical and biotechnology industries, academia, DoD and other relevant government agencies to assess the full range of potential bioscience-based threats to national security.

The administration should initiate a “National Dialogue” on bioterrorism preparedness with special emphasis on engaging the private health care sector. Such a dialogue would serve to define expectations of both the government and the private sector, clarify respective roles and responsibilities, foster stronger personal working relationships in a situation in which lack of familiarity continues to be an issue and move the action agenda forward. Such a dialogue might have precluded the public response to the administration’s smallpox vaccination plan.

The most important task in the area of intelligence, both domestic and foreign, is to foster a change in the cultures of the individual agencies. Continuing effort will be required to improve communications systems and allow for the sharing of information data resident in numerous databases. It is more important still to ensure that the pre-September 11 culture of separate intelligence “stovepipes” is ended.

The rapidly changing terrorist threat environment poses a particular challenge to the traditional working style of the Intelligence Community. To accomplish this, the Intelligence Community must dismantle the bloated bureaucracies of the large agencies and retool most employees to contribute more directly to the intelligence mission. Priority must be given to a workforce whose productivity is measured currently in terms of output. This must change to permit more useful processing of data and creation of more analytic products.

The administration must pay close attention to the operation of the Terrorist Threat Integration Center. It must ensure clear lines of responsibility for threat reporting. It must demand that the TTIC operate as the clearinghouse for intelligence information without the traditional agency biases. Finally, there needs to be consideration given on policies and procedures that allow for the maximum declassification of intelligence in order to make it useful to state and local officials.

With some 40,000 potential targets to consider, critical infrastructure protection poses a daunting challenge to the new Department of Homeland Security. The DHS is conducting the threat and vulnerability studies and the industry sector assessments that will underpin the development of prioritized plans. It is vitally important that this process be completed as soon as possible. Without the capacity to identify the subset of all critical infrastructure that must be protected, all claims for resources and attention in this area are equally valid. Moreover, it is as likely as not that resources expended will be wasted.

Neither the federal government nor industry alone can fully secure national infrastructures from attack. In order to achieve a collaborative relationship, the DHS needs to create an environment where government and industry freely share information related to threats, protection/deterrence measures, consequence mitigation and reconstitution efforts. Industry and government also need to work together to define concepts and measures of merit for the protection of critical infrastructure.

Cyber security may be the one part of the overall homeland security portfolio where less is more. Despite almost a decade of dire predictions, there is almost no evidence that cyber terrorism has occurred. Malicious attacks, hacking and interference with networks are commonplace. But the deliberate attacks on critical computer systems designed to cause a serious terrorist incident have not happened. This suggests that such attacks may be harder to conduct than we thought.

Most of the cyber infrastructure is in private hands. In addition, effective countermeasures to malicious or terrorist attacks are available on the open market. Therefore, the responsibility for cyber security should reside largely with the private sector and individual citizens. The federal government should be responsible for the systems that it controls and operates. If the government wishes to create incentives for industry to pay attention to securing computer systems and networks, it could establish as a matter of law and expectations a regime of strict liability that creates consequences for those who fail to protect their own systems, resulting in harm to third parties. A recent National Academy of Sciences report advocated a regime of liability for software makers.

The Department of Defense has done much to improve its ability to respond to the terrorist threat to the U.S. homeland. More remains to be done. Two issues need to be addressed. The first is the contribution of NORTHCOM to homeland security. This command is responsible not only for military support to civil authorities but for the protection of North America against attack. At this point in time, NORTHCOM is notable for its lack of effort to shape policy and programs for homeland security. The second issue is the role of the National Guard in homeland security. DoD needs to define the missions of the National Guard in homeland security and, if necessary, pursue its reorganization to facilitate those new missions.

The ability to deal with threats to the homeland will depend to a considerable degree on the ability to communicate. This means getting the right information to the right people at the right time. Effective communication is a pre-requisite for effective security. The current information infrastructure has some serious weaknesses that must be addressed. The system for communicating threat information needs to be enhanced. This involves both a sustained public information campaign regarding possible threats and how to deal with them and also a crisis communications system in the event of an actual attack.

Concluding Observations

As we look toward the long-term future the grade for the moment must be considered “incomplete” in the following sense: If we think that indeed, the problem is going to be with us for a long time and is going to characterize the age – that is, the problem of rogue-state and/or non-state-based terrorism, including those with weapons of mass destruction - then in fact we have not moved far enough in a variety of directions. We are not at the point of thinking about an integrated strategy that is, for the purpose of protecting Americans, seamless from the Special Forces overseas doing the operations, to the CIA special ops, to the intelligence personnel and all the way down to the first responders. That will be necessary if in fact this is going to be the “problem of the age.” In truth, such an approach is no different than the whole array of activities that the United States undertook when fighting the Cold War; a massive, integrated system. If this nation is going to invest the necessary effort in such a system, it will be under the presumption that this threat is real, perhaps even growing, and that this threat is going to be with us for the long haul.

However, if it is the administration’s opinion that this war is an isolated affair, where rogue states may exist, but no catastrophic collapse of order in the world will occur, then in fact the administration may not need to go much further. Unfortunately, we don’t know that yet, and perhaps we won’t know that for several years. Events in Southwest and Northeast Asia over this next year may indicate whether it is going to be a safer environment, generically speaking, or an unsafe environment.

This complex situation was reflected in the assessments by the Lexington team of experts. In general, most reviewers had a similar appreciation of the state of homeland security. In the past twenty-four months, good work has been done. Progress has been made on many fronts. However, these were the easy steps. In the future, changes need to be made. First there needs to be a comprehensive strategy for homeland security. Second, the administration must establish a credible and transparent process to evaluate threats and vulnerabilities. This process is absolutely necessary in order to make the maximum beneficial use of scarce resources. Third, priorities need to be established. Finally, there needs to be a means of matching efforts to protect the homeland with the ongoing global war on terror. In the end, however, even if all these steps are taken, the nation needs to recognize that it can never be one hundred percent secure from attack. That era is over.

The Lexington Institute
1600 Wilson Boulevard, Suite 900
Arlington, Virginia 22209

Phone: 703-522-5828

Fax: 703-522-5837

www.lexingtoninstitute.org