

PREFACE: ONE YEAR ON

Since the attacks of September 11, 2001, a good deal has been done to improve the safety of Americans, not only in the offensive war on terror abroad but in protecting the homeland as well. Now aware of the harm terrorists can inflict, Americans are on alert, providing a first, crucial line of defense. Air travel is much safer. Intelligence sharing has improved, especially information about specific individuals suspected of ties to terrorism. Measures have been taken to ensure that suspicious ships entering U.S. waters are screened more frequently. Some early steps, with more to follow, have been taken to reduce the country's exposure to biological attacks, and oversight has been tightened on labs working with biological materials. Terrorism insurance is now backstopped by a new federal program. Certain types of major infrastructure, such as well-known bridges and tunnels and nuclear reactors, are protected by police and National Guard forces when terrorism alerts suggest that such measures are necessary.

But much, much more remains to be done. Most of the above steps reflect a response to the past tactics of al-Qaida and do not anticipate possible future means by which that organization or other terrorist groups might try to harm Americans. Moreover,

most of those steps were taken in the immediate aftermath of September 11. In 2002 the country lost a good deal of momentum on improving homeland security. The primary focus of Washington policymakers in 2002—creation of a Department of Homeland Security (DHS)—may have some merit, although we believe the department to be larger and more complex than desirable or necessary. But the department will not in and of itself make Americans safer. To the contrary, the complexity of merging so many disparate agencies threatens to distract from other, more urgent security efforts. Furthermore, excessive focus on organizational matters during the past year and broader battles over fiscal policy impeded adequate funding for homeland security issues. The budget for 2003 was delayed for several months, losing valuable time for buttressing our national defenses against terrorist attacks. In addition, President Bush vetoed several specific (and relatively cost-effective) measures proposed by Congress that would have addressed critical national vulnerabilities. As a result, the country remains more vulnerable than it should be today, and on the eve of a likely war against Iraq that could inspire more terrorist attacks. In all, we have squandered precious time bought by the disruption of al-Qaida in Operation Enduring Freedom that should have been used to prepare ourselves against the next major strike.¹

A major unmet agenda for homeland security must be addressed in 2003. New organizations, and in particular the new Department of Homeland Security, must be built. Primary initial focus should be placed on those elements of the department addressing border security, on intelligence, and on the federal government's interactions with state, local, and private actors in their efforts to improve the country's safety.

But policymakers must avoid the temptation to declare victory with the creation of a new bureaucracy alone. More important—and far more urgent—is filling the gaps that remain in the current homeland security effort. These range from creation of a new networked intelligence capability that tries to anticipate and prevent future terrorist actions, to greater protections for private infrastructure like chemical plants and skyscrapers, to a much stronger Coast Guard and Customs service (within DHS). They also include obvious steps that should have been taken soon after the 9/11 tragedy but were not—such as making sure first responders can communicate over commonly accessible radio networks during emergencies, hastening

development of port security plans, and improving security of transportation networks aside from airports.²

As we argued in the original edition of this book (generously supported by the MacArthur Foundation), it is impossible to stop every potential type of terrorist violence. But by focusing on preventing attacks that can cause large numbers of casualties, massive economic or societal disruption, or severe political harm to the nation, the United States can approach the homeland security problem systematically and with a better chance of preventing future attacks on the scale of the 9/11 tragedy. That will take more attention from Congress and the administration. It will also take more money—perhaps \$10 billion a year (less than 3 percent of the defense budget) above what the administration proposes to spend in 2004, making for a total federal homeland security budget of about \$50 billion a year.

Strategy and Priorities

Homeland security is daunting in its complexity and in the sheer number of potential targets against which attack might be contemplated in an open country of nearly 300 million people. As such, it requires a conceptual foundation and a set of priorities, if efforts are not to degenerate into a scatter-shot set of activities that leave many gaps and fail to make good use of available resources.

Recognizing as much, the Bush administration put forth a strategy for homeland security on July 16, 2002.³ It was somewhat illogical that the strategy should be produced more than a month after the administration proposed a new Department of Homeland Security, since the organization of a department should presumably be based on a clear sense of what it needs to accomplish. But as a practical matter, the strategy and the department were designed largely in tandem, mitigating the downsides of this backward approach.

The administration's strategy document recognizes that terrorists are themselves strategic, adaptive actors who will pursue new modes of attack and new weaponry. The administration's strategy makes particular reference to the further danger that terrorists will seek or obtain weapons of mass destruction. It emphasizes the necessary roles played by state and local governments as well as the private sector and individual citizens; indeed,

according to administration estimates, all of the latter collectively outspend the federal government on homeland security efforts today (total national spending is about \$100 billion a year, of which the federal share is about \$35 billion).

The administration's strategy is similar in many ways to what we proposed in this book's first edition in April 2002. We suggested a four-tier approach to preventing terrorism in general, and catastrophic terrorism in particular: protect the country's borders; prevent attacks here at home by pursuing terrorists in the United States preemptively and keeping dangerous materials from them; protect key assets and population centers here at home as a final line of defense; and mitigate the results of any attacks that occur despite our efforts. In short, our four-layered approach emphasizes border protection, domestic prevention, domestic protection, and consequence management.

The Bush administration proposes a six-tier approach, involving six "critical mission areas." The first is intelligence and warning, followed by border and transportation security, domestic counterterrorism, protecting critical infrastructures and key assets, defending against catastrophic threats, and emergency preparedness and response. The administration also proposed four key methods or "foundations" for enhancing all six tiers of defense: law, science and technology, information sharing and systems, and international cooperation. One can always quibble with specifics; for example, the Bush administration's critical mission area of intelligence and warning seems more of a foundation or method than a separate tier of defense. But the taxonomy serves its main purposes well.

Moving from the general and conceptual to the detailed and specific, the administration's strategy then highlights a handful of key activities. Within the mission area of intelligence and warning, for example, it advocates enhancing the analytic capabilities of the FBI, building a new information analysis unit within the Department of Homeland Security, and employing "red team" techniques to anticipate likely future avenues of terrorist attack. Within border and transportation security, the most notable priorities are to create "smart borders," increase the security of international container shipping, implement the Aviation and Transportation Security Act of 2001, "recapitalize" the Coast Guard fleet with newer vessels and technologies, and reform immigration services.

Domestic counterterrorism efforts include improving intergovernmental law enforcement cooperation, reorienting the FBI to focus on counterterrorism, pursuing terrorist financing, and tracking foreign terrorists. Infrastructure protection involves improving partnerships with state and local actors and the private sector, developing an infrastructure protection master plan, and securing cyberspace. Defending against catastrophic terrorism emphasizes greater use of nuclear radiation detectors as well as chemical and biological detectors, improved chemical decontamination techniques, and development of better vaccines and medications. Finally, emergency preparedness emphasizes communications and training and equipment for first responders as well as greater preparations for health care services needed to respond to any attack.

The administration's strategy and corresponding budgetary and programmatic initiatives to date have produced a number of important accomplishments in the effort to make the nation more secure against terrorism. A National Joint Terrorism Task Force, working with local task forces in every state, has been created. An improved FBI database has led to hundreds of arrests in the United States. The Student Exchange Visitor Information System enables universities to transmit data about their students electronically to the government, reducing the chances that individuals with no intention of studying will be able to enter the country and remain in the country on student visas. A new database is being created to track the entry and exit of all visitors to the United States. Airplane and airport security is clearly much better, including the addition of thousands more air marshals, reinforced cockpit doors, and comprehensive baggage screening. Smallpox vaccine has been procured for all American citizens; twenty million doses of antibiotics are available in the event of another anthrax attack. Research funding for new vaccines and antidotes to various types of biological attacks has been increased threefold. Several hundred million dollars in added research funding are available to develop better detectors for nuclear materials and biological agents, better means of using biometric indicators to verify the identities of individuals, and improved technologies for first responders at the state and local levels.⁴

But the administration's strategy leaves out several key priorities for action that we strongly advocated in early 2002 and continue to believe important. They can be organized into four broad categories. One concerns

major infrastructure in the private sector, which the Bush administration largely ignores. A second concerns information technology (IT) and its proper uses; despite rhetoric about using information technology aggressively to promote homeland security, the Bush administration budgets and program activities to date do not match the rhetoric. A third concerns the presently unrecognized need to greatly expand certain specific capacities for homeland security such as the Coast Guard and Customs, as well as security for forms of transportation such as trains. A final concern relates to intelligence, where the administration has taken smart initial steps to bring together the efforts and terrorism databases of various agencies, but at present has not done enough to anticipate the possible next actions of terrorists.

Regarding the private sector, the Bush administration is too willing to take a free-market approach. But the business of business is business, not homeland security. It is therefore not surprising that, for example, the chemical and trucking industries have not moved adequately on their own to improve safety, leaving their assets vulnerable to theft or sabotage. In regard to information technology, the administration still has no plan for quickly improving real-time information sharing not only in the national law enforcement community, but also among the broader set of public and private actors who are vital to preventing and responding to homeland attacks. And its investments to improve information sharing throughout the government at all levels fall woefully short of what is needed. Finally, while it plans to modernize the Coast Guard and adopt a new approach to Customs, it does not recognize the need to increase the overall size and capacity of these organizations. The former was already undersized for a wide variety of missions it performed before 9/11; since then, homeland security imperatives first demanded more than half its fleet and continue to employ perhaps a quarter of it. The latter still only inspects less than 5 percent of all cargo entering the country, even if it has become savvier about which small percentage to examine.

These flaws are also reflected in more concrete terms—most notably in insufficient funds for certain agencies and activities. For that reason, it makes sense to turn next to a more specific assessment of the homeland security programs that the Bush administration has advocated to date and flesh out these omissions in its initial efforts. Following that section, we address two other major issues that have been at the center of policy debates

since our book was released—the creation of the Department of Homeland Security and proposals for fashioning a new domestic intelligence unit within or outside that department. The first challenge is just beginning, since the task is not solved by putting up new signs on a building and choosing a secretary of DHS and declaring the subject over. The second remains at an even earlier stage of conceptualization and implementation.

Programs and Budgets

In February 2002 the Bush administration released a homeland security funding proposal for 2003 that would have roughly doubled spending relative to pre–September 11 levels (see table 1). That proposal was formed in the four months after the September 11 and anthrax attacks and emphasized four main efforts: support to first responders, defenses against bioterrorism, improved border security, and improved airport and airline security.⁵ It was a reasonable first response. But quite naturally, it had major gaps. And those gaps have persisted in the administration's proposal for its 2004 budget.

During the second half of 2002, the debate over the Department of Homeland Security diverted the attention of policymakers and the public from directly addressing the nation's underlying vulnerabilities to terrorist attack. Meanwhile, in late 2002, battles over the federal budget more generally disrupted funding for homeland security initiatives ranging from equipping first responders to improving information technologies and developing vaccines against potential bioterrorist threats. For example, only about \$750 million in federal funds apparently was directed to the nation's three million first responders in 2002 for training and equipment for responding to terrorist attacks, when the administration had promised \$3.5 billion. The 2002 level works out to an average of \$2.50 per first responder nationwide—though, in fact, funds only reached 80,000 first responders, or less than 3 percent of the total.⁶ It is deeply disturbing that Congress and the executive branch allowed their disputes over broader fiscal policy to interfere with what is probably the nation's top urgent priority, protecting itself against further terrorist action. In addition to the budget disputes, insufficient progress was made in regulating the private sector, with little or no action taken by the government to improve security at large buildings, chemical facilities, and other potential targets. The bottom line is

Table 1. *Homeland Security Funding by Department*

Millions of dollars of budget authority

<i>Agency</i>	<i>2002 level</i>	<i>2004 request</i>
Department of		
Agriculture	230	390
Commerce	99	153
Defense	4,423	6,714
Energy	1,067	1,361
Health and Human Services	433	3,776
Homeland Security	11,398	23,890
Justice	1,019	2,290
State	438	811
Treasury	84	91
Transportation	635	284
Veterans' Affairs	47	145
Army Corps of Engineers	...	104
Environmental Protection Agency	13	124
Social Security Administration	113	147
National Aeronautics and Space Administration	114	170
National Science Foundation	240	307
Other agencies	267	590
Total	20,620	41,347

Source: Office of Management and Budget, *Fiscal Year 2004 Budget of the U.S. Government* (February 2003), p. 315.

Notes: The Department of Homeland Security did not exist in 2002; the totals shown for that department in 2002 are for the homeland security functions of those agencies ultimately incorporated within it. Functions of the various departments and agencies not pertaining to homeland security are not shown. Of the 2004 totals, \$3.497 billion is to be recouped by user fees (for visa processing, airport security, and the like). Another \$2.897 billion is considered mandatory spending for activities such as immigration enforcement and border protection. Subtracting Defense's funding levels as well leaves a total discretionary budget of \$28.239 billion for the net nonmilitary discretionary elements of homeland security.

The 2002 supplemental budget included \$11.531 billion in non-Defense funding and \$733 million in Defense funding, for a grand total of \$12.264 billion in additional funds.

that the nation did not make as much progress as it should have in improving homeland security during 2002.

The Federal Budget

Various funding problems impeded homeland security efforts in late 2002. The federal government finances homeland security almost entirely within

the discretionary spending component of the budget; such discretionary spending is determined in a set of thirteen annual appropriations bills. Battles over the size and shape of the budget meant that as of December 2002, only two of the thirteen bills that fund the government had been enacted for the fiscal year that runs from October 2002 to September 2003. The rest of the government was financed through a series of “continuing resolutions,” a type of stop-gap measure that basically rolls over funding from the previous year into the current one. This approach, by its very nature, gives short shrift to new initiatives and it threatens to disrupt funding for many crucial homeland security programs. The stop-gap measures continued through late February 2003, when the rest of the discretionary appropriations bills for 2003 were enacted.

In the meantime, the disruption in funding associated with the continuing resolutions forced the Department of Energy’s National Nuclear Security Administration to freeze hiring and the Transportation Security Agency to withhold \$20 million in grants for truck security.⁷ Rep. David Obey (D-Wis.) argued that the continuing resolutions financed activities against bioterrorism at \$2.3 billion less than the administration’s budget suggested was necessary, and financed first responder programs at \$2.5 billion less than the administration’s budget called for.⁸

Even following enactment of the 2003 budget in February, two problems remain.

First, the design of the federal budget has not been updated to reflect the emergence of homeland security as a priority for policymakers. “Homeland security” funding is spread across myriad budget items. (It took several weeks following the ultimate passage of the 2003 budget for analysts to even calculate the total spending for homeland security.) Until now specific homeland security items have not been evaluated as part of an overall homeland security package, but rather in the context of the other non-homeland security items. Fortunately, the House and Senate have now agreed, as per our earlier recommendation, to create separate subcommittees for homeland security of their appropriation committees.⁹ This will ensure that the debate over homeland security funding is not unnecessarily complicated by having too many subcommittees share responsibility for a single mission.

Second, the overall funding level for homeland security in the 2003 appropriations legislation enacted in February is lower than we believe

necessary. Even the administration has admitted that the enacted 2003 levels are inadequate, noting, for example, that the 2003 bills provide only \$1.3 billion for first responders.¹⁰ The problem deserves immediate attention, and the administration itself is at least partially to blame. Looking forward, the administration has requested \$41 billion for homeland security in 2004.

Since our analysis last year, moreover, additional national vulnerabilities have become evident, such as the possibility that civilian airliners could be attacked by small man-portable surface-to-air missiles. Moreover, most foreign airliners flying into the United States do not benefit from the special safety precautions adopted in this country since 9/11, meaning that they could be hijacked as they enter American airspace or bombed with Americans aboard. Simply dealing with these air safety problems could require \$10 billion to \$20 billion in additional spending, averaging out to \$1 billion to \$2 billion a year over a decade. (Countermeasures against missile attack can cost \$3 million per plane, for example, and the country has thousands of commercial aircraft that could require protection.) Given al-Qaida's fascination with aircraft, such vulnerabilities probably should be addressed; given the state of airline finances, if such expenses are to be incurred the government will probably have to foot the bill (although the costs still could—and ultimately should—be borne by airline passengers, by imposing a user fee or by raising the airline ticket tax). Trains are another area of mediocre security; there is virtually no screening of passengers or luggage on the nation's trains, and many tunnels remain unhardened against bombing. A cursory review of these types of vulnerabilities suggests that \$50 billion is a more accurate rough estimate of the necessary level of federal funding for homeland security in the years ahead.

The administration's lower funding also manifests itself in areas such as information technology, where the Office of Management and Budget has temporarily frozen spending for developing new systems or modernizing old ones.¹¹ A freeze may be temporarily necessary to ensure that interagency communications problems are not exacerbated, but upgrading existing information technology systems to ensure better interoffice data sharing and compatibility is clearly going to be an expensive undertaking. The administration's budget simply does not recognize this fact, endangering progress in this crucial area. As we emphasized in the initial edition of our

volume, information technology should represent perhaps the highest priority for homeland security efforts. Conversations with homeland security IT specialists suggest that the lack of funding is crimping efforts to modernize IT systems. The proposed increase in federal funding for IT related to information security for 2004 amounts to just \$300 million—roughly what a major university might spend in a year on its computers and related assets.

Another example of inadequate funding involves port security. As one illustration of the problem, the Customs Service has created the Container Security Initiative, a program to screen containers at foreign ports before they are loaded onto ships. Such a program is extremely promising, since it “pushes the border back” to the foreign port and thereby keeps potential threats away from our shores. Yet the administration’s fiscal year 2003 budget included no additional funding for this initiative. The fiscal year 2004 budget does propose some resources (\$62 million),¹² but they are an order of magnitude too little to adequately finance the program, given its substantial potential benefits. Similarly, Congress recently passed legislation to improve security at the nation’s own ports. Yet the legislation did not provide funding to implement its requirements, and as of early 2003 the funding source remained unclear.

The Coast Guard has seen its budget increase by more than \$1 billion since 9/11. However, those funds are doing little more than addressing previous shortfalls and supporting the higher pace of operations required since the terrorist strikes. They are doing little to increase the size of the Coast Guard, which we consider significantly too small for the tasks before it. For example, the major new shipbuilding initiative in the 2004 budget appears to be funding for nine more coastal patrol boats, or about 3 percent of the existing total, hardly a change commensurate with the new responsibilities of this agency.¹³

As a final example, the administration’s budget would add some 2,000 agents to the FBI, whereas we estimated last year that new requirements called for perhaps 5,000 additional agents. In fairness, a single-year increase of 2,000 agents would be a strong start toward the 5,000 goal, and it is not always realistic to increase personnel rosters at rapid rates. But the absence of a detailed future plan for where the administration intends to take certain agencies and efforts makes one wonder if further increases in FBI staffing

would be forthcoming in future budget proposals, as we think they must be (unless the function is transferred to a different agency).¹⁴

The Private Sector

Another area of disappointment continues to involve government oversight of the private sector. As we underscored in the initial edition of this volume, the most difficult homeland security challenges involve the intersection between the federal government and the private sector. Private markets will often not provide adequate protection against terrorist attack on their own, since individual citizens and businesses tend to worry more about the immediate challenge of making a profit than about the extremely unlikely possibility that their properties and facilities will be attacked. But policy-makers must be careful not to impose undue economic costs in exchange for little improvement in true security. As we argued in our April book, this dilemma calls for innovative forms of public-private partnership in which government requires certain basic safety standards and also requires certain types of private firms to carry terrorism insurance. The latter insurance markets can then offer incentives, in the form of preferred rate structures, for firms to take greater precautions against possible attack, allowing free-market forces to catalyze most action.

Unfortunately, precious little progress was made in this crucial area during 2002. The administration proposed no new initiatives and failed to spark discussion or debate about the most cost-effective ways of improving security in private-sector settings. As a result, the federal government made little or no progress in guiding private-sector firms—even ones that handle dangerous materials—toward improving their own security. Perhaps the best example involves chemical facilities.

As we emphasized in the initial edition of this volume, the nation has 12,000 or more chemical facilities, including more than 100 storing toxic chemicals that could, if released, endanger one million or more people. These chemical facilities are not adequately protected against terrorist attack.

In June 2002 the Environmental Protection Agency was on the verge of announcing regulations to improve security at chemical facilities.¹⁵ Yet this effort was blocked by the administration, at least in part because other government lawyers did not agree with EPA that it had sufficient statutory

authority to proceed. In Congress, Sen. Jon S. Corzine (D-N.J.) spearheaded an effort to pass legislation requiring chemical plants to identify vulnerabilities; the legislation was approved by the Senate Environment and Public Works Committee but met with stiff resistance from industry groups and was not brought to a vote before the full Senate.

Following an early October 2002 article in the *Washington Post* highlighting the glaring lack of activity in imposing security requirements at chemical plants, then OHS Director Thomas Ridge and EPA Director Christine Whitman wrote that mandatory government intervention would be required.¹⁶ They noted that all chemical facilities “must be required to take the steps the industry leaders are taking at their facilities . . . voluntary efforts alone are not sufficient to provide the level of assurance Americans deserve.”¹⁷ Yet as of early March 2003, no action had been taken, underscoring the fact that in many private-sector settings—from chemical plants to hazardous materials trucking firms and nuclear facilities—current efforts fall woefully short of what is required. And, again, in its 2004 budget the Bush administration treats infrastructure protection as a major category of effort, yet increases its budget by only about \$500 million relative to 2003 levels. In early 2003 the Department of Homeland Security issued a strategy document for protecting critical infrastructure, but the document lacked the types of specific policy steps that are now overdue.¹⁸

The Department of Homeland Security

On June 6, 2002, President George W. Bush went on nationwide television to propose the creation of a new federal Department of Homeland Security. On November 25, he signed into law a bill providing essentially what he requested. On March 1, 2003, a new structure was created to combine twenty-two agencies employing nearly 200,000 workers. It is, as the president has noted, the largest federal reorganization in more than half a century.

Bush had previously opposed creating such a department, arguing that the White House Homeland Security Council and Office he had established in October 2001 were sufficient to coordinate the American response to the terrorist threat. But by spring 2002, the new White House operation and its director, former Pennsylvania governor Tom Ridge, were increasingly criticized as ineffectual. The administration was also under growing attack

for the failure of the FBI and the CIA to follow up on leads that might have led to exposure of the al-Qaida plot before the World Trade Center and Pentagon attacks. By reversing course, indeed by calling for a department larger than any of his critics had been seeking, the president regained the initiative. Congressional action on his proposal became *the* homeland security policy event over the second half of 2002. Bush also scored political points in his midterm election campaign by arguing for sweeping management flexibility in the department and accusing Democrats of placing labor union interests in job security above the security of the nation. With modest constraints, the new law grants him this flexibility.

Now comes the hard part. Congress has established the department, largely as the president sought it. His administration must now make it work. It will be a daunting task. The White House could have sought a less encompassing, “more focused” department, concentrating on functions that would gain most from integration—such as border security—and others for which a central, integrated focus seems clearly needed—such as intelligence and infrastructure protection.¹⁹ Or Congress could have cut the president’s proposed organization down to a more manageable size. But these paths were not taken, and the result is a huge, multifunction entity that may take years to bring together.

Organization

At the heart of the Department of Homeland Security are four policy directorates, each headed by an undersecretary: border and transportation security, information analysis and infrastructure protection, emergency preparedness and response, and science and technology (see table 2).²⁰ The undersecretary for border and transportation security oversees the preponderance of DHS employees, with direct authority over enforcement personnel and functions transferred from the Customs Service (Treasury), the Immigration and Naturalization Service (Justice), the Transportation Security Administration (Transportation), and, in part, the Animal and Plant Health Inspection Service (Agriculture). This undersecretary does not have specific authority over the Coast Guard, which by law will report directly to the secretary. However, effective management of border security will require close coordination of the Coast Guard’s port security functions with those of Customs and Immigration, for example.

Table 2. Department of Homeland Security Funding

Millions of dollars of budget authority, including nonsecurity activities

<i>Activity or unit</i>	<i>Pre-9/11 2002 level</i>	<i>2004 request</i>
Discretionary budget authority (yearly appropriations)		
Border and transportation security		
Customs and border protection	4,063	5,649
Immigration and customs enforcement	2,127	2,488
Transportation Security Administration	1,242	4,812
Federal Law Enforcement Training Center	137	146
Office for Domestic Preparedness	260	3,558
Subtotal, border/transportation security	7,829	16,653
Coast Guard	4,129	5,634
Emergency preparedness/response	3,098	3,287
Science and technology	90	803
Information Analysis and infrastructure protection	117	829
Other activities	1,516	1,979
Total, discretionary budget	16,779	29,185
Mandatory budget authority and user-fee-based programs		
Border and transportation security		
U.S. Coast Guard	1,267	1,398
Emergency preparedness and response	1,458	2,676
Other activities	1,567	1,764
Total, nondiscretionary budget	5,342	6,993

Source: Office of Management and Budget, *Fiscal Year 2004 Budget of the U.S. Government* (February 2003), p. 161.

Notes: The 2002 budget clearly preceded the existence of the Department of Homeland Security, so budget totals for that year pertain to the individual constituent agencies that later joined DHS. The supplemental appropriation for 2002 totaled \$14.272 billion of budget authority. The total for DHS in 2004 does not conform to that shown in table 1 because nearly \$12 billion in non-security activities are included here.

The second undersecretary oversees the related but distinct functions of information analysis and infrastructure protection. In contrast to border security, the entities transferred into this directorate are small: the National Infrastructure Protection Center from the FBI, for example, has about 800 employees, and the total number of current agency officials incorporated in this directorate comes to only about 1,000. Therefore, the task here is not so much integrating existing entities as building new capabilities: to develop a comprehensive capability to identify and protect critical national

infrastructure and to form an intelligence unit capable of acquiring and integrating law enforcement and intelligence information key to the department's overall functioning. As we discuss further below, this is one area where the reorganization does not go far enough.

The directorate for emergency preparedness and response brings together several small entities transferred from other departments—mainly Health and Human Services (HHS)—with the larger, multipurpose Federal Emergency Management Agency (FEMA). The new unit's functions are those stated in its title. The apparent rationale for including FEMA in DHS is to raise the priority of terrorism among the myriad threats (primarily natural disasters) that it must prepare for and respond to, and to improve coordination of responders at all levels of government with the security, intelligence, and infrastructure activities housed elsewhere in DHS.

The fourth major subunit is the directorate for science and technology. Here Congress renamed, and to some degree reshaped, the original administration proposal for a directorate on chemical, biological, radiological, and nuclear (CBRN) countermeasures. As established in the law, it includes small offices with CBRN functions transferred from Energy and Defense, but also provides for a broader research and development function in addressing these threats—notably by creating the homeland security equivalent of the Defense Advanced Research Projects Agency (DARPA), as well as a clearing house for coordinating homeland security–related research at universities and the National Laboratories. The undersecretary for science and technology will find that the basic capabilities for addressing this directorate's responsibilities remain in other departments—HHS for biological threats, Energy for nuclear technology, Defense for CBRN response, and so on. DHS effectiveness in this important sphere will therefore depend on the ability to mobilize their assets.

Outside of these directorates stand the Secret Service, the Coast Guard (as previously mentioned), a new Bureau of Citizenship and Immigration Services, and myriad offices and advisory groups dealing with state and local government coordination, civil rights and civil liberties, and other issues. The legislation also makes the president's Homeland Security Council into a statutory entity, with a reduced number of core members (the president, the vice president, the secretaries of homeland security and of defense, and the attorney general), with language that parallels that of the 1947 act creating the National Security Council.

In its totality, the new department is a complex, multifunction entity, with many of the larger units (Coast Guard, Customs, Transportation Security Agency, FEMA, Secret Service) protected as entities within the department. In making it work, Secretary Tom Ridge will face multiple challenges.

The Managerial Challenge

The U.S. government—or the private sector for that matter—has never done anything quite like this merger of so many different entities involving so many different people. Even the creation of the Department of Defense in the late 1940s, though it involved more people, represented a smaller managerial challenge by combining a more limited number of very-much-like-minded units. Even so, the Defense organization was revisited numerous times over the next few decades, and it was only with passage of the Goldwater-Nichols Act of 1986 that the government finally got the Pentagon's organization about right. As for the private sector, in which mergers are of course far more common, there, too, the record is sobering: most private-sector mergers either fail or do little to improve the functioning of their constituent parts.

Over the next few months, Ridge and his management team will merge 22 different agencies that contain more than 100 bureaus, branches, sub-agencies, and sections—each with its own distinct culture. All of these units bring into the department a vast array of largely incompatible management systems, including at least 80 different personnel systems mixed in and among the agencies. There are, for example, special pay rates for the Transportation Security Administration, the Secret Service, and the Biomedical Research Service; higher overtime rates for air marshals, Secret Service agents, and immigration inspectors; guaranteed minimum overtime for Customs officers and immigration inspectors; Sunday, night, and premium pay for the Secret Service, Customs Service, and immigration inspectors; and foreign language awards and death benefits for Customs officers.

The DHS Act gives Ridge a tremendous amount of flexibility to decide how these disparate systems are to be integrated. But the decisions are no less difficult to make for that. The secretary will have to decide who moves and who doesn't, where they will go, what information technology systems need to be integrated, whose human resources rules to adopt, what pay scales to use for which jobs, and a host of other details that will determine the success or failure of this merger.

By far the biggest challenge Ridge and his people face is to undertake this unprecedented task while clearly keeping their eyes on the main ball—which is not to organize for homeland security but to prevent, protect, and respond to a future terrorist attack on U.S. soil. The terrorists will not wait until the U.S. government has completed its restructuring. So, as Ridge goes about meeting the managerial challenge of setting up the third largest cabinet department (after the Pentagon and the Veterans Administration), he must ensure that the employees continue to focus on doing everything they can to make the country secure even as their employment circumstances are undergoing wrenching change. It is an extraordinarily difficult task—but vital for the security of the country.

Functions Not Related to Homeland Security

With few exceptions, all of the agencies merged into DHS were created many years ago, for reasons that had only limited relevance to our current concern with homeland security. The new department has therefore assumed a host of functions and competencies that are unrelated to efforts to secure the nation against terrorist attack. DHS is now responsible for confiscating stolen art works, determining asylum, immigration, and naturalization eligibility; conducting search-and-rescue operations; installing and maintaining buoys; setting ship standards and mariner qualifications; carrying out research on foot-and-mouth disease; and helping people harmed by earthquakes, floods, hurricanes, or tornadoes. These and many other non-homeland security tasks are the responsibility of the Customs Service, the Immigration and Naturalization Service (INS), the Coast Guard, the Animal and Plant Health Inspection Service, FEMA, and other agencies that have been absorbed by the new department.

Thus, although homeland security is job one for the new department, Ridge and other senior officials will need to devote time and effort to ensure that the non-homeland security functions will continue to receive the same degree of attention as at present. In some cases, they are inheriting highly dysfunctional agencies (such as the INS) requiring reforms for reasons unrelated to protecting against terrorism. Some of these functions have high political salience (for example, federal response efforts in cases of natural disasters), and may therefore demand the attention of the secretary and other officials on an ongoing basis. And each of these functions must be

fulfilled without taking too much time and energy away from the new department's primary mission.

Executive Branch Coordination

Even though DHS combines many of the U.S. government agencies involved in the effort to secure the homeland, many others with a crucial role in the effort remain outside the department. Among these are the most critical agencies—the FBI under Justice, the CIA, Defense, the Centers for Disease Control (CDC), and others. There is a need therefore to coordinate the actions of these other units with those of DHS and to develop and implement a governmentwide homeland security strategy.

Arguably, the secretary of homeland security could take on these responsibilities. But interagency coordination led by individual cabinet secretaries has seldom worked well in the past, and it is not likely to do so now. The secretaries of Defense, Treasury, Justice, State, and HHS are unlikely to defer to directives from another cabinet agency that is a competitor for funds and presidential attention. That means some kind of White House–led coordination system must be retained. Although Congress turned the Homeland Security Council, established by President Bush in the immediate aftermath of the September 11 attacks, into a statutory entity, it was largely silent on the question of staffing.

Until now, the Office of Homeland Security has been the focal point of the executive branch coordinating effort, with a staff numbering more than 100, but many of its most capable people have moved with Tom Ridge to the new department. As of mid-March 2003, a successor to Ridge had not yet been named, and there is justifiable concern that he or she is unlikely to have the clout within the administration or even the White House necessary for coordinating the activities of such major players as the secretaries of Defense and Homeland Security, the attorney general, and the FBI and CIA directors.

With many of the relevant agencies merged into DHS, it is now possible to abolish the OHS and assign the National Security Council (NSC) the federal coordination role. This has the benefit of integrating the homeland security effort at home with the counterterrorism effort abroad and drawing on the well-established experience of the oldest and most successful White House coordinating mechanism. In recent years, as the nature of the

national security challenge has evolved with the end of the cold war, the NSC has already begun to evolve to include a broader range of agencies and substantive policy issues. Including homeland security within the NSC's remit would substantially further this evolution. Of course, doing so would mean an expansion of the NSC staff, a broadening of its mandate, and its immersion in operational domestic matters to an unprecedented degree. Moreover, the NSC's track record has been decidedly mixed in areas outside its core emphasis on international political-military issues.

Reforming Congress's Role

Much of the benefit of consolidating the homeland security mission within the executive branch will be lost if our national legislature fails to reflect that reorganization in its own structure. Congressional oversight of homeland security activities has traditionally been scattered across Capitol Hill. By the administration's count, thirteen full committees in each house, and a total of 88 committees and subcommittees overall, shared responsibility for overseeing the homeland security mission in 2002. The House Appropriations Committee alone had eight subcommittees overseeing the agencies and programs merged into DHS. With authority so badly fragmented, coordination problems were rife, and no one was responsible for trying to bring coherence to the decisions made by individual committees.

The Department of Homeland Security Act expresses "the sense of Congress that each House of Congress should review its committee structure in light of the reorganization of responsibilities within the executive branch." To its credit, Congress has taken some important steps to meet this call. The House and Senate Appropriations Committees agreed at the start of 2003 to realign their subcommittee jurisdictions to create new homeland security subcommittees. This restructuring both institutionalizes the responsibility for appropriations oversight of the executive branch—increasing the chances that budgetary supervision will occur even if events shift political appeal to other topics—and reduces fragmentation—increasing the chances that Congress can identify major gaps and sensible trade-offs in homeland security spending.

Congress has not moved as aggressively to consolidate the badly fragmented authorization process. The Senate plans no changes to its committee structure. The Government Affairs Committee had responsibility for

overseeing the creation of DHS, while other authorizing committees have responsibility for overseeing individual programs and agencies within DHS. The House has gone somewhat further. It has created a Select Homeland Security Committee, composed on the Republican side largely of the chairmen of the committees with a stake in homeland security. The goal is to establish a permanent Homeland Security Committee at the start of the 109th Congress (2005–07). The question of what jurisdictions a permanent committee would take from other panels has yet to be answered. In the interim, the leadership of the select committee sees its task as coordinating the homeland security actions of other committees and reconciling any disagreements rather than establishing a claim to primary authorization oversight of homeland security.

Although the House's approach is preferable to the Senate's, neither is sufficient to ensure effective congressional oversight. Maintaining a fragmented authorization process increases the odds that Congress will drag its feet in considering executive branch proposals, bicker internally over the direction of homeland security, and issue conflicting directives to DHS. A streamlined appropriations process cannot eliminate these problems, even though appropriators normally follow the authorizers in the legislative process and can in theory reconcile any conflicting authorization mandates. Appropriators approach oversight largely through budgetary and management lenses. Their instinct is to ask how much is being spent and whether it can be spent efficiently. They devote less time to the related but distinct policy issues that the authorizing committees specialize in. As a result, the chances remain that broader policy issues either will be the object of turf wars or fall through the cracks of the authorization process. Bringing committee heads together as the House proposes can mitigate these problems in the short term. It is debatable, however, that a select committee will provide adequate oversight in the long term. Committee chairs have numerous competing demands on their time, many of which are more politically salient than homeland security. Moreover, the select committee approach by its nature focuses oversight attention on where committees disagree rather than on the equally pressing question of whether the sum total of committee decisions makes sense.

Congress would be wise then to take to heart its message in the Department of Homeland Security Act and reorganize its jurisdictions to

create standing authorizing committees for homeland security. Such a reorganization would not produce a unified decisionmaking process. Some fragmentation would remain as a result of bicameralism and the twin-track authorization and appropriations process. The task of coordinating the authorizers and appropriators on homeland security with those responsible for related activities by the intelligence agencies, the FBI, and the Pentagon (to name just a few) would also remain. But establishing dedicated homeland security committees to complement the homeland security appropriations subcommittees would likely maximize the efficacy of congressional oversight.

Priorities for the Secretary of Homeland Security

Secretary Tom Ridge and his management team must tackle their mammoth reorganization task without turning their eyes away from their overriding goal: securing America against a future terrorist attack. It is therefore crucial that Ridge set clear reorganization priorities—focusing on those areas that need the most immediate attention and leaving others until later.

First, he should make sure that information flows through the new department's entities and to other key actors inside and outside government with the necessary speed so that everyone will have access to all the information they need to do their jobs. As part of that effort, Ridge must also make sure that the new information analysis section is able to provide rapidly the integrated analysis of all foreign and domestically collected threat information that has until now been lacking.

Border and transportation security comes next. The people, agencies, and capabilities that will secure the national boundaries and the vast transportation network spanning the nation must be fully integrated as soon as possible. Critical infrastructure protection and science and technology efforts should also be in the list of top priorities.

Finally, emergency response efforts are already handled reasonably well. So Ridge would be wise to defer major reorganization efforts in this area until other, higher priority work is well advanced.

Intelligence

With the conclusion of the congressional debate over establishing the Department of Homeland Security, much of the focus of lawmakers and

policymakers should now return to the central issue of how to address the problem of collecting, analyzing, and disseminating intelligence for homeland security. To date, this issue has received inadequate attention; the administration has proposed a number of incremental reforms, but fundamental questions remains concerning the appropriate division of responsibilities of the key federal actors—especially the CIA, the FBI, and the Department of Homeland Security—and their relationship to state and local governments and to the private sector. In particular we believe that the time has come for a more integrated approach to the counterterrorism mission in the United States, separate from the FBI. Useful guidance on how to proceed was furnished by the report of the House-Senate joint inquiry of last year.²¹ It refocused attention on the core question of who should be responsible for domestic security intelligence analysis and collection and how to solve the problem of intelligence sharing both within and between agencies at the local, state, federal, and international levels, as well as with the private sector.

The joint inquiry report stated that “prior to September 11, the Intelligence Community was neither well organized nor equipped, and did not adequately adapt to meet the challenge posed by global terrorists focused on targets within the domestic United States. . . . Within the Intelligence Community, agencies did not share relevant counterterrorism information . . . not only between different Intelligence Community agencies but also within individual agencies, and between the intelligence and the law enforcement agencies. Serious problems in information sharing also persisted between the Intelligence Community and . . . other federal agencies as well as state and local authorities.”

The challenge of designing an effective domestic security intelligence architecture has two key dimensions. First, what information do we need to collect and who is best positioned to do it? Second, how do we ensure that the information is shared with all the relevant actors—analysts and those with operational responsibility both for policymaking and for providing protection—while protecting sensitive sources and methods as well as the legitimate privacy rights of individuals?

The “what to collect debate” was stoked by a number of post-9/11 proposals. These included the Justice Department’s proposed “Operation TIPS” (Terrorism Information and Prevention System), which would encourage non-law-enforcement personnel (such as postal carriers, utility workers, and others) to provide information on “suspicious” activities,²² and the

Pentagon's Total Information Awareness (TIA) program, which sought to test the counterterrorism value of sophisticated data-mining techniques, drawing on the masses of individualized data in private records, such as credit card transactions.²³ These proposals were challenged on two levels—first, that the information to be collected was of questionable value, and second, that they would constitute an unprecedented intrusion on individual privacy.

In parallel, there was a deepening controversy over “who should do it?” Specifically, this debate focused on whether there was a need for a wholesale reorganization of the intelligence community to address the challenge of homeland security.

The solution adopted by the Bush administration has focused largely on incremental improvements in the existing intelligence architecture. Under the Homeland Security Act, a new homeland security analysis capability was created in the new department with fairly broad responsibilities, including integrating and analyzing information concerning terrorist threats to the United States and vulnerabilities, and disseminating relevant information to federal, state, and local agencies and the private sector. To accomplish these tasks, Congress gave the secretary of homeland security authority to gain access to intelligence, including unevaluated intelligence, relating to threats of terrorism against the United States—a point that was a matter of some controversy during the debate over the legislation.

Just one week after the department was formally set up, President Bush, in the State of the Union address, announced a new initiative to create a Terrorist Threat Integration Center (TTIC), to fuse intelligence and analysis from both domestic and foreign sources. The new center would comprise primarily analysts from the CIA and the FBI, and it would report directly to the director of central intelligence.

As a further step toward integrating the domestic security intelligence structure, the TTIC is a positive step forward. But it raises a number of serious questions.

First is the problem of duplication and overlap. This new analysis center could duplicate other analytic capabilities already in place, including those at the CIA director's Counter-terrorism Center (CTC), the Defense Intelligence Agency (DIA), NSA, the State Department, and the FBI—not to mention the new analysis functions established in the Department of Homeland Security.

Second is the question of whether a joint venture, composed of analysts on assignment from their home agencies, can effectively provide real intelligence integration suited to the unique challenges of homeland security. The charter for the TTIC is nearly identical to the mission statement and organizational structure for the CTC, which is also a joint venture, raising the question about why the TTIC is any more likely to be successful than its predecessor. For this reason, the Gilmore Commission, an independent panel chaired by the former governor of Virginia to assess the nation's ability to respond to terrorism involving weapons of mass destruction, recently came out in favor of an independent intelligence fusion center, not dependent on employees seconded from home agencies.

Third is the question of the effect of the TTIC on the responsibilities of the secretary of homeland security. By locating the center outside DHS, the administration runs a serious risk of disconnecting the intelligence collection and analysis function from those actually responsible for carrying out the key homeland security missions—securing our borders, protecting critical infrastructure, and responding to emergencies. In effect, the secretary of homeland security must ensure that the homeland is safe without the authority to collect or access to the information (including raw intelligence) needed to carry out the task. Instead he will depend largely on the TTIC for analysis and the FBI for domestic intelligence collection—two entities over which he has no authority and only advisory input.²⁴

Of course, some of these problems existed even before the creation of the TTIC. For example, under the Homeland Security Act the new undersecretary for information analysis and infrastructure protection can “make recommendations” for policies governing information sharing, and “consult” with the director of the CIA and other intelligence and law enforcement agencies concerning intelligence collection priorities, but the law failed to provide any real authority in either area or any meaningful guidelines for how priorities should be set.

This approach has a number of serious limitations. In particular, there are strong reasons to question whether the FBI is the right agency to conduct domestic intelligence collection and analysis. The fundamental mission of the FBI as a law enforcement agency is to catch and prosecute perpetrators of crimes. Its methods are tailored to statutory and constitutional standards designed to protect innocent individuals from being deprived of

their liberty. By contrast, the principal mission of a domestic security agency must be prevention. Although apprehension and incarceration may contribute to prevention (by incapacitating dangerous people and deterring others by example), focusing on individual “bad actors” may leave us vulnerable to plots where the perpetrators (but not the object of attack) are unknown. And the desire to build a strong case for prosecution that will stand up in court may lead to delaying action that would prevent a dangerous attack from occurring in the first place. Although creation of the TTIC will lessen the FBI’s control over domestic intelligence analysis, it will remain a joint center depending on rotating employees from the FBI and other units, thus ensuring that, as a practical matter, the mindsets of the contributing agencies will continue to dominate TTIC’s work (just as they did for the CTC).

The perpetrator-based focus also pervades the administration’s approach to the second key problem of how to share information with state and local officials (as well as key members of the private sector such as health care providers and managers of critical infrastructure). Significant progress has been made in developing a comprehensive database that would allow local law enforcement officials to check whether an individual was listed on any of the key “watch out” lists—a major shortfall in the pre-9/11 environment.²⁵ And the administration vowed to increase the number of counterterrorism analysts at the FBI. But it is not at all clear that this system would help address one of the most serious failures of the old system—the failure to respond to the notorious “Phoenix memo,” warning of possible concerns about Middle Eastern males attending U.S. flight schools. Absent individual identifying information, the new architecture would not necessarily lead to a more effective response. Nor is it clear how state and local officials or the private sector would access analysis and intelligence from the new TTIC. As a practical matter, lines of communication will probably run from both DHS and the FBI, creating further confusion and uncertainty and lessening the responsiveness of the tasking and analysis function to the needs of these key end users.

There are two steps that would remedy these difficulties. The first is to create a single agency with responsibility for domestic security collection and analysis against foreign threats. This would go beyond the TTIC proposal in that it would have responsibility for both collection and analysis

and would not be dependent on employees on temporary assignment from home agencies. Such an agency could be housed within the Justice Department (reporting to the attorney general but not the FBI director) or within DHS or act as a stand-alone agency (with a link to the director of central intelligence). This agency would focus on “foreign” terrorism (that is, not on domestic terrorists such as Timothy McVeigh), would not have arrest powers, and would be governed by tailored guidelines that would allow effective use of investigatory tools essential to the homeland security mission while protecting against overly broad intrusions on privacy.²⁶ This approach has been endorsed by the Gilmore Commission and by several former intelligence community officials and members of Congress.²⁷

The second is to develop a more decentralized architecture that would enhance information exchange at the local level among all relevant actors, as well as facilitate two-way flows from the federal government to local communities and vice versa. Some of this challenge is technological—providing peripheral devices that can communicate in real time with all relevant actors. Some is organizational—such as reducing the security “compartments” that make it difficult for all but those with high-security clearances and a predefined “need to know” from accessing the networks of information. The Pentagon’s Afghan war chat-rooms are a rudimentary model of what is possible through the use of new information technologies and an open architecture.²⁸ The recently released report of the Markle Foundation Task Force on Security in an Information Age, *Protecting America’s Freedom in the Information Age*, outlines a set of principles that should guide the creation of a “next generation” homeland security information network.

The important points here are three. One, the major institution for domestic intelligence collection and analysis should not be within the FBI. Two, wherever it is, the new unit or agency must have serious mechanisms for protecting civil liberties, including formal guidelines for acquiring, sharing, and maintaining personally identifiable data and strong measures for accountability, as well as independent oversight of its activities monitoring U.S. citizens and noncitizens alike. Three, the debate over where to place the new and strengthened institution must not be allowed to swamp all other debates and action on homeland security in 2003, in the manner that the debate over the creation of DHS regrettably impeded other homeland security action in 2002. Whether that new intelligence agency should be

within DHS or independent is debatable; that it should be outside the FBI, however, is, in our judgment, imperative. One logical approach might be to put it within DHS to start, but leave open the possibility of turning it into an independent agency reporting to a new director of national intelligence as part of a future reform of the entire U.S. intelligence community.

Conclusion

The Bush administration, Congress, and many other levels of government as well as private American citizens need to reinvigorate their efforts to improve homeland security against terrorist attack. We could well be experiencing a hiatus between major attacks made possible by the combination of offensive military operations in Afghanistan, the resulting severe but potentially temporary disruption of al-Qaida, good follow-up intelligence and law enforcement work, and perhaps a bit of good luck. The federal government, after a respectable start in 2001, did not on the whole distinguish itself in its homeland security efforts in 2002 and must accomplish more this year and thereafter.

The first priority relates to resources. Congress and the president enacted an inadequate level of funding in 2003 for homeland security. In addition to rectifying that problem, they need to turn promptly to the 2004 budget and redress vulnerabilities not yet given sufficient priority. These include the use of information technology, where federal funding to date has been a pittance of what is required. They also include public-private cooperation on protecting assets such as chemical facilities, hazardous materials trucking, and the air intakes of skyscrapers. Finally, a number of existing capabilities and capacities need dramatic and rapid augmentation. Such strengthening has already occurred in areas such as airport security and airplane marshals; it now is needed for the Coast Guard, the Customs Service, train travel, airliner protection against surface-to-air missiles, and many state and local capacities (such as first responder teams and hospitals) as well.

Another major part of the challenge is making real what Congress and President Bush have created on paper, but not yet in reality—a new and huge federal Department of Homeland Security. Tom Ridge and his management team face a mammoth reorganization task—larger in many ways than anything ever attempted in government. And they must undertake that

task without in any way reducing their attention to the demanding effort of securing America against a future terrorist attack. It is therefore crucial that Ridge sets clear reorganization priorities—focusing on those areas that need the most immediate attention such as border security and information analysis (and leaving others, such as federal emergency response, until later). Ridge’s undersecretary candidates will need to display strong organizational and managerial abilities, particularly in areas such as infrastructure protection, where whole new capacities need to be created and where little has been accomplished to date, despite the heightened attention given to homeland security since 9/11.

Finally, the government needs to organize itself much more effectively to monitor terrorists and try to determine where their next attacks may come. A stronger domestic counterterrorism entity is needed, including a new agency independent from the FBI. At present, we are hoping to get lucky by identifying and apprehending individual terrorists before they can strike. We also need to develop an alternative approach that allows us to address the “unknown unknowns,” using “red teams” to prepare for what terrorists might do next even if they have shown no proclivity for such attacks to date.

It is tempting to give policymakers a grade for their efforts at homeland security. But that would be simplistic; for every important step that has been taken, an equally important one has been neglected. It would also be misleading, because the job is just beginning, so the grade must be incomplete for now. The challenge in Washington and elsewhere is to act quickly enough that the next major terrorist attack does not happen before we are ready.