Protecting the American Homeland: One Year On

IVO H. DAALDER I. M. DESTLER

DAVID L. GUNTER JAMES M. LINDSAY

MICHAEL E. O'HANLON PETER R. ORSZAG

JAMES B. STEINBERG

THE BROOKINGS INSTITUTION
Washington, D.C.
January 2003

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. Americans, aware now of the harm terrorists can inflict, are on alert, providing a first, crucial line of defense. Air travel is now 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 have been taken to reduce the country's exposure to biological attacks, with more to follow, 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 past tactics of al Qaeda, not an anticipation of possible future innovations in how 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 — may have some merit, though 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. Moreover, excessive focus on organizational matters during the past year was one reason Congress has so far failed to pass a federal budget for homeland security for 2003. Even assuming that budget is soon passed, valuable time will have been lost in 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, 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 Qaeda 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 focusing on 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 possible 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 — and more money, perhaps $10 billion (less than 3% of the defense budget) a year above what the administration proposed to spend annually a year ago.

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 set of priorities, if efforts are not to degenerate into a scattershot 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 would be produced more than a month after the administration proposed a new department of homeland security, since the organization of

the 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 backwards 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, 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 are to 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 makes a start, but it leaves out several key priorities for action that we strongly advocated in April 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 and its proper uses; despite rhetoric about using IT aggressively to promote homeland security, the Bush administration budgets and programmatic 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 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 now 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 April 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. 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.[4] It was a reasonable first response. But quite naturally, it had major gaps. And those gaps are likely to persist if the administration bases its 2004 budget on the July strategy document.

Indeed, the 2003 budget has not yet even been approved as of this writing. That is because, during the second half of 2002, the debate over the

Department of Homeland Security diverted the attention of policy-makers 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. It is deeply disturbing that the 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 also made in regulating the private sector, with little or no action taken by the government to improve security at large buildings, chemical facilities, and ports. The bottom line is 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 within the discretionary spending component of the budget; such discretionary spending is determined in a set of 13 annual appropriations bills. Battles over the size and shape of the budget meant that as of December 2002, only 2 of the 13 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.

Media reports, for example, suggest that the disruption in funding associated with the continuing resolution 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.[5] Representative David Obey (D-Wisconsin) noted that the continuing resolution finances bioterrorism activities at $2.3 billion less than the administration's budget suggested was necessary, and finances first responder programs at $2.5 billion less than the administration's budget called for.[6]

Even assuming that the problems created by the continuing resolution are addressed by the new Congress and the relevant agencies make up fairly well for the lost time caused by the funding difficulties in late 2002, however, two problems will remain.

First, the design of the Federal budget has not been updated to reflect the emergence of homeland security as a priority for policy-makers. "Homeland security" funding is spread across myriad budget items and is distributed across multiple appropriations sub-committees. As a result, specific homeland security items are not evaluated as part of an overall homeland security package, as they should be, but rather in the context of the other non-homeland security items facing the individual sub-committees. In the initial version of our volume, we recommended the creation of a new appropriations sub-committee to handle homeland security spending, and we still think such a Congressional reform makes sense. In the meanwhile, the debate over homeland security funding is unnecessarily complicated by the existing budgetary setup, since too many subcommittees share responsibility for a single mission.

Second, the overall funding level proposed for homeland security in the administration's FY 2003 budget, which would be reflected in the appropriations bills that the Congress could enact for FY 2003, remains lower than we believe necessary. The administration has requested $38 billion for homeland security although Congress may reduce that amount in January; our analysis, however, suggests that about $45 billion would be more prudent. The administration's lower funding 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.[7] A freeze may be temporarily necessary to ensure that inter-agency communications problems are not exacerbated, but upgrading existing information technology systems to ensure better inter-office 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 version 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.

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 FY 2003 budget included no additional funding for this initiative.[8] Similarly, the 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 late December 2002, it was unclear whether such funding would be provided in other legislation.

The administration's FY 2004 budget will be unveiled in February 2003. Unless it includes a healthy increase in the amount proposed in the FY 2003 budget and thereby provides homeland security funding adequate to addressing the types of deficiencies discussed above, the nation will continue to under-invest in our homeland defense efforts.

The Private Sector

Another area of disappointment in 2002 involves government oversight of the private sector. As we underscored in the initial version 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 businessmen 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 version of this volume, the nation has 12,000 or more chemical facilities, including more than 100 that store 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.[9] 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, Senator Corzine (D-NJ) 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 article in the *Washington Post* highlighting the glaring lack of activity in imposing security requirements at chemical plans,[10] OHS Director Thomas Ridge and EPA Director Christine Whitman wrote that mandatory government intervention would be required. 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."[11] Yet as of December 2002, 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 fail woefully short of what is required.

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. By March 1, 2003, twenty-two agencies employing nearly 200,000 workers will be moved formally if not physically into the new structures. It will be, 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

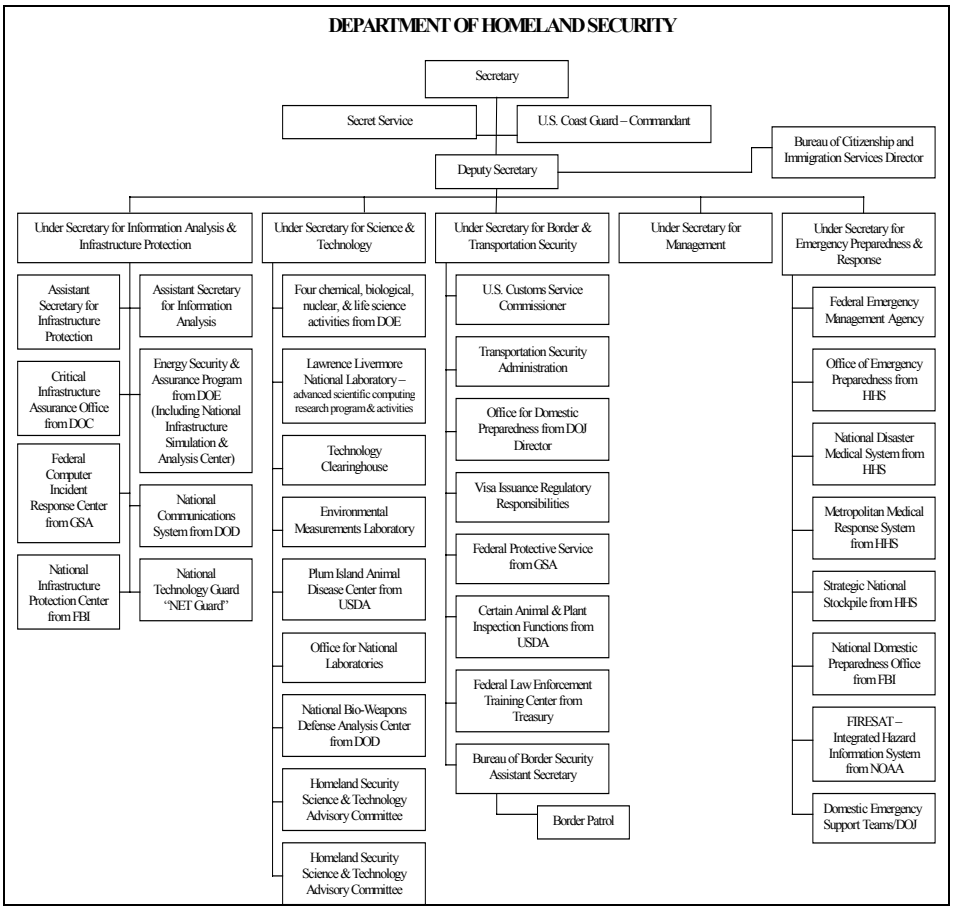
increasingly criticized as ineffectual. The administration was also under growing attack for the failure of the FBI and the CIA to follow up on leads that might have led to exposure of the Al Qaeda plot prior to the World Trade Center and Pentagon attacks. By reversing course, indeed by calling for a 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 mid-term 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. Now his administration must 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 — like border security—and others for which a central, integrated focus seems clearly needed — like intelligence and infrastructure protection.[12] Or Congress could have cut the President's proposed organization down to a more manageable size. But this path was not taken, and the result is a huge, multi-function 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 under secretary: Border and Transportation Security, Information Analysis and Infrastructure Protection, Emergency Preparedness and Response, and Science and Technology.[13] (See Figure.) The under secretary for border and transportation security will oversee the preponderance of DHS employees, with direct authority over enforcement people 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). He will 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 the Customs and Immigration, for example.

The second under secretary will oversee 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 a thousand. Therefore, the task here will be 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 will bring together — and perhaps integrate — several small entities transferred from other departments (mainly HHS) with the larger, multipurpose Federal Emergency Management Agency (FEMA). The new unit's functions will be 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) which 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 the Congress renamed, and to some degree reshaped, the original administration proposal for a directorate on Chemical, Biological, Radiological, and Nuclear 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 in universities and the National Laboratories. The under secretary for science and technology will find that the basic capabilities for addressing this directorate's responsibilities remain in other departments — HHS for biological threats, DOE for nuclear technology, DOD for CBRN response, etc. 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, etc. 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 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, TSA, FEMA, Secret Service) protected as entities within the department. In making it work, Secretary-designate 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 the 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 DOD reorganization 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: 70 percent of all 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 have to merge 22 different agencies that contain over 100 bureaus, branches, subagencies, and sections—each with its own distinct culture. All of these units will 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 the new secretary 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 resource 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. The flexibility Congress has granted Ridge means that the decisions are his to make — but in itself that does not mean his decisions are going to be any easier to make.

By far the biggest challenge Ridge and his people will face is to undertake this unprecedented task while clearly keeping their eye 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 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 that they succeed.

Functions Not Related to Homeland Security

With few exceptions, all of the agencies being 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 is therefore assuming a host of functions and competencies that are unrelated to efforts to secure the nation against terrorist attack. DHS would be 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 diseases, and helping people harmed by earthquakes, floods, hurricanes, or tornadoes. These and many other non-homeland security tasks are currently the responsibility of the Customs Service, INS, Coast Guard, Animal and Plant Health Inspection Service, FEMA, and other agencies that the administration proposes to move into the new department. All of these functions are now DHS's responsibility.

Thus, although homeland security will be 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 will inherit highly dysfunctional agencies (like the INS) requiring reforms for reasons unrelated to protecting against terrorism. Some of these functions have high political salience (*e.g.*, 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 will remain outside the department. Among these are the most critical agencies — Justice, FBI, CIA, Defense, CDC, etc. There is a need therefore to coordinate their actions with those of DHS and to develop and implement a government-wide 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 over one hundred, but many of its most capable people are slated to move with Tom Ridge to the new department. A successor to Ridge has yet to be 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 NSC the federal coordination role. This has the benefit of integrating the homeland security effort at home with the counter-terrorism 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 immersing it 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

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." Much of the benefit of the consolidation enacted for the executive branch will be lost if our national legislature fails to reflect that reorganization in its own structure. By the administration's reckoning, thirteen full committees in each house, and a total of 88 committees and subcommittees share responsibility for homeland security today. Although this count overstates matters somewhat, the dispersal of congressional oversight of homeland security is considerable — far more than is necessary. INS, the Customs Service, the Animal and Plant Health Inspection Service, the Coast Guard, the Transportation Security Administration, and FEMA together constitute 79 percent of the budget of the department President Bush proposed and 95 percent of its employees. These agencies are now primarily overseen by four authorizing committees in the House (Agriculture, Judiciary, Transportation and Infrastructure, and Ways and Means) and five in the Senate (Agriculture, Commerce, Environment and Public Works, Finance, and Judiciary). In addition, five different appropriations subcommittees in the House and five in the Senate have a say over these same agencies. Authority is badly fragmented, coordination problems are rife, and no one is responsible for trying to bring coherence to the decisions made by individual committees.

To rectify this situation, both houses of Congress must reorganize by creating authorizing committees and appropriating subcommittees for homeland security. The House has already made an important start by establishing a new Select Committee for Homeland Security. Such a restructuring would both institutionalize the responsibility for overseeing the executive branch — increasing the chances that oversight would occur even if events shift political appeal to other topics — and reduce fragmentation — increasing the chances that Congress can identify major gaps and sensible trade-offs in homeland security. Of course, some degree of fragmentation would remain as a result of bicameralism and the twin-track authorization and appropriations process. The task of coordinating the actions of 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 that problem could never be resolved unless Congress chose to operate entirely as a committee of the whole, thereby forfeiting all the benefits of specialization.

Powerful representatives and senators who stand to lose from a reorganization like this are bound to oppose the changes. But leaders in both bodies seem to recognize that effective congressional oversight of homeland security demands no less. Though change is often difficult, particularly when powerful political interests are at stake, history gives ground for optimism that Congress can make the organizational changes required. In merging the Naval and War Committees into unified Arms Services Committees after World War II and in creating the Budget and Intelligence Committees in the mid-1970s, members overcame their innate inertia and put their policy interests above their parochial concerns. The same logic would support a comparable reorganization today.

Priorities for the Secretary of Homeland Security

The first task for Secretary-designate Tom Ridge is to recruit a top-flight management team, with particular emphasis on the under secretaries who will head the four directorates. Together they 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 in and out of government with the necessary speed so that everyone will have access to all the information they need to do their job. As part of that effort, Ridge must also make sure that the new information analysis section is rapidly able to provide 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 attention 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. This matter remains far from resolved despite the fact that DHS is already mandated to contain its own intelligence unit. It should have a stronger unit that takes over the role many still advocate for the FBI, an organization that is poorly suited to the counterterror tasks at hand for a number of reasons.

Useful guidance on how to proceed was furnished by the report of the House-Senate Joint Inquiry of last year.[14] It refocused attention on the core question of who should be responsible for domestic security intelligence analysis and collection, and of how to solve the problem of intelligence sharing both within and between agencies at the local, state, federal and international level, 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, etc.) to provide information on "suspicious" activities,[15] 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, etc.[16] 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 focused largely on incremental improvements in the existing intelligence architecture. A new homeland security analysis capability was created in the new department of homeland security, 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.

But this new analysis center was created in addition to all the existing analytic capabilities, including those at the DCI's Counter-terrorism Center (CTC), DIA, NSA, the State Department and the FBI. The new under secretary 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 fails to provide any real authority in either area or any meaningful guidelines for how priorities should be set. To date, there is little insight into how the FBI and DHS intelligence functions will interact. Domestic intelligence collection remains the responsibility of the FBI, while analysis would appear to be shared between the two. And early reports indicate that guidelines for sharing information with the department are more restrictive than the legislation envisages (and more in line with what the administration originally proposed).[17]

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.

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, managers of critical infrastructure, etc.). 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 shortcoming in the pre-9/11 environment.[18] 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.

There are two steps that would remedy these difficulties. The first is to create a separate agency with responsibility for domestic security collection and analysis against foreign threats. Such an agency could be housed within the Justice Department (reporting to the attorney general but not the FBI director), within DHS, or as a stand-alone agency (with a link to the director of central intelligence). This agency would focus on "foreign" terrorism (that is to say, not on domestic terrorists like 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.[19] This approach has been endorsed by the Gilmore Commission and by several former intelligence community officials and members of Congress.[20]

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 facilitating 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 pre-defined "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.[21] The recently released report of the Markle Task Force, *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 non-citizens 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 the 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 of 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, the 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 Qaeda, 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.

The first priority relates to resources. Congress needs to pass the 2003 federal homeland security budget quickly. It then needs 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 trucking, and the air intakes of skyscrapers. Finally, a number of existing capabilities and capacities need dramatic and rapid augmentations. Such strengthening has already occurred in areas such as airport security and airplane marshals; it now is needed for the Coast Guard, Customs, train travel, 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 like border security and information analysis (and leaving others, such as federal emergency response, until later). Ridge's choices for under secretaries 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 imagine 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, since 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.

ACKNOWLEDGMENT:

This project was made possible through the generous financial support of the John D. and Catherine T. MacArthur Foundation.

ENDNOTES:

[1] For a similar conclusion, see Gary Hart and Warren Rudman (co-chairmen), *America — Still Unprepared, Still in Danger*, Report of an Independent Task Force sponsored by the Council on Foreign Relations (October 2002), available at: http://www.cfr.org/pdf/Homeland_TF.pdf.

[2] See Jack Weiss, *Preparing Los Angeles for Terrorism* (City of Los Angeles, October 2002).

[3] See Office of Homeland Security, *National Strategy for Homeland Security* (July 2002), available at www.whitehouse.gov.

[4] See *Securing the Homeland and Strengthening the Budget* (February 2002), available at www.whitehouse.gov/homeland/homeland_security_book.pdf.

[5] Jonathan Weisman, "Spending Bill Delays Crimp War on Terror: Congress's Inaction Slows Domestic Plans," *Washington Post*, November 19, 2002.

[6] Rep. David Obey, "Defending the Homeland: A Case of the 'Slows'", December 18, 2002.

[7] See, for example, the discussion in Nicholas Kulish, "Security Agency Beset by Babel," *Wall Street Journal*, December 24, 2002, page A4.

[8] Rep. David Obey, "Defending the Homeland: A Case of the 'Slows'", December 18, 2002.

[9] Leaked EPA documents describing the proposed regulations were posted on the Greenpeace website.

[10] "EPA Drops Chemical Security Effort," *Washington Post*, October 3, 2002, p. A17.

[11] Thomas Ridge and Christine Whitman, "A Security Requirement, *Washington Post*, October 6, 2002, p. B06.

[12] We proposed such an approach in Ivo H. Daalder et al, *Assessing the Department of Homeland Security* (Washington, D.C.: Brookings Institution Press, July 2002), available at: http://www.brookings.edu/dybdocroot/fp/projects/homeland/assessdhs.pdf.

[13] For details, see Public Law 107-296.

[14] See *Findings of the Final Report of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence Joint Inquiry into the Terrorist Attacks of September 11, 2001*, http://intelligence.senate.gov/pubs107.htm

[15] Operation TIPS was unveiled as pilot project in January, 2002 and the Administration initially included it in its draft legislation for DHS. Congressional

opposition led to a specific prohibition on Operation TIPS in the final DHS bill. See Dan Eggen, "Proposal to Enlist Citizen Spies Was Doomed From Start," *Washington Post*, November 24, 2002; p. A11.

[16] See John Markoff, "Pentagon Plans a Computer System That Would Peek at Personal Data of Americans", *New York Times*, November 9, 2002, p. A12. For the Pentagon's description of the program, see: http://www.darpa.mil/iao/TIASystems.htm..

[17] Dan Essen and John Mintz, "Homeland Security Won't Have Diet of Raw Intelligence," *Washington Post*, December 6, 2002, p. A43.

[18] The lack of a central database and a single point for all source analysis were key findings of the Joint Inquiry

[19] For an example of guidelines that could be used to govern government access to private databases, see Markle Foundation Task Force, *Protecting America's Freedom in the Information Age*, p. 32-33.

[20] See the Fourth Annual Report of Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, http://www.rand.org/nsrd/terrpanel/. See also *Hearings before the Committee on Governmental* Affairs, 107. Cong. 2 sess., June 26 and 27, 2002, especially the testimony of Jeff Smith, Former General Counsel of the CIA, and General William Odom, former director of the NSA. See also Duncan DeVille "How to Split Up the Bipolar F.B.I.," *New York Times*, June 18, 2002, p. A23; Senator John Edwards, "Agenda for Homeland Security" Brookings Institution, December 12, 2002, available at: http://www.brookings.edu/comm/events/20021218edwards.htm#TRANSCRIPT.

[21] The Department of Homeland Security legislation recognizes the importance of these linkages through the creation of an Office of State and Local Coordination (Sec. 801), and a Special Assistant to the Secretary with responsibility of liaison to the private sector (Sec 102(f)).