Testimony Before
The Committee on Governmental Affairs
United States Senate
Wednesday, June 26, 2002

# ROLES FOR THE WHITE HOUSE AND THE NEW DEPARTMENT

**Ashton B. Carter**
Co-Director, Preventive Defense Project
John F. Kennedy School of Government
Harvard University

Mr. Chairman and members of the Committee on Governmental Affairs, thank you for inviting me to appear before you today. My written statement addresses the overall architecture of the federal government for homeland security, including the respective roles of the White House and the proposed new cabinet department. My oral comments will focus on several new types of "intelligence" – which I mean very generally to denote information and analysis bearing upon the successful accomplishment of the mission of homeland security over time – that the new Department of Homeland Security could usefully devise and then practice. These are modes of intelligence that the CIA and FBI are unlikely to practice well by themselves, but to which they can furnish important inputs.

Still homeless after 9/11. Dealing with homeland security is quintessentially a managerial matter, and it is consequently not surprising that Washington has fumbled it so far. Washington is best at tackling policy problems, not managerial problems. In 2000, I made a judgment in *Foreign Affairs* that I see no reason to amend as yet, two years later and nine months after the disaster of 9/11:

> Today some of the most critical security missions – counterterrorism, combating WMD proliferation, homeland defense (including protection against computer network attacks and biological weapons), information warfare, peacekeeping, civil reconstruction, and conflict prevention (or "preventive defense") – are accomplished in an ad-hoc fashion by unwieldy combinations of departments and agencies designed a half-century ago for a different world. Too many of these missions are institutionally "homeless": nowhere are the authority, resources, and accountability brought together in sharp managerial focus. Although it is widely agreed that the United States needs the means to accomplish these homeless missions (even if debate continues over exactly when and where it should perform them), the U.S. government is not well structured for these jobs.
>
> Many of the homeless missions, although apparently unrelated, have a key element in common: they cut across different cabinet departments and require the coordinated actions of several agencies. This is hardly surprising, since the problems they address do not respect neat distinctions between foreign and domestic threats, military and economic remedies, or states of war and states of peace. Such distinctions are outdated and merely reflect what the world was like in the era after World War II, when the American national security establishment was founded. It is due to such distinctions than no one agency is automatically in charge of these missions or responsible for developing and directing the capabilities they require.[1]

The nation is still struggling with the organization and management of the "homeless mission" of homeland security. For eight months we have had an Office of Homeland Security (OHS) in the White House, and for some days a proposed Department of Homeland Security (DHS). Congress has long ago proposed an architecture containing both these ingredients. I would agree that both are needed to make a home for this mission, but each has a distinctive role to play. The main points made below are:

- Creation of a DHS in no way supplants the paramount need for a strong White House OHS.
- The key White House OHS role is that of *architect,* devising an investment program to build *new* homeland defense capabilities, not "coordinating" the inadequate capabilities that already exist.

- Establishment of a DHS will not bring order to the border, transportation, and emergency management functions unless the reorganization is aggressively implemented.
- DHS should not just bring order and focus to existing functions, but should accomplish new functions, especially development and practice of new types of "intelligence" and new technology and techniques for homeland security.
- Several new types of "intelligence" – red teaming, intelligence of means, countersurveillance, and risk assessment – that should be practiced by the department will be the focus of my oral statement.

**THE ROLE OF THE OFFICE OF HOMELAND SECURITY**

Coordinating the old versus building the new. The announcement of an intention to create a cabinet-level Department of Homeland Security should in no way obscure the paramount need for a strong White House hand over *all* aspects of homeland security. It remains unresolved how this function will be exercised.

Governor Tom Ridge's charter for the Office of Homeland Security uses the word "coordinate" 29 times to describe what its authors imagined was the essence of his managerial task. Much of the commentary on OHS's slow start has focused on the strength of Ridge's power to coordinate and the supposed fallacy that a White House staffer, however close to the President, can effectively do so.

A larger fallacy lies in the idea that "coordination" describes what the nation in fact needs. The nation's capabilities for homeland security, even optimally coordinated, are simply not adequate to cope with 21st century terrorism. What is needed is far less a coordinator of what exists than an *architect* of the capabilities we need to build. All the managerial models advanced and tried over the past decade for counterterrorism – coordinator, czar, lead agency – have made this mistake. The result is a "come as you are party" in which each agency shows up with whatever capabilities its previous history happens to have bequeathed to it. Tom Ridge needs to position himself as the architect of new capabilities. Only then will his OHS add value and leave a legacy.

As architect, Ridge would first identify needed capabilities and then assign resources to the various agencies to build those capabilities. Where no agency naturally forms the right base to build on, the architect would recommend new agencies. The result, schematically, would be a multi-agency, multi-year investment and management plan that can be arrayed on a spreadsheet as in Figure 1. (Even though the Congress budgets annually, a multi-year program plan is a common and essential tool in procurement management.)

Figure 1 is what we should expect from Tom Ridge. He should create it in collaboration with OMB, take it to the president for approval, and ensure that the president directs his cabinet officers to prepare their budget submissions in accordance with the plan. The Congress has the last word, of course, but experience demonstrates that Congress tends to make only marginal adjustments to a coherent program plan that has presidential backing.

**Figure 1. Dimensions of a Homeland Security Program: The Architect's Plan.**

| | Intelligence & Surveillance | Prevention | Protection | Interdiction | Response & Recovery | Attribution | Analysis & Invention |
|---|---|---|---|---|---|---|---|
| **Justice/FBI** | | | | | | | |
| **Defense** | | | | | | | |
| **Intelligence** | | | | | | | |
| **Health and Human Services** | | | | | | | |
| **Border** (Coast Guard, Border Patrol, Customs, Immigration, etc.) | | | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **FEMA** | | | | | | | |
| **Other** (Energy, Transportation, Agriculture, State, etc.) | | | | | | | |
| **New Federal Agencies (DHS) and Nonprofit Institutions (e.g., FFRDCs)** | | | | | | | |
| **State and Local Government** (supported by federal grants) | | | | | | | |
| **Private Sector** (via regulation, subsidy, and indemnification) | | | | | | | |

Alas, the money gets appropriated whether there is an architect and plan or not. The FY03 budget provides a clear example, where $38 billion is apportioned largely on the basis of agency and congressional initiatives rather than any overall investment plan emanating from the White House.

Equipping the Office of Homeland Security to do the job. Producing the investment plan represented in Figure 1 is no small job. It cannot conceivably be done by a small White House staff, however talented and focused. To be capable of producing a plan of the requisite scope and complexity, OHS will need an organic analytical and planning capability like RAND provided to the Air Force in the 1950s, the MITRE Corporation provided to the Sage continental air defense system, and the Aerospace Corporation has provided to the Air Force and NRO for space. Without such a new not-for-profit institutional founding, OHS cannot do the job.

A reasonable approach to the task of investment planning is provided in the forthcoming report of the National Academy of Sciences Committee on Science and Technology for Countering Terrorism. It examines the vulnerabilities associated with each of the following infrastructures:[2]

- *Human, animal, and agricultural health system*;
- *Toxic/explosive materials and food/water storage, production, and distribution systems*;
- *Nuclear and radiological hazards*;
- *Information Technology (IT): Communication, Data, and Identification systems*;
- *Borders, Transportation and Distribution systems*;
- *Energy Systems*;
- *Physical Infrastructure, Cities, Buildings, and Important Events*;
- *Linked Vulnerabilities, Simulation, and Modeling*. This category covers the important interrelationship of different infrastructures which depend upon one another. For example, the energy distribution system depends on an IT system which controls power generation, distribution, and switching. Simulation and modeling are used to analyze and predict the technical response of society's complex and interrelated infrastructures to terrorist attack.
- *People*: This category refers to quality of life and morale, as opposed to physical health and safety, and deserves separate consideration.

The National Academy report then identifies countermeasures that can be taken to alleviate these vulnerabilities throughout all the phases of a hypothetical terrorist attack: intelligence and surveillance, prevention, protection, interdiction, response and recovery, attribution, and analysis and invention.[3] Deploying the countermeasures becomes the basis for the investment program plan of Figure 1. It is clear that this job requires breadth of technical knowledge and independence from interests that might be disadvantaged by its findings, characteristics of a new non-profit institution.

Washington spending versus state and local spending: the theory of fiscal federalism. Many of the investments needed for homeland security that the architect will identify must be made in state and local governments. After all,

terrorist incidents affect first and foremost a particular locality in which the target is located, and the police, fire, emergency management, and other public officials there will be the first on the line. It is not practical for each locality to develop its own comprehensive response to the possibility of terrorism or to engineer protective systems, let alone to develop new tactics, techniques, and technology. Creating common solutions to local homeland security challenges is therefore a logical task of the federal government. The federal role in creating common solutions and providing them (with partial funding) to state and local authorities, or to collective bodies such as associations of governors, fire chiefs, and police chiefs, will be a key task for the architect to sort out. In federalism terms, homeland security will end up somewhere in between education, where everyone talks about it and does research on it at the federal level but the real action is local, and national defense, where all the action is at the federal level.

Spending on homeland security by the private sector. The architect also needs to take account of the fact that the critical societal infrastructures that are the target for the terrorist are largely owned and operated by the private sector, not government. Much of the needed investment and adaptation to protect these infrastructures will have to be made by private companies. The funds for these investments will need to come from some mixture of funds provided by the federal government and funds provided by the companies themselves. The private sector's own investments will arise in several ways, either because they are mandated by law or regulation, or because incentives are provided (e.g., tax relief), or because insurance companies require them, or because competitive business practices recommend them. The experience of the "energy crisis" in the 1970s, when similarly large and pervasive investments were seen as needed, provides a useful caution here: the key will be consultation between the architect and private parties. This is another key role for the White House architect.

Mobilization and sunset. Finally, the architect should attend to the legal foundation of the U.S. counterterrorism effort. In that connection, the concepts of mobilization and sunset should prove useful. Until the mid-twentieth century, successful prosecution of war depended on the ability to mobilize nations and armies. A similar concept can apply in the war on terrorism. In the face of reasonably credible and specific information about actual or imminent mass terrorism, extraordinary measures might be advisable that are undesirable when there are no such warnings. In an emergency, the government will assume special authorities, restrict movement and other freedoms, and impose economic disruptions as the nation hunkers down. It is important to the quality of civil society in the long run that this mobilized state be clearly distinguished in statute and procedures from "normal" times when catastrophic terrorism is an ever-present, but not specifically anticipated, contingency. Experience in the United Kingdom during its century-long struggle against Irish terrorism suggests that even in liberal democracies powers granted to the government in the name of imminent terrorism are seldom rescinded when the threat recedes.[4] It is therefore important to write into any statute or regulation conferring extraordinary powers on the government a sunset clause describing the time and method of demobilization, placing the burden for extending the mobilization squarely on the government's ability to produce credible and specific information of imminent threat.

**THE ROLE OF A DEPARTMENT OF HOMELAND SECURITY**

Three Provisos. A DHS can be a constructive addition to the federal architecture, but only subject to three provisos.

A Department of Homeland Security is an appropriate ingredient or output of the architect's plan, but not a substitute for the architect. While the proposed DHS contains much, it also omits much – the CIA, DOD, and FBI, in particular. An architect is needed for *all* the agencies involved. The first proviso is that the founding of the DHS not be viewed as supplanting the OHS.

This second proviso is that the administration successfully complete the reorganization of the border, transportation, and emergency management agencies that are supposed to go into DHS, improving their management and focusing them on their new priority. Most reorganizations in the federal government are only partially completed. Agency heads, after first fighting the merger, will next aim to send their weakest performers to the new agency and keep their very best. Temporary inconveniences associated with reorganization – moving people into new office buildings, for instance – will be argued as detracting from day-to-day pursuit of the urgent mission of homeland defense. Government unions, strong in some of the agencies proposed as part of the new DHS, will scrutinize personnel policies. Congress will

need to disband influential committees with established relationships to constituencies. All this is necessary but difficult. A reorganization done halfway could make things worse.

The third proviso is that the DHS do truly new things and not merely gather together old functions under one roof. The new department's most important contributions could be in intelligence analysis and science and technology. Indeed, two of the four proposed undersecretary positions in DHS are assigned these functions; the other two undersecretary positions are in charge of aggregating existing border/transportation and emergency management functions, respectively.

Developing and Practicing Alternative Conceptions of "Intelligence". There is considerable debate in Washington over whether the United States could plausibly have "connected the dots" leading to 9/11. Useful insights have emerged from this debate. One insight is the danger of continuing to separate foreign and domestic intelligence related to terrorism, the institutional reflection of which is the separation of the national security and law enforcement functions. Steps are underway to bridge this historical chasm. Another insight, stressed by the Attorney General and FBI Director, is the need to encourage and reward FBI agents to prevent terror crimes from happening in the first place rather than "solving" them after they have occurred.

However, these important insights, and most of the debate over intelligence, conceive of intelligence as perpetrator-centered and event-focused: locating individuals associated with terrorism and uncovering their plots. Debate centers on whether those collecting such intelligence, chiefly the CIA and FBI, are sharing the information. There are, however, other concepts of "intelligence" of great potential importance to homeland security which, at first approximation, are not currently accomplished *anywhere* in the federal government. A clear and valuable role for the new DHS would be to develop and practice some of these "intelligence" techniques, among them red teaming, intelligence of means, countersurveillance, and risk assessment.

RED TEAM/BLUE TEAM. Most Americans were probably not shocked to learn on September 12 that the U.S. government did not have advance information about the dozen or so individuals residing in the country who plotted and took part in the airline suicide bombings of September 11. They probably were deeply disturbed to learn, however, that the government was as heedless of the tactic used as it was of the perpetrators. The airline security system inspected for guns and bombs, not knives; aircrews were trained to deal with hijackers who sought hostages or conveyance to Cuba, not kamikaze attack. In retrospect, a huge gap existed in the U.S. air safety system. Terrorists detected it before the security system did—and exploited it.

To avoid tactical surprise of this kind, the homeland security effort needs to adopt a standard mechanism of military organizations: competing red and blue teams. The red team projects itself imaginatively into the terrorist's shoes and tries to devise attack tactics. The blue team tries to design countermeasures. When the United States developed the first stealth aircraft, for example, the air force created a red team to try to detect and shoot it down. When the red team identified a weakness in the stealth design, the blue team was charged to fix it, systematically balancing risk of detection against the cost and inconvenience of countermeasures.

A comparable red/blue team mechanism should be the central feature of the program for homeland security. To work, the mechanism must be systematic and institutionalized, not ad hoc. It must be independent of the interests —airlines, for example—that stand to be inconvenienced by its findings. It must have the money to conduct experiments, tests, and inspections, not just paper studies. It must be knowledgeable about the technologies of terrorism and protection. Above all, it must be inventive. These criteria all argue for a new institutional founding outside of, but close to, government – a sort of "national laboratory" for homeland security.

INTELLIGENCE OF MEANS. Surveillance of the *means* that terrorists could employ is potentially more important than surveillance of *persons* who might be terrorists, and raises far fewer civil liberties issues. Placing all Middle Eastern male noncitizens who reside in the United States under surveillance, for example, is both objectionable and impractical. But inquiring after all those who take flying lessons but are not interested in learning to take off or land, who rent crop dusters, or who seek information on the antibiotic resistance of anthrax strains or the layout of a nuclear power plant is feasible and extremely useful.

Likewise, it is undesirable to restrict access by citizens to the Capitol building and congressional office buildings, but there is no fundamental technical barrier to seeding these buildings with sensors that would promptly, and with a low rate of false alarms, detect the presence of anthrax on surfaces and in ventilation systems. Nuclear weapons are much harder to detect, but the streets in the vicinity of the White House could be laced with sensitive detectors that would stand a good chance of detecting a nuclear weapon or radiological weapon. Although these detectors would individually have a high rate of false alarms, when networked so that their outputs are correlated in space and time, they could comprise an effective warning system. Such a system is preferable to registering truck drivers or other methods of surveilling persons in the White House vicinity.

COUNTERSURVEILLANCE. The concept of countersurveillance is illustrated by a tactic that has proved very useful in embassy and force protection. In its crudest form, someone stands on the roof of the embassy and looks for people who seem to be conducting surveillance of the embassy. Does a certain car pass by more than once; is someone photographing architecturally unnoteworthy features of the compound? "Honey pots" are another example of countersurveillance: label a web site "CIA Director Personal Files" and see who visits. The point of countersurveillance is to estimate the information a terrorist would need to plan an attack, and then to look for people collecting that data.

RISK ASSESSMENT. For the architect to complete his investment program plan, he must decide where additional funds can make the most impact on protecting the homeland. Such risk assessment involves ordering terrorist scenarios according to how destructive they are, how likely they are, and how expensive and disruptive protective countermeasure would be. The gravity of a terrorism scenario is measured both by "hard" variables (loss of life, damage to property) and "soft" variables (disruption of society's key functions, injury to the population's way of life and overall peace of mind). One indicator of likelihood is the ease with which the act of destruction or disruption can be accomplished. Does it require many terrorists acting in concert, or will just one person suffice? Does it require the complicity of an "insider" who is part of the conspiracy – a nuclear reactor operator, say, or a computer network administrator? Do the means entail a large expenditure of funds, a complex organization, or sophisticated technology that only a nation-state or an established terrorist network could assemble, or is the scale of effort such that someone could undertake it in his or her garage? The final risk analysis arrays the scenarios against the countermeasures, technical and procedural, that could be deployed to thwart the terrorists. The result of balancing risk and cost is an investment portfolio in protection.

Marshaling Science and Technology. While the advance of science and technology (S&T) is the reason that terrorism has the potential to be catastrophic in the 21st century, S&T is also America's critical tool for safeguarding society against that threat.

America surely has weaknesses compared to other societies when it comes to facing terrorism. Its vulnerability is connected to many of the characteristics that its people also treasure: openness and mobility, freedom and personal initiative, and an emphasis on economic efficiency that relies on complex and technologically advanced social systems. America likewise has several inherent strengths as it approaches reducing this vulnerability – its immense size and wealth, its high level of education, its political cohesion and values.

But a critical comparative advantage of this country in facing challenges has traditionally been its strength in science and technology. In traditional national security affairs, for example, S&T has long been the key to America's preeminence. During the Cold War, the United States decided that it could not match the Soviet Union and its allies man for man, or tank for tank, in the defense of western Europe. Moreover, Warsaw Pact forces could invade from territory contiguous with western Europe, whereas U.S. forces were separated from the battlefield by an ocean. Finally, neither the United States nor its allies wished to live perpetually on a war footing like the Soviet Union. The solution to these military disadvantages was to offset them with superior U.S. technology – precision munitions, stealth aircraft, spy satellites, and so on. Since the end of the Cold War, the United States has continued to rely on S&T to give this nation an asymmetric advantage that offsets an opponent's superior number of soldiers, favorable geographic access to the battlefield, and greater willingness to accept casualties and to impose sacrifice in the citizenry – whether Saddam Hussein's Iraq in 1991 or Afghanistan's Taliban in 2002.

In the effort to counter catastrophic terrorism, as in traditional military affairs, S&T can offset the vulnerabilities that unavoidably arise from America's best characteristics of openness, freedom, and economic efficiency. In many cases, S&T provides vital alternatives to other protective measures that, were we forced to adopt them, would alter the quality of American life.

DHS therefore needs to develop a strong contract research program. Much of this program should cover entirely new technology, but it should be coordinated with ongoing research, especially that sponsored by DOD.[5]

Conclusion. The United States is at the beginning of a long process of adapting to the threat of terrorism. Our key objective must be to build new protective capabilities we do not now have. That objective is more important than optimizing the capabilities we do have. It can only be accomplished by an architect in the White House. A Department of Homeland Security can complement but not replace the White House architect. Besides providing managerial focus for the border, transportation, and emergency response functions, the DHS should make entirely new contributions to homeland security through a widened conception of "intelligence" and by harnessing American inventiveness in science and technology.

---

[1] "Keeping America's Military Edge," *Foreign Affairs*, January/February 2001, p.94.

[2] Specifically, the examination of each infrastructure covers three aspects:

- Each infrastructure can serve as a *target* for terrorism. For example, the World Trade Center buildings of New York served as the target of the September 11, 2001 airline attacks. The human health system was the target of the anthrax mailing attacks of the same months.
- Some infrastructures can also serve as a *means of attack*. For example, on September 11, 2001 the transportation system – airliners – served as a weapon to attack another infrastructure, the buildings of the city of New York. A system of distributing goods – the mails – served as the means of anthrax attack.
- Other infrastructures serve as a critical part of the *response to attack*. The information technology (IT) system, for example, is vital for coordinating emergency response, law enforcement, and military operations. The IT system is also necessary for informing the public in an emergency. Terrorists might select the infrastructures that are essential to response as part of their attack. For example, spread of a biological warfare agent might be accompanied by a cyber attack on the Internet and 911 systems.

[3] *Intelligence and surveillance* involves surveillance of persons, groups, and motives—a delicate matter—but also surveillance of potential means of destruction such as fissile materials or germ cultures.

*Prevention* involves addressing the motivations for catastrophic terrorism where possible, but in any case keeping the means of mass destruction out of the hands of potential terrorists. Safeguarding fissile materials and preventing the hijacking of airliners are examples of prevention.

*Protection* is needed in case detection and prevention fail. In military parlance, protection means "hardening the target" so that destruction or disruption becomes harder for the terrorist. Examples of protection are making borders, buildings, airplanes, and critical infrastructures more difficult to breach, disrupt, or destroy through technical design and procedures. Protection might also mean making people more resilient to disease through vaccination and other public health measures.

*Interdiction* or "crisis management" seeks to disrupt and destroy potential perpetrators of catastrophic terrorism and their base of support before they can mount an attack, as in the current campaign against al Qaeda in Afghanistan.

*Response and recovery* or "consequence management" means containing and limiting the level of damage and the number of casualties by organizing emergency response, public health measures, and restoration of critical functions in the aftermath of a terrorist attack.

*Attribution* refers to the capability to find the perpetrators of an act (e.g., by typing an anthrax culture or performing radiochemical analysis of nuclear bomb debris) and choosing retaliation, prosecution, or other response.

*Analysis and invention* involves the systematic learning from incidents that do occur, studying terrorist tactics and devising countermeasures through "red team versus blue team" exercises, understanding motivations and modes of deterrence, eliminating vulnerabilities revealed through past attacks, and developing systematic plan for ongoing operations, future investment, and scientific and technological innovation.

[4] Laura K. Donohue, "Civil Liberties, Terrorism, and Liberal Democracy: Lessons from the United Kingdom," BCSIA Discussion Paper 2000-05, ESDP Discussion Paper 2000-01 (Cambridge, Mass.: Belfer Center for Science and International Affairs and Executive Session on Domestic Preparedness, John F. Kennedy School of Government, Harvard University, August 2000).

[5] The Bush administration has so far left the role of DOD in homeland security unclear. While traditional military tools are not appropriate for most aspects of homeland security, the Department of Defense has enormous resources of potential value. These resources arise in the normal course of DOD's principal mission of conducting joint military operations against foreign opponents. Many of these resources are technical. For example, DOD will be developing technology for detection of and protection from chemical and biological threats as a necessary part of its principal mission. Deployed

forces are a prime target of terrorists, and DOD's protective efforts (called "force protection" by DOD) have much of the same technical content as homeland security. Many of the industrial and technical projects undertaken for homeland security will probably be awarded to firms that do defense work, since these firms have the large systems engineering capabilities required and they are accustomed to doing government contract work. Given the likely scale of these DOD efforts and the overall size and
quality of the DOD technology and industrial base, it is important to find a role that makes best national use of the defense asset for homeland security.

DOD has taken some preliminary steps to adapt its structures to contribute to homeland security. A Northern Command was established to vest responsibility for DOD operational support to homeland security in a single joint Commander in Chief (CINC). At this writing, Northern Command combines two principal entities from DOD. The first is the U.S.-Canadian North American Aerospace Defense Command, responsible for, among other things, shooting down commandeered airliners. The second is the Army's role as executive agent for DOD support to domestic agencies; this has long been DOD's office for coordinating such measures as provision of airlift to convey supplies in disaster relief situations. From these initial ingredients DOD expects to develop Northern Command as the DOD focal point for whatever the executive branch determines is an appropriate operational role for the military in homeland security.

The Department of Homeland Security should carefully coordinate its own technology efforts with such DOD programs as those of the Defense Advanced Research Projects Agency, the Defense Threat Reduction Agency, the Chemical and Biological Defense Program, and the U.S. Army Medical Research Institute of Infectious Diseases -- all of which will be carrying out closely related and large-scale technology efforts.