The Markle Foundation
Task Force on National Security in the Information Age

Protecting America's Freedom in the Information Age

A Report of the Markle Foundation Task Force

October 2002

A Project of

The Markle Foundation,
New York City

In Alliance with

Miller Center of Public Affairs,
University of Virginia

The Brookings Institution,
Washington, D.C.

Center for Strategic and International Studies,
Washington, D.C.

TABLE OF CONTENTS

OVERVIEW

The geographical boundaries of national security have changed. America has become a potential battlefield for major assaults. Yet, though our military has deeply integrated intelligence and information technology into war fighting, we have not developed a similarly sophisticated use of information and information technology to protect Americans from attacks at home.

Information analysis is the brain of homeland security. Used well, it can guide strategic, timely moves throughout our country and around the world. Done poorly, even armies of guards and analysts will be useless. The Task Force that we had the privilege of chairing has reached some important conclusions to assist our nation in developing its information collection and analysis capabilities.

The federal government is preparing to spend nearly $40 billion a year to protect the homeland. While this report takes no position on any pending legislation, the White House has developed the important concept of homeland security, the centerpiece of which is the Department of Homeland Security (DHS). But almost no dollars have been directed to creating the capacity for the sharing of information and integrating the way it is analyzed, so that out of information collection comes enhanced knowledge. Neither the White House nor the current appropriations pipeline for the new Department of Homeland Security have yet identified the money to turn information collection into knowledge.

With even relatively small sums of money, however, tremendous gains can be made. The new Department of Homeland Security can be the central hub for decisions about what information needs to be collected and stored—in the government or in the private sector—and about where the information should be analyzed and how. The DHS can help develop rules for protecting the well-established liberties of our citizens when information is collected and used. And it can support meaningful research and development efforts. This report describes how. To protect our freedoms, our task—as in previous generations—is to craft the national framework that will draw on this generation's and this society's greatest strengths.

To protect freedom, America's physical safety is essential. Protecting freedom also requires securing the values that define America, including the civil liberties and rights to privacy that make our country special. Rights go together with responsibilities in preserving the public order in which our values can flourish. When Americans feel they must start trading fundamental rights in return for more security, we will know our national security policies are failing. The rule of law is our strength.

Fortunately, to paraphrase John Paul Jones, we have not yet begun to fight. We have not taken adequate and thoughtful advantage of the laws and resources that are already available. We have barely begun to create a serious domestic intelligence capability, one that learns from the abuses of the past and uses the powers that can already be brought to hand.

We have not yet begun to mobilize our society's strengths in information, intelligence, and technology. The Task Force agrees that the U.S. government needs the proposed Department of Homeland Security. But, to us, the most compelling argument for the DHS is that it is a necessary foundation for building entirely *new* capacities for national action. We need to train people, sponsor research, and cre-

ate systems that use information in new ways, finding smarter and more cost-effective strategies that provide both real security and real accountability.

Meanwhile, every agency is rushing out to collect information and buy technology for its own stovepiped systems. As they do so, with congressional and citizen watchdogs trying to chase them across the political countryside, one Task Force member spoke for the group when he warned that, "We may end up getting all of the disadvantages of invasion of privacy with none of the national security gains."

Instead of matching unguided power with unfocused oversight, there is a better approach that borrows from best practices in public and private management: telling officials what they *can* do, as well as setting the limits on their power.

Start by spelling out the kind of information and analysis the country really needs. The solutions start in the way people think and work together. This report illustrates the kind of roadmap that can guide them.

Technology is not a panacea. Those who have called for endless mining of vast new government data warehouses to find intricate correlations are not offering the promise of real security. They instead evoke memories of the walls of clippings collected by the paranoid genius, John Nash, in *A Beautiful Mind*.

Knowledge of the world and those who would do us harm is what is needed. Knowledge does not come from the accumulation of random data, but rather it is found in thoughtful and informed inquiries. Great progress can be made just with sensible, straightforward use of relatively simple tools and already-collected data. Inexpensive data checks, strategically planned, should have been able to prevent the 9/11 attacks. Yet, then, the government lacked the capacities to perform them. Now, more than a year later, the government still has not acquired them.

With this improved definition of the analytic task, the President should issue well-crafted operating guidelines for all federal agencies to encourage confident performance. Only the President can establish and be accountable for the proper balance between development of domestic intelligence and preservation of liberty. These guidelines can embed respect for essential values into the very fabric of the institutions—their core training and their routines. Those guidelines should provide transparent focal points for strong, constructive oversight and proper accountability, both within the agencies and from outside.

America will make a mistake, however, if we create a centralized, "mainframe" information architecture in Washington, D.C., rather than the networked, decentralized system that is needed to defeat the challenge of decentralized, sometimes networked adversaries. The problem is not just information sharing among federal agencies in Washington, D.C. Most of the people, information, and action will be in the field—in regional or local federal offices, in state, regional, and local governments, and in private firms. The federal approach and guidelines can inform and support these local efforts, but information needs to be available widely and should not be required to flow through a central hub.

That is why the information management challenge is also organizational. Our country's leaders should set up the new Department so that it will empower local efforts, nationally coordinated. Promising, innovative local efforts are already springing up across America. To use the power of a net-

work, rather than rely on a mainframe, the federal government must build an operating system that can harness the distributed power of local, state, and federal officials and analysts across the nation. And it needs to be able to integrate information developed from around the world through our foreign intelligence capabilities. This report outlines the organization and the network architecture to do the job.

One aspect of the organizational problem is to sort out the roles of key federal agencies, especially the Department of Homeland Security and the FBI. Our Task Force's basic conception is that the Department of Justice and its FBI should be the lead agencies for law enforcement, exercising the power to investigate crimes, charge people with crimes, perhaps take away their liberty, and prepare cases for trial and appeal. The DHS should be the lead agency for shaping domestic intelligence products to inform policymakers, especially on the analytical side, so that there is some separation between the attitudes and priorities of intelligence analysis and the different, more concentrated, focus of law enforcement personnel authorized to use force on the street to make arrests and pursue or detain citizens.

We understand that criminal investigation (and counterintelligence) often overlaps with intelligence work. Some overlap is natural and good. But the case for a fundamental separation is strong. Intelligence has much broader purposes than criminal investigation. The operational objectives are different. The training is different. The rules about how to collect, retain, and share information are different. The relationships with sources of information are different.

Therefore the DHS should take the lead in collecting information that is publicly available or voluntarily obtained and in analyzing domestic information and intelligence from all sources and setting overall priorities for new collection efforts, working within an interagency process that will include the FBI and other relevant agencies in the intelligence community. It should coordinate the national organization of homeland security task forces in states, regions, and metropolitan areas across the country. But the FBI should continue to have the responsibility for managing clandestine collection operations, like FISA wiretaps or the recruitment of undercover agents, under the supervision of the Attorney General.

The DHS must also develop science and engineering strengths to be able to incorporate advanced technologies that are available in the private sector. This will require procurement practices and private sector expertise that facilitate knowledgeable evaluation of promising capabilities. In addition, the DHS should be able to stimulate progress in IT areas where national needs are great, yet not well served by market forces.

We commend this report to those in government, business, and non-profit communities who feel responsibility for protecting America and to all of our citizens, who play such a key role in ensuring the strength of our nation.

Zoë Baird   James Barksdale

Acknowledgments

This Task Force commenced its work with a plenary meeting in April 2002. In our six months of work, we have been greatly encouraged by the priority and resources that the federal government and many state and local authorities have devoted to tackling the challenge of improving the potential of information and information technology to enhance our national security. We have therefore tried to develop a truly national framework, fusing this energetic outpouring of patriotic effort into a broad plan of action.

Our Task Force addressed the following questions, to develop a new national framework:

1. What information and which analytic methods do we need most in order to protect Americans at home?

2. How can government better employ the best private sector practices in managing information and developing technology?

3. How should the U.S. government task its agencies to more effectively gather, analyze, and use the national security information it needs, working with the private sector? And what new boundaries to such deployment of information are needed to protect essential liberties?

We organized three working groups to help develop our analysis of these questions, led respectively by Task Force members James Steinberg, Abraham Sofaer, and John Hamre. John received particular help in his working group from Mary DeRosa. These working groups then refined and presented their views at another plenary meeting of the Task Force, held in July 2002. (Their final working group papers are in Part Two of this Report.)

As the report then took shape, we created two additional working groups to take on even more specific tasks. One, on "Connecting for Security," was led by Tara Lemmey; the other, developing illustrative guidelines on "Collection, Use, and Analysis," was led by William Crowell. The efforts of those two working groups are incorporated directly into the Task Force report itself, as readers will see.

This report is not the final work of the Task Force. As governments and citizens around the country create new institutions and guidelines, perhaps along some of the lines we suggest, a series of new challenges will arise calling for more specialized technical, political, and legal assistance. The Task Force will continue to facilitate that phase of construction, helping build structures to use information to protect our freedom in the 21st century.

Our executive director, Philip Zelikow, provides exceptional drive and intellect. He joins us in acknowledging the contributions of an extraordinary staff. Mary McKinley runs the operation. Ryan Coonerty and Laura Rozen handle government relations and provide key substantive research and analytical support to the working groups. Wistar Morris oversees the project for the Miller Center Foundation.

Garth Wermter is a resource on technology issues, and Karen Thomas provided an excellent platform on the Web for the Task Force's work. Ann-Woods Isaacs, Chris Freise, and Courtney Stephens work day-to-day to support the Task Force members and staff.

James Lewis of CSIS has been a great asset to our work. At the Markle Foundation headquarters in New York City, we thank Stefaan Verhulst for his thoughtful research assistance, Peter Kerr for his contribution to ensuring that this report contributes to the public's education on these issues, and Karen Byers for her financial management.

Zoë Baird   James Barksdale

PART ONE:
THE TASK FORCE REPORT

The Task Force Report

Many Americans understandably believe that technology is the source of America's military and economic power. They believe this so much that they often seek technological solutions to essentially human problems. But America's technological achievements—in weaponry, commerce, and science— are merely the reflections of strengths in our society, a society that has evolved and is organized supremely well to unleash and promote human initiative. Though we need technology to secure our nation, a successful domestic intelligence and information strategy should start with the way we organize our people to take advantage of innovation.

The way we obtain and use information will determine how well we can protect freedom while striving to attain the objectives set forth in the President's National Strategy for Homeland Security, to:

- prevent terrorist attacks within the United States;

- reduce America's vulnerability to terrorism; and

- minimize the damage and recover from attacks that do occur.

Our vision starts with development of a networked and national homeland security community in agencies, firms, and neighborhoods. In connecting for security, we outline the elements of a next-generation national security infrastructure. We also discuss the organization of domestic intelligence collection and analysis in Washington, D.C., within a framework that respects our nation's traditions and civil liberties.

The problem is broader than just collecting and sharing information. It is the challenge of using information effectively, linking collection with sound and imaginative analysis derived from multiple perspectives and employing cutting-edge technology to support end-users, from emergency responders to Presidents. In other words, we need to *mobilize* information for the new era of national security we have entered.

Domestic intelligence has a deservedly bad reputation in America. Yet we nonetheless believe the country now needs a serious capability to analyze domestic intelligence. In the past we drifted into such serious undertakings through wartime directives and unchecked agency initiatives. Now we should learn from our history and foreign experiences to move ahead thoughtfully and deliberately. To take our civil rights seriously, right from the start, we can chart a path for protecting freedom. To take domestic intelligence seriously, we must address the specifics of the analytical work that needs to be done. To link analysis to action, we give some illustrations of how information can empower people in the field, while also recommending guidelines to protect American liberties, not just American lives.

We also suggest how governments at all levels can form a more effective partnership with the private sector. Some key government agencies have been demonstrably unable to meet the challenge of securing the best information technology. The new Department of Homeland Security must be able to enlist outside expertise. We can tap the best practices found in our private sector. From basic research to product development to acquisition, there are specific reforms that can leverage the power of information to safeguard our freedom.

A Networked and Nationwide Analytic Community

At the working level in the federal agencies in Washington, D.C., the problem of information and homeland security has been seen, first of all, as a problem of buying new technology. At least that is where practically all the federal money is being spent, like the $300 million for the Information Technology Initiative in FBI's budget for Fiscal Year 2003, a multiyear $1 billion plan for the new Transportation Security Administration's information technology infrastructure, the five-year $550 million plan for the Immigration and Naturalization Service, the $6.9 billion Navy and Marine Corps Intranet system, and the $2 billion "Project Groundbreaker" of the National Security Agency. In fact, according to the White House, the federal government spends a total of about $50 billion a year on information technology.

That may be a good thing. Perhaps even more money should be spent. But while such sums are being spent to modernize each agency's own information systems, some of it relevant to homeland security, almost none of this money is being spent to solve the problem of how to *share* this information and intelligence among theose federal agencies. To be fair, we acknowledge that agencies inside the Department of Defense do spend money on sharing data with each other. On a lesser scale, agencies inside the community of foreign intelligence agencies, like the CIA, also invest in sharing data with their colleagues in the Pentagon and the National Security Agency. But when it comes to homeland security and using integrated information systems, adequate efforts and investments are not yet in sight.

In its $38 billion FY 2003 budget request for homeland security, the administration requested only $200 million for information integration, and is having trouble getting even that. The administration originally sought to create an Information Integration Program Office in the Commerce Department. That faltering effort is now being superseded in hopes of creating such a program in the new Department of Homeland Security. The White House Office of Homeland Security and the Office of Management and Budget are developing promising plans and using their powers of persuasion to realize them. But they need money to make their plans become reality, and money to give agencies positive inducements to cooperate, and the money is not there.

Washington, D.C., is important. It is where foreign and domestic information can often come together, a place where varieties of domestic, foreign, law enforcement, and military information can readily be combined, and where central coordination of a national community can be organized. If anything goes wrong, the spotlight will be on the President. It is up to him to set the expectations for the strong but balanced system we will need. But such a system cannot be based in or directed just from Washington. The President needs to set an expectation and design a system that is truly national and decentralized.

Most of the real frontlines of homeland security are outside of Washington, D.C. Likely terrorists are often encountered, and the targets they might attack are protected, by local officials—a cop hearing a complaint from a landlord, an airport official who hears about a plane some pilot trainee left on a runway, an FBI agent puzzled by an odd flight school student in Arizona, or an emergency room resident trying to treat patients stricken by an unusual illness.

Seen from New York, or Texas, or Utah, or California, the homeland security picture is very different. Those officials think *they* are the ones who really manage homeland security. They have a point. Consider that:

- There are only 11,500 FBI agents; there are more than 50 times as many state and local law enforcers.

- There are only a few thousand professionals in the Federal Emergency Management Agency (FEMA); there are about two million potential emergency responders in the field.

- To work on domestic intelligence against terrorism, the FBI currently has only about a hundred analysts, even by the FBI's definition of the term. Meanwhile there are 40 counter-terrorism analysts just in the Los Angeles Police Department and the NYPD's analytic effort is larger still.

Seen from outside Washington, D.C., local leaders in law enforcement and emergency services have also realized that, although the necessary technology is often beyond what their budgets can afford, linking the right people together is even harder.

The intelligence and other information critical to homeland security will come from across the country and around the world. Washington, D.C., is a critical node in that network, but only one of many. To bring together this far-flung community of analysts and operators working directly on the problems is the real challenge.

Within the federal government we should focus on two key institutions to bring information together for "all-source" analysis. First, there is the Counterterrorist Center (CTC) based at the CIA. It is run as a service for the entire intelligence community by the Director of Central Intelligence. The CTC endeavors to bring together all the agencies concerned with gathering and acting on intelligence from other countries.

The second principal focal point should be the new intelligence analysis center that will be created in the Department of Homeland Security (DHS). This center should bring together relevant information from all sources within the United States, as well as foreign intelligence and open-source information gathered through the Counterterrorist Center. It should combine this information on threats with a mapping of America's vulnerabilities at home and plans to respond.

The DHS should become the base for building up a national community of intelligence contributors and analysts. To create a national infrastructure that is aware, robust, and resilient to the many challenges we face in the 21st century, we have to harness the power and dynamism of information technology by utilizing the strengths and mitigating the weaknesses of our networked society.

Connecting for Security

The technological advances that created and define the information age have primarily taken place in three arenas (the "three C's"):

- computation (raw computing power);

- communication (degree of connectedness); and

- caching (data storage).

The last 50 years have seen tremendous increases in the capacity of all three of these defining technologies of the information age. Computation tools have advanced from slide rules to pocket calculators to personal computers. Processor speeds have increased by many orders of magnitude. Memory and storage technology have advanced to the point where it is possible to archive previously undreamed of quantities of data. Just in the U.S., connectivity of the Internet has grown to include more than 150 million computer hosts, with far greater numbers connected from these hosts to the Net.

Analytic capacities have grown accordingly. For instance, the tremendous utility of increased processing power combined with increased storage capacity has had a noticeable impact on biotechnology, as the human genome project has made genetic data available online for sophisticated searches and data-mining, leading to new drug candidates and cures for genetic diseases. Everything from economic forecasting to weather forecasting has been significantly enhanced by increases in the capabilities of the three C's.

Just as important is the massive increase in interconnectedness that we have experienced in our daily lives. Dynamic, efficient networks dominate our environment and shape every facet of modern life (the power grid, financial networks, air-traffic and transportation networks, and, most recently, the Internet). Through these networks, moving things like words or money from here to there can be just a click away.

We are gaining a far better theoretical and practical understanding of the natural forms, inherent efficiencies, and inherent vulnerabilities of these interconnected relationships. Whole new areas of study and new scientific disciplines are springing up around these networks and network effects.

The threats to national security are also decentralized, networked, and dynamic. As the new Department of Homeland Security takes shape, we have a unique opportunity to design and implement systems that will enable the best use of central and local resources. We have learned a great deal from the rapid growth in networks of all types in recent years. We can draw on our accumulated knowledge and our existing networks to create a robust, decentralized, and networked national security framework.

As our society has grown more interconnected, communications networks have evolved. Traditional communication networks typically were hierarchical. Primary directories and data repositories were centrally located, with information flow regulated from the top. Emerging communications networks, though, tend to be peer-based, forming dynamic connections among individual participants at and often across levels of an information community. Directories and data repositories are frequently distributed and dispersed.

Participation in such networks can take many forms. Individuals act in a variety of roles, as part of changing organizations. In a national security infrastructure, local police officers, state health officials, and national intelligence analysts are all important actors in the network. Communities of practice—groups of participants in fields like public safety, transportation, agriculture, or energy—can also collectively act in a network. These communities benefit greatly from increased connections to those with similar roles in different organizations or at other levels. In addition, the collective community may come together as ad hoc workgroups, mobilized for specific tasks.

Ad hoc workgroups evolve as they respond to a particular challenge. Members may change in response to community needs. For example, a public health community might include state officials, local hospitals and the Center for Disease Control and Prevention, and in the case of a community with a vulnerable water system, might also include public utility commissioners, building inspectors, and watershed conservationists. In times of crisis, these groups might also involve school officials, transportation officials and the local Red Cross chapter.

These participants are not distinguished by their relationship to a central gatekeeper, but by their relationship to one another. In a distributed, decentralized network, they can, will, and should form unique and utilitarian relationships in order to best support their particular role in national security, whether in prevention, analysis, response, or protection. This peer-to-peer collaboration allows federal, state, and local participants to draw upon the collective expertise of the community.

In an environment of such great risks, empowerment of local actors will lead to better prevention or response management. What we face today is a global, multifaceted problem, and the tools for addressing the challenge may be dispersed among thousands of police officers, state public health officials, firefighters, emergency room staff, or soldiers.

Without waiting for instructions from Washington, D.C., we are already seeing these networks take shape in pioneering pilot efforts around America. Here are some examples:

- In hosting the 2002 Winter Olympics, Utah created a Utah Olympic Public Safety Command, handling dozens of venues and entry points. With resources from the State of Utah and the Pentagon's Defense Threat Reduction Agency, an extraordinary Incident Management System linked—in real time—local and state law enforcement, fire and emergency medical services, and a variety of federal and military agencies. It worked flawlessly.

- Using local resources from the FBI's InfraGard program (an infrastructure protection effort connected to the National Infrastructure Protection Center, now at the FBI but proposed for transfer to the DHS), the Dallas office of the FBI has created an Emergency Response Network that can receive law enforcement or emergency information from the public or any agency operating in north Texas and disseminate it in minutes to thousands of relevant offices through phone, e-mail, or pagers, all while immediately locating the best contacts organized by skills, duties, time of day, and proximity to the incident. The network already links about 500 local police and sheriff's offices, 33 federal and nine state agencies, all branches of the U.S. military, more than 30 fire departments, 15 different critical infrastructure systems, and more than 250 private corporations and organizations.

- The California Department of Justice has established the California Anti-Terrorism Information Center (CATIC) that links federal, state, and local law enforcement agencies throughout the state. CATIC helps organize special task forces, an all-source "situation unit" to analyze and distribute terrorist-related intelligence, and a group analysis effort striving for a broader understanding of terrorist incidents and how to prevent them. Running off RISS.Net (a law enforcement regional information sharing system), the California effort has attracted help from entrepreneurial officials at the Defense Intelligence Agency (DIA), who are connecting the California system to DIA and the New York City Police Department.

- The Houston Police Department and the local FBI's Joint Terrorism Task Force have helped create a Texas Coastal Region Advisory System (TCRAS) to support federal efforts to get homeland security related information to law enforcement and emergency service agencies.

- Within the Department of Defense, the Defense Advanced Research Projects Agency (DARPA) has created an Information Awareness Office that is developing a prototype system for "total information awareness." This system will integrate ideas and technology from more than eight individual DARPA R&D projects. The new Information Awareness Center is based at the U.S. Army's Intelligence and Security Command. That Command also supports the Army's Land Information Warfare Activity at Fort Belvoir, which Congressman Curt Weldon (R-PA), among others, credits with already having one of the most effective open-source data analytical capabilities in the intelligence community.

- Law enforcement officials in Pennsylvania have benefited significantly from JNet, a Java-based tool that can query police, parole, probation, corrections, and motor vehicle databases at the state and local levels. JNet is accessible to more than 2,800 state law enforcement personnel and is often used by federal officials to track suspects. JNet will soon be available to law enforcement officials statewide. But already it has been touted as a model for future information sharing infrastructures.

- The Los Angeles County Sheriff's Department has created a Terrorism Early Warning (TEW) group to connect law enforcement, fire, health, and emergency management agencies to circulate warnings, analyze possible dangers, check public health and epidemiological indicators, and manage possible consequences of a terrorism event.

These systems use various technologies and different standards to format and exchange data. What unites them and makes them successful models is that they have incorporated and expanded upon existing organizations and professional networks already working in their communities and regions. They took local needs, practices, and input into account. They are "ground-up," not "top-down." They are "integrated," not "stovepiped." As Dallas ERN Coordinator Art Fierro (an FBI special agent) told our staff, "We serve as an umbrella. We don't replace local business and infrastructure. We build and work through the networks and individuals that are already there." That is a start. What is needed now is national leadership to combine these experiences and knowledge into a truly national system.

Emerging Bush administration plans for homeland security information sharing envision a three-layer system, or enterprise architecture:

- The top layer would be comprised of top secret information drawn from sensitive sources or methods of collection. Dominated by foreign intelligence, this network would build on existing

intelligence community networks like "CT Link," connected by the Joint Worldwide Intelligence Communications System.

- The middle layer would have secret information, including military data. This network would use existing networks like "IntelLink," joined by the Defense Department's Secret Internet Protocol Router Network (SIPRNET).

- The bottom layer would contain unclassified information, including the actionable data fed down from the higher layers, and sending unclassified information upward. This information would principally be of a law enforcement or domestic character. Existing and emerging networks might be linked through some still undetermined mix of the Defense Department's Unclassified Internet Protocol Router Network (NIPRNET) or a single Web interface for the two main Justice Department networks for law enforcement—Law Enforcement Online (LEO) and the Regional Information Sharing Systems (RISS.net).

This planned system would be governed by the agencies that host the networks (like DOD for SIPR-NET), perhaps with some overarching guidelines supplied by the White House Office of Homeland Security and the new Department of Homeland Security.

While we welcome this emerging plan as a starting point, we believe that this concept is too Washington-centered, too hierarchical, and too narrow in its scope. It does not go far enough to take advantage of the distributed, networked concepts already becoming evident in some of the pilot projects mentioned above.

The federal agencies are rightly concerned about the security of this prospective network and the security of the data being shared on it. We understand the importance of protecting intelligence sources and methods as well as sensitive personal or law enforcement information. A balance must be struck. But we believe the current balance should tilt further in favor of using the power of networked information and analysis, letting much more varied ad hoc communities of practitioners work together without waiting for central permission. Parts of the Defense Department are already realizing some of this potential in the way they are conducting the ongoing war in Afghanistan. DOD researchers sponsored by DARPA's Information Awareness Office have also concluded that the whole government should adopt ambitious networked information strategies for homeland security. Leaders may need to craft bolder architectural designs and then pull their agencies toward building them. Technology solutions, like firewalls, can help, and so can the use of audit trails to record and check on who has accessed which data.

To guide and support—not quash—local initiative, the new Department of Homeland Security, working with the President's Office of Management and Budget can develop guidelines to "charter" projects involving federal, state, local, and private sector participants. These projects can become the elements of a next-generation national security infrastructure. To show what we have in mind, we offer **ten elements** of effective programs in Illustration #1, "Some Characteristics of a Next-Generation Homeland Security Information Network."

We welcome the initiative of the National Governors Association to build on the burgeoning pilot projects and develop model "charters" that can facilitate creation of a national, networked analytic community across America. We are encouraged by the support this initiative has received from governors and from administration officials. This Task Force will be a partner in that effort.
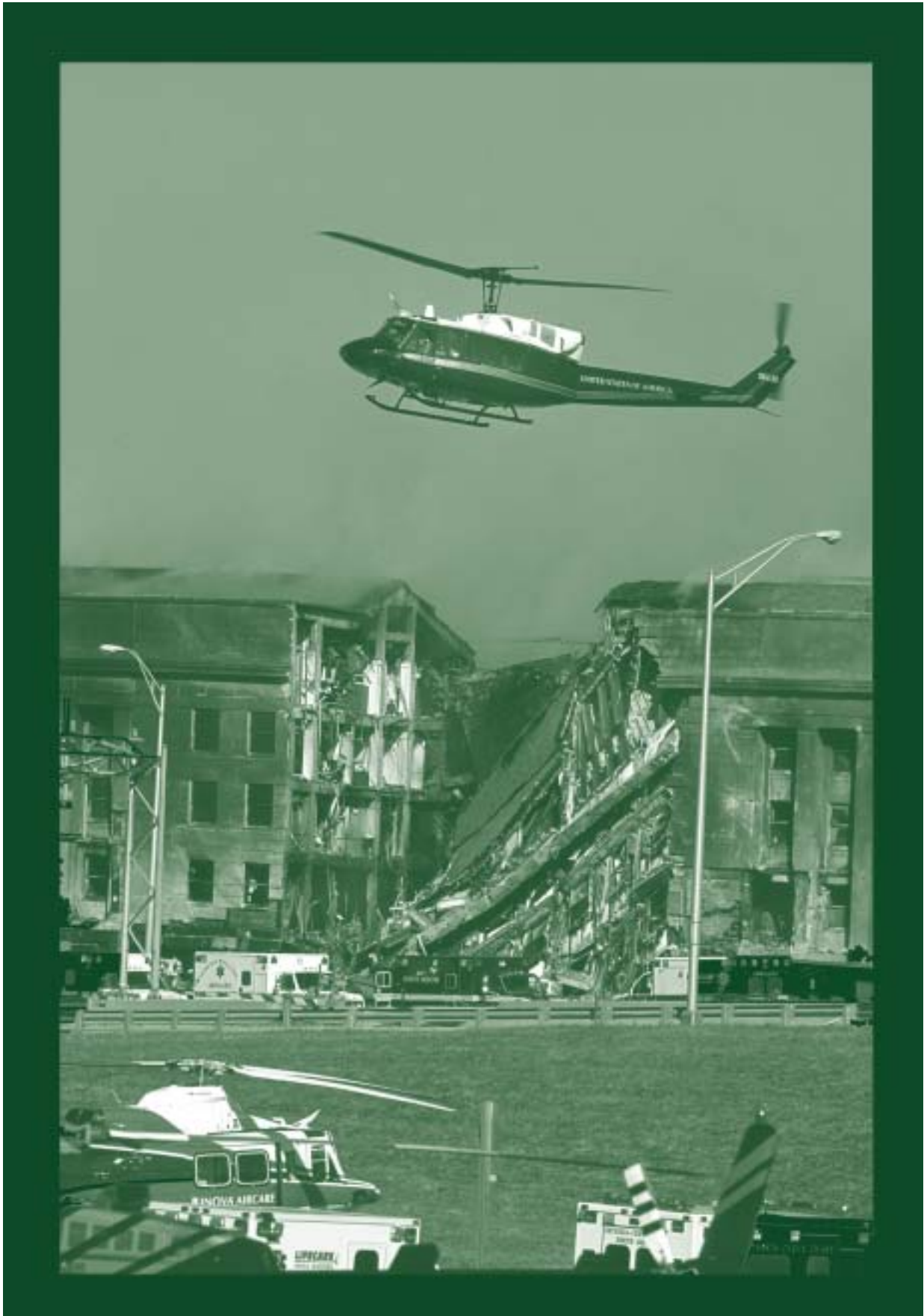
Illustration No. 1: Some Characteristics of a Next-Generation Homeland Security Information Network*

1. Empower Local Participants

Local participants must be empowered to contribute, access, use, and analyze data. At the same time they must be allowed to identify, access, communicate with, and assemble other participants in both the public and private sectors.

Expert groups must be allowed to form at the edge of the network. Data should be maintained and rule sets should be developed and implemented by and among local participants. Each should be allowed to undertake as much work as they are capable of doing.

Push computing requirements away from the center to utilize excess capabilities at the "edge" of a network, allowing mini-centers to develop around local expertise, which can then be accessible to other network participants.

2. Provide Funding and Coordination

Centrally designed and controlled systems are too rigid to evolve quickly, but a well-coordinated system of empowered participants can be nimble, effective, and responsive. Such a system is not only desirable, but also crucial to the success of our national security personnel in the future.

The DHS has the unique power to coordinate the many elements of this system. There are many areas that demand coordination: appropriate data sharing technologies such as XML must be identified and evaluated for applicability; decentralized and comprehensive directories will be required to ensure that individual participants can identify and access information; querying systems must be developed and maintained; network traffic and usage must be tracked and analyzed; and a common vision must be articulated and rewarded to effect cultural change.

3. Create Safeguards and Guidelines to Protect Civil Liberties

National security systems should raise concerns about privacy, civil liberties, and due process. To protect against abuse in how information can be used, accessed, or shared, participants need clear guidelines based on our laws and social values.

The DHS should take the lead in creating robust permissioning structures and audit trails that will help enforce appropriate guidelines. These critical elements could employ a wide variety of authentication, certification, verification, and encryption technologies. Role-based permissions can be implemented and verified through the use of certificates, for example, while encryption can be used to protect communications and data transfers. A robust Public Key Infrastructure (PKI) or other authentication system within the network, driven by DHS at the core, may turn out to be crucial. Auditing tools that track how, when, and by whom information is accessed or used ensure accountability for network users. These two safeguards—permissioning and auditing—will free participants to take initiatives within the parameters of our country's legal, cultural, and societal norms.

4. Eliminate Data Dead Ends

Intelligence and law enforcement officials have already identified the stovepiping of information within an agency as a dangerous impediment to national security. But they have failed to overcome it.

Information must be shared on the network, subject to need, suitable permissions, and classifications. In some cases the information shared may not be the data itself, but pointers to the person

who controls the data, or who is informed about a topic, or who has access to more classified information. This allows for an object-oriented and self-organizing approach to the information. Participants must be able to identify, contact, and engage their peers through robust directories and identity systems, and access useful and relevant information by using comprehensive querying and analysis tools.

A national security infrastructure must enable, facilitate, and at times, demand two-way communication. To the extent feasible, one-way communications should be eliminated, ensuring that users never reach a "dead end" on the network. Networks that only enable one-way communication often break down into insular groups and isolated regions, inhibiting the flow of information needed to address today's threats. Individuals who contribute to the network must also receive information and feedback from the network and other participants, ensuring that participants at the edge of the network remain engaged and motivated.

5. Design a Robust System

The network must be designed and deployed to withstand extreme stress or crisis. Points of failure must be identified and minimized, just as points of access must be maximized to encourage widespread usage among qualified participants. Systems must be designed from the "bottom-up," in order to facilitate dynamic and rapid evolution in response to changing needs.

Redundancy, interoperability, and open standards are all elements that constitute robust networks. Ensuring that the network can continue to operate in the event of the loss of a portion of the network is crucial—a so-called "graceful collapse" will prevent catastrophic failures. The ability to find, access, and use data demands common or interoperable data structures and schemas; the industry standard, XML, is an obvious option that can facilitate access to legacy data as well as provide utilitarian structures for to-be-collected data. Meta-data, watermarking, and indexing tools can facilitate data interoperability, storage, and retrieval. Communications standards— TCP/IP, HTTP, and other common Internet technologies—can help simplify and ensure that connectedness is maintained throughout the network. Keeping computation and storage at the edge of the network also allows for redundancy and capacity building.

6. Create Capacities for Network Analysis and Optimization

Network traffic and usage analysis is a powerful tool. Noticing a surge of inquiries from public health officials about a particular problem might alert analysts to a larger danger. The homeland security infrastructure should employ a wide variety of these techniques for counter-intelligence, finding network vulnerabilities, and enhancing robustness. Future networks should be designed with interfaces that give insight into transactions across the network and take advantage of new applications that enable and enhance analysis.

Network traffic and usage data may reveal significant findings, especially when collected and compared over time. Increased activity in one area or an increase in searches on a particular topic may in itself be useful knowledge. The development of local expert groups may alert other network participants to potential concerns or especially useful information.

Modeling of optimal coordination among the network players can provide empirically based scenarios on how to centralize, decentralize, or otherwise improve local coordination based on events and needs.

7. Design for Growth and Plan for Upgrades

Networks should be implemented with the simplest design possible and designed from the bottom up, allowing the requirements of local participants to shape the growth of the network.

Multiple, layered simple elements always provide a more robust and evolutionary environment than preplanned systems. For example, requiring minimal common data formats allows for interoperability and does not limit the organization to a specific or outdated technology solution, while at the same time such minimal common formats can provide for future growth and expansion.

Such a design also allows for the addition of new technologies with minimal disruption to the existing infrastructure or operations. Increased use of sensors and telemetric devices in data collection, for example, can be incorporated into a flexible system based on open standards much more simply than into centralized, proprietary systems. Redundant systems allow for the continued operation of the network even as upgrades are made on portions of the network.

8. Enhance Existing Infrastructures

Existing data collection and analysis processes and infrastructures remain crucial. Emerging infrastructures must be designed to exploit these existing tools. The ability to share and transfer data between older "legacy" systems and the new ones will depend, for example, on the use of open data standards. Connecting local participants at the edge of the network with users who still use more traditional, centralized information systems may require bi-directional communications and appropriate permissioning and authentication systems.

9. Create Network Aware Scenarios

With today's ever-increasing computational power, we can use the data being provided by the various local participants to explore new scenarios. Models for possible attacks and responses— "red" and "blue" team exercises—are enriched by being able to explore, generate, and simulate complex scenarios. These models can then inform or make better sense of puzzling but disturbing queries that might come from analysts in the field.

10. Create a Connected Culture

A cooperative, collaborative culture is required for the success of dynamic connectedness. Just as individuals are empowered through next-generation network designs, participants must also support the successful exploitation of these technologies through positive reinforcement, peer pressure, and accountability as well as repudiation of users who abuse the system.

Feedback systems that reward valuable contributors will help establish credibility both for individual participants and the network as a whole. Reliable, robust, and secure communications will encourage interactivity. Appropriate and verifiable permissioning systems will support the development of trustworthy relationships. Networks that drive both electronic and traditional collaboration can create a mutually reinforcing environment for all involved.

This illustration was drafted principally by the Task Force's working group on "Connecting for Security," with particular contributions from Tara Lemmey, Lauren Hall, James Morris, John Gage, Governor Michael Leavitt, Robert Clerman, and Mary McKinley.

ORGANIZING THE NATIONAL HOMELAND SECURITY COMMUNITY

It should be apparent by now that we believe the new Department of Homeland Security (DHS) offers an extraordinary institutional opportunity to create the new capacities for government action that the country will need. The new Department should be the hub for accumulating, analyzing, and networking domestic information and intelligence from every available source. This analysis would then be linked firmly to action from a federal executive department operating in every part of America, in concert with state, local, and private sector partners.

With this conception in mind, the most important organizational challenge for the President and Congress may be to sort out the respective roles of the DHS on the one hand and the Department of Justice, specifically the FBI, on the other.

America's past experience with domestic intelligence is illuminating. During and after World War I, without special statutory authority, the predecessor of the FBI and other federal agencies engaged in activities that a subsequent Attorney General, Harlan Fiske Stone, described in 1924 as "lawless, maintaining many activities which were without any authority in federal statutes, and engaging in many practices which were brutal and tyrannical in the extreme." When the FBI was created, Stone instructed its new director, J. Edgar Hoover, that "the activities of the Bureau are to be limited strictly to investigations of violations of law."

In the mid-1930s, based upon vague, conflicting, and informal presidential requests to investigate "subversion" and "potential crimes" related to national security, the FBI built up a broad domestic intelligence program, notably in a "General Intelligence Division," *in addition* to its growing and vital counterintelligence efforts. The executive branch chose not to seek any legislative authorization for these moves, and Congress declined to confront President Roosevelt or Hoover about it. The programs expanded and became institutionalized as part of the effort against internal Communist subversion from 1946 to 1963. The FBI became increasingly isolated from effective outside control. During the 1960s and early 1970s these domestic intelligence programs were applied to a widening range of domestic activity by American citizens, as documented in the Church Committee report of 1976.

As presidents and Congress reacted to these abuses, the FBI's domestic intelligence activities were dismantled. The Bureau returned to a narrower definition of its law enforcement mission. During the 1980s, and especially the 1990s, growing dangers from domestic and international terrorism forced the FBI to devote significant resources to investigation of terrorist groups in addition to its continuing counterintelligence duties. But until quite recently the FBI has not developed a systematic domestic intelligence capability, in part because of its dedication to its traditional law enforcement mission and in part because of internal factors—pressed on one side by leadership at headquarters anxious to avoid the abuses of the past and pressed on the other by public criticism and lawsuits.

Today the FBI is under pressure once again to return to the work of domestic intelligence that needs to be done, to hire and train hundreds of new intelligence analysts and use the collection authorities that were recently expanded by the USA PATRIOT Act and revised investigative guidelines issued by the Attorney General.

The proposed creation of a new Department of Homeland Security is a remarkable opportunity to reflect and consider the way ahead. The administration and many leaders in both houses of Congress agree that this new Department should have a key role in domestic intelligence.

Our Task Force's basic conception is that the Department of Justice and its FBI should be the lead agencies for law enforcement, exercising the power to investigate crimes, charge people with crimes, perhaps take away their liberty, and prepare cases for trial and appeal. The DHS should be the lead agency for shaping domestic intelligence to inform policymakers, especially on the analytical side, so that there is some separation between the attitudes and priorities of intelligence analysis and the different, more concentrated, focus of people authorized to use force on the street to make arrests and pursue or detain citizens.

We understand that criminal investigation (and counterintelligence) often overlaps with intelligence work. Some overlap is natural and good. We believe the FBI should continue to be the entity responsible for domestic intelligence collection operations in countering terrorism that are undertaken under their criminal and foreign intelligence collection guidelines. But there is a strong case for a fundamental separation of the analytic function, which will also gather information that is publicly available or volunteered. Intelligence has much broader purposes than criminal investigation. The operational objectives are different. The training is different. The rules about how to collect, retain, and share information are different. The relationships with sources of information are different.

The working group paper in Part II, drafted for that group by John Hamre and Mary DeRosa, points out that, unlike an intelligence agency, the orientation of a law enforcement agency is primarily reactive. Its purpose is to capture and prosecute criminals. Law enforcement agencies often will prevent acts of terrorism or other crimes by catching a criminal before a crime is committed, but they collect information to detain criminals, not to provide warnings, assess vulnerabilities, or inform policymakers. The customer for law enforcement information is the prosecutor and a significant concern in its collection is the suitability of the information for use in court. Law enforcement and foreign intelligence information are collected using many of the same tools and techniques, but different legal authorities and guidelines.

The FBI's culture is that of a law enforcement agency. There is little representation, particularly in the senior levels of the agency, from people with experience in national security. Although senior personnel interact regularly with national security policymakers, there is a resistance ingrained in the FBI ranks to sharing counterterrorism information with the national security community or others outside of law enforcement channels. Unlike our foreign intelligence agencies, the FBI has no effective process for providing intelligence on terrorism to policymakers and others outside of the law enforcement community who need it. Moreover, the FBI has not prioritized intelligence analysis in the area of counterterrorism. The role of analysts is not valued at the FBI the way it is in other intelligence agencies. There is insufficient funding and staffing to conduct the kind of intelligence analysis that is needed for domestic intelligence in the counterterrorism area.

For the FBI to achieve its important potential in this field, it should concentrate on its own law enforcement, counterintelligence, and counterterrorism mission. As Director Robert Mueller has acknowledged, the FBI should do a better job of analyzing its own law enforcement information, and in the process it can also reach its potential as a contributor to the intelligence community as a whole.

The DHS should rely on the FBI to carry out FISA wiretaps and recruit informants or other clandestine agents, under its existing legal authorities. Thus the implementation of clandestine collection would remain under the supervision of the Attorney General, without requiring the enactment of any new warrant authorities for the DHS.

The FBI has few true intelligence analysts working against terrorism. It is only beginning to build a serious capability. We think those efforts should focus on the analysis of law enforcement intelligence to support the FBI's own operations and contribute to the intelligence community. Some highly skilled analysts now at the FBI may then transfer to the DHS, perhaps finding a better career niche in an environment more devoted to intelligence analysis.

The problem of the FBI's multiple roles has been spotlighted recently by the U.S. Foreign Intelligence Surveillance Court. In an unusual May 2002 opinion the Court publicly voiced grave concerns about the FBI's past failures to maintain a distinction between gathering foreign intelligence and gathering evidence for criminal prosecution. The Court sharply criticized repeated FBI distribution of its intelligence information to criminal squads and to prosecutors who were trying to build cases for trial. (The case is *In re All Matters Submitted to the Foreign Intelligence Surveillance Court,* written by Presiding Judge Royce Lamberth with the concurrence of all seven judges of the Court.)

The Justice Department is appealing the decision, arguing that the USA PATRIOT Act passed in 2001 has lowered the wall between law enforcement and intelligence gathering. The DOJ may prevail in its argument that the newly revised law permits prosecutors and law enforcement agents to run intelligence wiretaps. But that does not mean it is a good idea to combine the two functions. The war on terrorism needs good police and good prosecutors, but it does not have to put them in charge of all information gathering and intelligence collection.

The FBI and its judicial overseers must go through elaborate and inefficient contortions in order to manage the combination of so much sensitive intelligence collection and law enforcement responsibility in one set of institutional hands. In proposing a new Department of Homeland Security that has explicitly been granted substantial domestic intelligence responsibilities, Congress and the President now have an excellent opportunity to devise a more workable division of responsibilities.

Whatever they decide, in order to justify keeping the clandestine collection mission in the FBI, the Bureau needs to build up a dedicated and specially trained collection staff, with its own structures for accountability and oversight. To keep this mission in the FBI as we have suggested, one option might be to create a separate division with these special characteristics and its own career track within the Bureau, a service within a service.

We agree with the administration and both Houses of Congress that the DHS should receive and analyze foreign and domestic intelligence from every part of the government. We further believe it should collect and sift information about vulnerabilities from many kinds of federal, state, and local agencies as well as from hundreds of firms in the private sector. Meanwhile it should coordinate plans, training, exercises, and federal assistance for responding to many kinds of emergencies that may arise. Specifically in the area of information, the DHS should be the main federal coordinator for the next generation homeland security network we recommend in the previous section.

The DHS should have lead responsibility as the all-source intelligence analysis center for all relevant domestic information, which should be integrated with assessments of vulnerability and incoming foreign intelligence. The bills moving through Congress would make the intelligence portion of the DHS a formal part of the intelligence community.

In the United Kingdom, Israel, Germany, France, and Canada, distinct agencies have lead responsibility for domestic information and intelligence gathering as well as all-source analysis. We are not advocating that the United States mimic the precedents set in any of these countries. But the precedents are suggestive. In these countries the domestic intelligence agencies are separate from the lead law enforcement agencies. But once a terrorist incident occurs, or operations are mounted against particular suspects, the lead is handed off to the national or local police, who often, and rightly, have strong anti-terrorism operations of their own.

- The domestic intelligence organizations in the United Kingdom (the Security Service, also known as MI-5), Germany (BfV), France (DST and DCRG), and Canada (CSIS) are separated from their countries' law enforcement organizations but are within the same ministry (the UK's Home Office, Ministries of the Interior in Germany and France, and Canada's Ministry of the Solicitor General). In Israel, the domestic intelligence agency (the Security Agency) is also separate from the law enforcement organizations, but in this case the Security Agency reports directly to the Prime Minister, while the national police are under the Ministry of Public Security.

- All of these relationships have been worked out through painful experience. None are easy. But each of these countries has found that law enforcement and intelligence work do not mix easily. Law enforcement has special requirements, including an overt, dominant presence in tactical operations "on the street" and the preparation of cases for trial. Intelligence planning and analysis is a long-term craft, usually operating best behind the scenes with different training and objectives.

As part of an interagency collection management process, the DHS should have the lead responsibility for setting priorities, and giving overall guidance, for obtaining the collection of domestic intelligence required in order to deliver the robust analysis policymakers need. As a statutory member of the intelligence community (such provisions are in both the House and Senate bills), the DHS should develop intelligence collection priorities in concert with the Director of Central Intelligence, the FBI, the Department of Defense, and the National Security Adviser to the President (as well as the Homeland Security Advisor, if that position is retained).

Of course, nothing should prevent the DHS itself from overtly gathering domestic information. In the foreign intelligence world, overt collection is what the Department of State or even the CIA's Directorate of Intelligence can do on its own: go about openly, talk to people, and buy or collect open source data. It would not recruit clandestine agents or secretly eavesdrop on communications.

The DHS could take the lead in processing and analyzing the full "take" from such operations where they have an intelligence purpose, while the FBI retains all its current collection and analytical responsibilities in its own law enforcement, counterintelligence, and counterterrorism work. Where the intelligence and law enforcement material is mixed, the DHS can filter and pass information back to the FBI for specific criminal investigations.

Foreign/domestic distinctions also matter in the way information is shared. By putting the DHS at the hub of the distribution, that agency can filter the flow of domestic intelligence into the hands of police and prosecutors preparing a possible criminal case, where this information could also be discoverable by attorneys representing the criminal suspect. The DHS can also filter the flow of domestic intelligence into foreign intelligence agencies like the CIA, which are still restricted in their domestic activities by laws and executive orders.

Since protecting the homeland is a responsibility shared by every citizen, private sector cooperation will be easier as part of the wide-ranging analysis of domestic information that the DHS must necessarily perform as part of its responsibilities for protecting critical infrastructure. Even now, the private sector is much more likely to cooperate with government agencies in administrative proceedings than in the shadow of criminal investigations.

Clarifying lead responsibility in the DHS for shaping the priorities and analysis of domestic intelligence is a major undertaking, but this executive responsibility is already stated or implied in both the House and Senate versions of the legislation that would create the new Department. This arrangement could become a source of friction between the new department and federal law enforcement agencies like the FBI. Some of that is unavoidable and will need to be worked out in day-to-day practice.

Finally, the networked, national community we have described earlier should be built around organizations that bring together people, not just their computers. We therefore endorse the administration's proposed creation of Homeland Security Task Forces in every state, and recommend that they be supplemented by regional Homeland Security Task Forces as well.

Each of these Homeland Security Task Forces could be co-chaired by a representative of the President—a state or regional DHS representative—along with a representative of the governor (or top regional/local official)—such as the state's director of public safety. These task forces should bring together law enforcement, health, and emergency management officials from all levels, along with representatives from Defense Department elements such as the National Guard and the new Northern Command, and key representatives from the private sector.

In our conception, shared by at least some senior administration officials, these Homeland Security Task Forces would be broadly based. They should include but transcend the existing law enforcement interagency bodies like the Joint Terrorism Task Forces. They can be constructed by using the foundation already laid by the regional organization of the Federal Emergency Management Administration, an organization that is likely to be absorbed into the DHS.

Such a virtual homeland security community could eventually be extended internationally to include countries that have the closest information-sharing relationships with the United States. This would be part of a national security policy that extends the concept of joint planning from the military sphere to the wider range of agencies involved in homeland security. This is an aspect of NATO's transformation. Our institutions for bilateral cooperation may need to adapt too. The varied counterpart officials in these countries would be expected to respect our guidelines to avoid misuse of information.

What the Analysts Should Do

(A) Wide Scans to Identify Vulnerabilities.

Intelligence is often conceived as perpetrator-centered and event-focused, locating individuals associated with terrorism and uncovering their plots. As the paper from the working group on analytic methods (included in Part II of this Report) points out, however, the highly focused threat-based approach should be supplemented by peripheral vision. Working with other relevant agencies, the DHS center should map and prioritize the most vulnerable potential *targets* and the most dangerous *means* that could be used to attack them. This is why it is so essential that intelligence and critical infrastructure protection *both* be placed under the DHS's Undersecretary for Intelligence. The analysis of threat and vulnerability must be combined in one place.

Scenario analysis is one name for a method that puts analysts in the place of a potential enemy and then works through the specifics of how that enemy would work through the operational details of a possible attack. This kind of analysis is also sometimes referred to as using "templates," or a "project planning paradigm," or "red-teaming." This analytic effort can be top-down, which in this context means that intelligence analysts might organize the effort and then reach out to specialized teams drawn from the agencies that focus every day on those subjects, like agriculture or nuclear reactor safety.

But scenario-generation should also come from the field—from the "nodes" of the networked analytic community. They may add some original ideas because they start with different preconceptions. (An example is the "Phoenix" memo from an FBI agent in Arizona who encountered a particular local case and began worrying about Muslim terrorists in U.S. flight schools.)

"Means" analysis, looking hard at access to particular technologies or vehicles of attack, is another powerful tool, especially if combined with countersurveillance of possible targets or means of attack. Means analysis might reveal the most cost-effective forms of prevention. For instance, means analysis would think about how to harden airplane cockpit doors to prevent terrorists from being able to take over a plane.

Risk analysis is an especially prominent technique among engineers and other safety experts. That field has developed some proven methodologies for ranking and filtering possible dangers and assessing the most effective ways of preventing them.

Once wide-scan efforts can home in on key access points to high value targets or means of attack, national guidelines can be developed for screening individuals for entry through these "gates." Biometric identification systems work best in controlled settings, where combinations of biometrics (*e.g.,* facial recognition algorithms and digitized fingerprints) can be taken more reliably and compared in real time against reference databases or watch-out lists.

(B) In-Depth Focus on Known Concerns.

The all-source centers for intelligence analysis at the DHS and the CIA should mount overlapping efforts to analyze extensive information about people and groups that potentially pose real dangers to

the United States, whether they live in the United States or in foreign countries. The analysts should understand who they are: their goals, strategies, capabilities, networks of contacts and support, the context in which they operate, and their characteristic habits/patterns across the life cycle of operation—recruitment, intelligence and reconnaissance, target selection, logistics, and travel.

Linking together available information can yield rewards, but the analytic techniques must be used carefully to avoid mismatches and false identifications. We need to build the expertise, systems, and "middleware" that can draw out reasonably straightforward sets of connections from data that government agencies already collect. Here are some hypothetical examples:

> Illustration #1: Analysts could have asked how many holders of visas from certain countries had spent more than a month in Afghanistan and then correlated those people with others who have spent time in Afghanistan to see who shares addresses, phone numbers, credit cards, or bank accounts. Such searches can and should be done in ways that reveal only the identities of the matches.

> Illustration #2: Analysts could identify purchasers of airline tickets who have telephoned persons on a terrorist watch-out list during the past year.

> Illustration #3: Analysts checking applicants for visas to come to the United States could correlate dates of travel to Afghanistan or certain cities with the times of known terrorist activities in those places.

> Illustration #4: An example to avoid: Analysts put someone who just has the same last name as a known terrorist on a watch-out list.

In other words, linking of information should be based on criteria that are developed to balance security gains against the potential for overreaching and threatening liberties.

Existing law for the *collection* of information and intelligence in general permits very extensive analysis. If properly interpreted and defined by new guidelines that balance privacy and security, recommended later in this report, existing law may be sufficient for adequate information sharing among government agencies that will perform such analysis without intruding on essential liberties.

The DHS intelligence analysis center or the DCI's counterterrorist center do not need to accumulate and hold all relevant databases to which they may gain access. In other words, there is no need to build one big data warehouse. Instead, the centers should interface with such databases as needed.

Data mining can be a useful tool. But it is also a tool that invites concern about invasion of privacy. Extravagant claims have been made about the potential uses of data mining, matched by similarly extravagant notions of the vast private or public databases that should be opened to such journeys of exploration. Neither the real needs nor the real capabilities are so exotic. Though there are areas where more data may need to be collected, the immediate challenge is to make more effective use of the mountains of data that are already in government hands or publicly available. Data mining, like any other government data analysis, should occur where there is a focused and demonstrable need to know, balanced against the dangers to civil liberties. It should be purposeful and responsible.

LINKING ANALYSIS TO PROTECTIVE ACTION: USING WATCH-OUT LISTS

The first type of analysis we described was "wide scans to identify vulnerabilities." There we introduced the idea of specifying critical "gates" where officials can lawfully control access to especially dangerous means of attack. Airport security is a natural focal point, but others might include points of access to dangerous pathogens, transportation of extremely hazardous materials, or vulnerable points of access to the country's electronic networks.

We also just discussed a second type of analysis—an "in-depth focus on known concerns." That effort gathers and analyzes information on known concerns, like suspected terrorists. That information can contribute to lists of people wanted for arrest, for questioning, or just for surveillance of their movements.

To bring the two forms of analysis together in practice, governments can combine "gates" and "lists" for protective action. As officials try to notice and analyze the people who pass through certain kinds of "gates," the use of watch-out lists becomes critical. This tool can be exceptionally valuable, *if* it is used in a responsible and reliable way and focused on the terrorist danger.

To illustrate the power of such "gates" and access to quite modest forms of data, we examine the concrete case of the 9/11 hijackers in Illustration No. 2.

Illustration No. 2: "Watch-Out Lists" and "Gates": A Hypothetical Application to the 9/11 Attacks*

Hypothesis: Each person buying an airplane ticket is checked against lists of possible terrorists. If there is a "hit," that person's available information is checked to identify possible associates.

- Software already exists that can check names and addresses against multiple databases. It is capable of accounting for errors and variations in the way names are spelled, and can perform these functions on very large databases in seconds.

The Application:

- In late August 2001 Nawaq Alhamzi and Khalid Al-Midhar bought tickets to fly on American Airlines Flight 77 (which was flown into the Pentagon). They bought the tickets using their real names. Both names were then on a State Department/INS watch list called TIPOFF. Both men were sought by the FBI and CIA as suspected terrorists, in part because they had been observed at a terrorist meeting in Malaysia.

- These two passenger names would have been exact matches when checked against the TIPOFF list. But that would only have been the first step. Further data checks could then have begun.

- Checking for common addresses (address information is widely available, including on the Internet), analysts would have discovered that Salem Al-Hazmi (who also bought a seat on American 77) used the same address as Nawaq Alhazmi. More importantly, they could have discovered that Mohamed Atta (American 11, North Tower of the World Trade Center) and Marwan Al-Shehhi (United 175, South Tower of the World Trade Center) used the same address as Khalid Al-Midhar.

- Checking for identical frequent flier numbers, analysts would have discovered that Majed Moqed (American 77) used the same number as Al-Midhar.

- With Mohamed Atta now also identified as a possible associate of the wanted terrorist, Al-Midhar, analysts could have added Atta's phone numbers (also publicly available information) to their checklist. By doing so they would have identified five other hijackers (Fayez Ahmed, Mohand Alshehri, Wail Alshehri, Waleed Alshehri, and Abdulaziz Alomari).

- With days still remaining before the scheduled flights, additional investigations could have turned up information about attendance at flight schools (information that the U.S. government then did not have in a digitally searchable form) or on puzzling foreign links (like common financial links to Hamburg, information that the government was not able to access in real time.)

- Closer to September 11, a further check of passenger lists against a more innocuous INS watch list (for expired visas) would have identified Ahmed Alghamdi. Through him, the same sort of relatively simple correlations could have led to identifying the remaining hijackers, who boarded United 93 (which crashed in Pennsylvania).

* Information for this illustration was drawn from work done by Systems Research & Development, one of the firms that has developed relevant software, in this case with the help of venture capital supplied by the CIA-sponsored firm, In-Q-Tel.

In this hypothetical illustration, combining the "gate" with a virtual watch-out list works because two of the 9/11 hijackers were wanted as suspected terrorists and bought airplane tickets using their real names. Let us assume, then, that future terrorists use false names or otherwise attempt to conceal their identity. The individuals can still be identified, not by a name but instead with a biometric algorithm derived from a photograph of the face or the digital measurement of fingerprints.

Facial recognition and other biometric identifiers can be evaded or defeated, although it is difficult, especially when compared to the paper-based ID systems (driver's licenses and passports) now used in the United States. But evasion becomes far more difficult if the photograph or other identifiers are taken, and then checked, under controlled conditions by a human observer.

Hence the concept of the "gate" is important as a way of focusing the use of these potentially intrusive technologies and increasing their reliability. For example, if the visa applicant and the person passing through an airport security checkpoint are scanned, voluntarily, under controlled conditions, the technology is powerful.

If multiple biometric identifiers are used, such as both photos and fingerprints, as a check against false positives, the technology can be still more effective. The biometric identifiers can go into a government database when the information is originally acquired (when someone applies for a visa, or is arrested, or receives a driver's license, for instance), regardless of whether the biometric information is encoded on the visa document itself. If the information is in the database and then can be compared under controlled conditions with the actual individual, the suspect cannot beat the system just by switching or forging identity documents of the kind ordinarily used now.

Such checks are not foolproof. No system is. But it raises the bar significantly, adding more complications to enemy planning. As plans become more elaborate and difficult to carry out, the chances of mistake and exposure go up as well.

But with any such protective system the preparation of guidelines is essential. These guidelines must standardize the conditions under which the biometric data is gathered and compared by various agencies, and how any biometric identifier is issued, and regulate what actions will be taken if a person at a gate is a "match."

Various agencies of just the federal government currently maintain more than a dozen different kinds of watch-out lists. Each of these were created for different purposes. We do not recommend combining them into one vast list. But we do recommend the creation of "virtual" consolidated watch-out lists. The DHS should be able to pass names across the various lists to check for "hits," without actually building a data warehouse of its own.

Other agencies at all levels of government will want to perform such checks. The White House can take the lead in requiring all such lists to meet certain common, minimum standards—including interoperability and accessibility from one agency to another. Therefore we also recommend that:

- Guidelines and procedures are needed on what information will get a person on such a list, and off of it. It should not take months to get someone on a list. Nor should it take even longer, and a team of lawyers, to get someone removed from it.

- Guidelines are also needed on how such information or lists would be used in the field—whether for arrest, interviews, or simply for tracking location or movements. These databases should have common protocols for data entry and indexing, such as digital fingerprint and facial recognition algorithms. The DHS should develop these guidelines as a national service for various federal, state, and local agencies.

- Also, as a common national service, the DHS could be responsible for quality control, and thus also be accountable for operation of the system in compliance with the written guidelines. Frequent review will be needed. The use of such lists must be consistent with constitutional requirements (detailed in the background research paper on profiling and watch lists) and with the democratic ideals of our nation. Targeting citizens based solely on a single factor, like their race, or their gender, or their political or religious beliefs, should be expressly prohibited in the guidelines for operating these systems.

As illustrated in detail in our 9/11 hypothetical, the method can be reasonably straightforward. It can start with a search for specific individuals already wanted or otherwise known to government agencies—like the hijackers Al-Midhar and Alhazmi before 9/11. And, if such people are identified, it is then reasonable to try to identify any associates of those people, by checking for common addresses, phone numbers, and so on. Even in our other hypothetical illustrations we are still using relatively concrete correlations (travel to/from Afghanistan and dates of terrorist activity, etc.).

Employing watch-out lists without proper preparation of the kind we describe could be counterproductive, discrediting a valuable tool. As an example of such more ambitious worrisome "profiling" efforts, the new Transportation Security Administration (TSA) wants to check passenger lists against watch-out lists. But, even though it is not yet able to perform the simpler data analysis tasks recommended above, TSA is reportedly trying to develop a CAPPS II system for screening air travelers, in part by creating "profiles" of possible terrorists by analyzing behavioral characteristics of the general population. According to one report, by Robert O'Harrow in the September 4 *Washington Post:*

> Under the plan, passengers would be required, when making their reservations, to provide identifying information, such as a name, address, and driver's license, passport, Social Security and frequent-flier numbers. Those details would be used by private data services, such as ChoicePoint, Inc., an identification and verification company, to supply more information about the individual.

> TSA computers would then use artificial intelligence and other sophisticated software, along with behavior models developed by intelligence agencies, to determine whether the passenger is "rooted in the community"—whether he or she is well established in the United States—and find links to others who might be terrorists, according to government documents and interviews.

The aim is to create an "automated system capable of integrating and simultaneously analyzing numerous databases from Government, industry and the private sector…which establishes a threat risk assessment on every air carrier passenger, airport and flight", according to a government document.

If the "TSA computers" step in to use "behavior models" to assess the general population, that would be profiling. Some federal officials have reportedly discouraged adoption of the simpler analytic approaches we recommend, fearing that adoption of such strategies will hinder acceptance of their more ambitious plans to "score" passengers for presumed riskiness.

All profiling is not inherently bad. But we are cautious about claims that "behavior models" of the kind postulated here can effectively identify possible terrorists in the general population. Such a profiling system would also need to consider the risk of false positives that could number in the tens of thousands when such searches for correlations are applied to pools of people numbering in the tens of millions. The quality control issues arising from bad underlying data are also compounded in such a system.

We recommend that, first, our governments as promptly as possible at least acquire the capability to do the simpler analytic tasks they still cannot perform. Using watch-out lists more effectively is imperative. We should see how well that works. Meanwhile these experimental behavioral explorations should be treated as research projects that need to be tested before they are tried out upon the vast community of American air travelers.

GUIDELINES TO BALANCE PRIVACY AND SECURITY

As we have suggested in the use of watch-out lists, guidelines must be set by the President so that all agencies come to share a common, minimum set of goals and standards. To succeed, the system must have the confidence of the American people it serves, while the analysts and operatives involved must feel confident that they know what they are expected and allowed to do, and that their work is lawful and appropriate.

The scope of domestic intelligence work should be defined. Specific guidelines are essential to guide intelligent analytic work, draw on the strengths of a national community, and provide a basis for training. Guidelines are also a key to assessing performance.

Guidelines also enable managers to embed respect for privacy and civil liberties into the core definitions of the analytic work itself. That too becomes a basis for training and developing routines, and for holding the officials accountable for compliance with the rules.

The Task Force formed an ad hoc working group on "Collection, Use, and Analysis" to develop a concrete framework illustrating the kinds of guidelines we recommend. That sample framework is presented as Illustration No. 3.

Illustration No. 3: Guidelines for Database Access and Use*

Fighting terrorism requires new weapons. One weapon being used by the government is the increased use of public and private databases to prevent attacks. The analytic purposes of this work have not been well defined. In specified circumstances, these guidelines will require analysts to identify the types of databases involved, define the purpose of the data review, and clarify the authorization for collecting and disseminating whatever is found. Such considerations must be addressed before embarking on broad new uses of information resources. This is not just because of the privacy and constitutional interests at stake, but also to avoid fruitless searches for intriguing but essentially meaningless correlations.

Guidelines like those illustrated below seek to employ the capabilities of new technology to provide new protections for privacy—protections that will allow the effective use of information in the war against terrorism while respecting individuals' interests in the use of private information about themselves.

Existing guidelines are inadequate. Developed in the course of traditional, reactive law enforcement, they often require some degree of individualized suspicion and prior judicial approval before information can be accessed. This impedes the quick, effective use of existing databases to identify and prevent terrorist acts. Once the data has been lawfully gathered, however, existing approaches offer little or no privacy protection at all.

The following recommendations spell out some of the principles that will allow more effective use of information in the war against terrorism. Proceeding from the premise that security and privacy can coexist, these suggested new guidelines are a first step toward designing a system that will allow us to fight terrorism effectively and secure modern privacy protections for individuals.

1. Importance of Access to Information in Public and Private Hands

Access to information in the hands of public and private entities is an essential tool in the fight against terrorism. Government agencies responsible for combating terrorism—including state and local as well as federal authorities—should have timely and effective access to needed information, pursuant to appropriate legal standards. The legal constraints and exceptions provided by current laws are generally sufficient to allow a homeland security agency to gain necessary access to information held by other government agencies. These new guidelines offer a framework and procedures to allow that information to be effectively used, analyzed, and disseminated. At the same time, these guidelines are intended to ensure that information about people in the United States is used in a responsible fashion that respects reasonable claims to individual privacy.

2. Purpose and Interpretation

a. These guidelines should be interpreted and applied in a fashion that encourages rapid, effective, and responsible access to data that can assist in the task of identifying, thwarting, or punishing terrorists. These guidelines should also be interpreted and applied in a fashion that encourages respect for fundamental liberties, creativity, innovation, and initiative in the use of data for the purpose of fighting terrorism.

b. These guidelines should be used only for the gathering and analysis of information for intelligence in the war against terrorism. The procedures and authorities for using the legal process for obtaining information for law enforcement purposes should remain unchanged.

3. Coordination and Authorization

An intergovernmental body, chaired by the Secretary of the Department of Homeland Security and composed of representatives of the relevant federal, state, and local agencies, should be formed to coordinate the procurement and use of private as well as state and local databases containing information about United States citizens. Because databases have varying degrees of utility, privacy interest,

and reliability, the Task Force concluded that a single point of coordination would provide accountability for privacy concerns as well as allowing for the effective and efficient use of information. In addition, this intergovernmental body will provide a focal point for private companies and state and local administrators' concerns about burdensome, duplicative, and inconsistent requests for information.

Similarly, the authorization for procuring or requesting access to databases should not be burdensome on investigators and analysts. These guidelines envision a process in which a single authorization for the procurement of the database will be sufficient for all necessary and continuing access by agency personnel, if it is for the authorized use.

4. Relevance

Agency personnel should have access to and use information available under these principles only for purposes relevant to preventing, remedying, or punishing acts of terrorism.

5. Accountability

Agencies and their employees should be accountable for the ways in which they access and use information available under these guidelines. An agency should be able to identify how its uses of databases are relevant to preventing, remedying, or punishing acts of terrorism. While it would be plainly inconsistent with the purposes of these guidelines to require that an agency or employee explain the relevance of every query before gaining access to data, mechanisms such as database access records, audits, and spot checks, should be used to ensure that agencies move toward demonstrable compliance with this principle.

6. Dissemination and Retention

Information about American citizens should not be disseminated or retained by the collecting agency unless it is demonstrably relevant to the prevention of, or response to, an act of terrorism. Administrative rules, training procedures, and technology should be implemented to prevent the unauthorized disclosure of private personal information. An electronic audit trail in how information is used, and penalties for misuse, can reinforce these guidelines.

7. Reliability of Information

Agencies should strive to use the most accurate and reliable information available. Nevertheless, information used under these guidelines may include data of questionable or varying reliability. Where feasible, and to promote effective antiterrorist action, limitations on the reliability or accuracy of data should be made known to those using the data. In the event that an agency determines that information is materially inaccurate and that an individual is likely to be harmed by future use of that inaccurate information, reasonable efforts should be made, and a process put in place, to correct the inaccuracy or otherwise avoid harm to the individual concerned.

8. Information Technology Tools

To the extent consistent with the purpose of these guidelines, information technology tools should be developed and deployed to allow fast, easy, and effective implementation of the relevance, accountability, and reliability principles of these guidelines.

Consistent with a vigorous defense against terrorism, these guidelines envision tools that create audit trails of parties who carry out searches, that anonymize and minimize information to the greatest extent possible, and that prevent both the intentional and unintentional dissemination of irrelevant information to unauthorized persons or entities.

9. Information in the Hands of Intermediaries

a. Much of the information relevant to the fight against terrorism will be in private hands. As a general principle and where consistent with the purposes of these guidelines, it is preferable to leave information in the hands of private intermediaries rather than consolidating it into agency databases.

b. In many cases, an agency may be required to transfer information into an agency database because it does not have the tools needed to search privately held data effectively and quickly. Agencies are encouraged to develop and deploy tools that would allow such searches and thereby allow information to remain exclusively in private hands.

c. Private databases are not created for the government; they are created by private parties for their own commercial purposes and subject to the constraints of the marketplace. An agency seeking access to such databases should treat these intermediaries fairly. In particular, the agency should
    i. preserve necessary confidentiality and protect intermediaries from liability for any assistance they may provide to the agency in good faith; and
    ii. use commercial contracts or similar arrangements to compensate intermediaries for any assistance provided to the agency.

d. Agencies should initiate and maintain a cooperative dialogue with the private sector to develop voluntary data retention policies that maintain information necessary for the war on terrorism. Agencies should endeavor to identify critical information and advise private firms of the importance of their voluntary efforts to retain such data. If necessary the government may even encourage the formation of self-policing groups within the private sector to help achieve the data retention objectives. In other words, the more the government does to articulate specifically what information should be retained and why, the greater the obligation the private sector should feel to cooperate with these agency requests. In a narrowly defined set of circumstances, such as with airline passenger manifests and sales of certain biological pathogens, data retention may appropriately be required.

10. Revisions and Public Comment

a. These principles are preliminary steps toward establishing the fundamental authorities and protections for the use of information in thwarting terrorism. They should be reviewed, revised, and made more specific in the light of actual experience.

b. These guidelines and any future revisions and specific rules that are established based on the guidelines should be available to the public and subject to public comment, unless the President finds that disclosure will endanger classified intelligence collection or analytic methods and threaten the national security of the United States.

11. Agency Implementation

a. Compliance with these guidelines should be achieved to the greatest extent possible through training, advice, and quick correction of problems rather than through after-the-fact punitive measures that may lead antiterrorism agencies or employees into risk-averse behavior.

b. Investigations of suspected violations should be performed by a single office and should focus principally on systemic measures to avoid future violations.

12. Congressional Oversight

Nothing in these guidelines restricts review of the guidelines by Congress. Members of Congress or Congressional staff conducting reviews of the guidelines or their implementation should expressly agree to protect an individual's privacy, classified information, and confidential sources and methods used to combat terrorism.

These guidelines were developed by a working group chaired by William Crowell and reflect particular contributions from Robert Atkinson, Stewart Baker, Jerry Berman, Ryan Coonerty, James Dempsey, Mary DeRosa, Esther Dyson, Daniel Ortiz, Jeffrey Smith, James Steinberg, and Michael Vatis.

Although the new DHS can be a hub for development and accountability in using guidelines, they should apply to all responsible agencies. For this reason and to promote transparency and accountability, the guidelines should be promulgated in the form of public Executive Orders and—if necessary—classified National Security Presidential Directives issued directly by the President. They should supersede older, analogous documents that now are out of date.

The full range of information activities needed for new national security requirements will gain the confidence of the American people by being accountable to Congress. The Congress should concentrate these oversight responsibilities in *new* committees that can consolidate and focus oversight over the new Department.

• The oversight system can benefit from using the written guidelines that we have recommended be developed for the most sensitive activities that the DHS and other government agencies will conduct.

• Under the bills moving forward in Congress, the DHS will likely have at least an Inspector General and a Privacy Office, and possibly a Civil Rights and Civil Liberties Office as well. The Task Force endorses the goal, but the duties of these various internal overseers need to be clarified by combining the two offices into *one* well funded and staffed civil liberties and privacy office, and then spelling out the referral criteria for the agency's Inspector General.

• Since the DHS may have unusual duties thrust upon it, it needs effective mechanisms for oversight. The purpose of these mechanisms would be proactive, helping to guide officials on how to achieve what they need to do, as well as steering them away from what is out of bounds.

The domestic intelligence capabilities of the DHS must be managed as part of the intelligence community. That system is and should be overseen by the President and the interagency process organized under the National Security Council. This aspect of its duties should also involve the Director of Central Intelligence's role in managing the intelligence community, including the interagency boards operating to assist the DCI.

Within the NSC system, the highest-level resource planning for the intelligence community can be managed by reconstituting an interdepartmental Executive Committee for this purpose. It should include the DCI, the Secretary of Defense, the Secretary of Homeland Security, and the Attorney General, with the President's national security adviser serving as the executive secretary for this group.

The President could also adapt his Foreign Intelligence Advisory Board and its Intelligence Oversight Board to help him continue to oversee the intelligence community in all its activities, both foreign and domestic.

KNOWN ASSOCIATES : 3
HITS RETURNED : 3
RECORD VERIFIED : 09/19/02

KNOWN ASSOCIATES : 20
HITS RETURNED : 11
RECORD VERIFIED : 07/06/02

KNOWN ASSOCIATES : 9
HITS RETURNED : 0
RECORD VERIFIED : 10/01/02

KNOWN ASSOCIATES : 112
HITS RETURNED : 31
RECORD VERIFIED : 09/28/02

MATCH

JOHN DOE N34079 - RETURN NAME MATCH

… AND TRAINING PEOPLE TO DO THE WORK

Pending legislation anticipates supplying needed expertise to the DHS by detailing employees from other government agencies. This may be inadequate. The needed skills are currently in short supply across the government.

The DHS, or at least its intelligence and information directorates, will need the flexibility to be able to hire certain key employees with needed skills. Another option is to allow the DHS to rely on staff they may be able to find in government-supported research centers.

Aside from the disadvantage of diverting scarce talent from other agencies, a number of the specific needed skills may not exist in adequate supply in the federal government at all. There is a particular shortage of people with both the needed analytical *and* data skills. At a minimum, significant investments in training will be needed, training oriented to the analytic methods and challenges described above and the networked, decentralized approach to using these methods.

In addition, the DHS and other agencies will need much better access to IT expertise in the private sector, a topic to which we now turn.

ROLES AND RISKS FOR THE PRIVATE SECTOR

A large portion of the costs of homeland security, tens of billions of dollars, are already being borne by the private sector. The strategies currently contemplated to enhance our homeland security are likely to generate even greater costs. An overbroad and rigid approach to homeland security will make that worse, creating severe economic burdens for the country, and eroding historical strengths of the American workforce such as its members' mobility, speed, diversity, and willingness to think for themselves.

But if systems are designed effectively, they can enhance security and cut costs. Expensive and time-consuming paper- and person-based processes can be replaced with processes that take advantage of information technology. Information is also the key for how government regulators can avoid unnecessarily disruptive strategies. Properly analyzed information and intelligence can yield powerful insights about which policy interventions are likely to be cost-effective and which are not.

The government will need access to public and private sector data for national security. The DHS should develop innovative service-delivery models for using information held within and outside of the government (on trade or specific cargo, for example) and guidelines on the circumstances and procedures for purchasing or requesting access to such data.

EXPLOITING AMERICA'S IT ADVANTAGE

While government agencies have been instructed or have attempted to acquire and use more advanced IT, progress has been slow. Widespread inadequacies still exist in the full range of IT related issues, relative to technology or methods used in the private sector.

Many reasons have been identified for the inadequate use of IT by government in the United States, including: excessively restrictive procurement rules; bureaucratic resistance; inadequate skills and knowledge by government personnel; ineffective, top-down planning for IT improvements instead of user-based perspectives; inadequate and inconsistent support by Congress and state legislatures of IT investments, especially for interagency cooperation; unwillingness of private sector experts to join or work with government due to perceived rigidity, absence of protection of intellectual property, potential liabilities, and by the failure of some large IT projects and vendors to deliver the promised results.

Consolidation of agencies or departments along functional lines is potentially helpful in enhancing efficiency. But to contribute to IT improvements, consolidation must add the new capacities needed to overcome barriers that have led to failures to use existing IT or to develop needed capacities.

In a Fiscal Year 2003 budget request of more than $38 billion, the information management and integration task received a share of about $200 million. Congressional appropriators have cut back even that very modest request. The Information Integration Office proposed by the President has been zeroed out. This was an unfortunate decision because investments in the proper use of information can make all the rest of the spending more productive.

But now a National Strategy for Homeland Security has been announced. A new Department of Homeland Security is being created. The best reason to create this Department is to create entirely new capacities for government action, above all in the area of information.

Information and information processing is to homeland security as the brain is to the human body. Once a convincing information strategy is in place, the President and Congress should allocate the resources to make it work.

A particular problem is the need for resources for activities that cut across agencies, specifically individual agency budgets. The DHS can be a focal point for appropriations that can benefit the entire country, horizontally across the federal government and vertically in supporting networked national operations.

Adequate resources are also essential to create positive incentives for interagency cooperation, rather than relying on White House (OMB) coercion.

Finally, adequate resources are critical to a robust research and development program, if that program is designed to take full advantage of the best practices that have been developed in the private sector. Some specific suggestions follow.

Procurement rigidities and an NIH (Not Invented Here) culture are frequently noted as a major problem in technology acquisition by government. Improvements can be made in the procurement process, but this is not the principal problem. Ways to overcome traditional difficulties are being developed and used. Several helpful ones are likely to be included in the homeland security legislation.

Among these are the following:

- Government entities should have the flexibility to engage in "Other Transactions," as has been authorized for the Department of Defense when acquiring IT for national security purposes. These contracts enable agencies to enter into joint ventures, to extend intellectual property protections to companies doing business with the government, and to engage in other exceptional arrangements. This authority should not be limited to a five-year period.

- Agencies involved with national security IT issues should be able to procure personal services of a limited set of experts without regard to the usual civil service limitations. This authority exists in draft legislation for the DHS, but the power to hire should not be limited to periods of less than a year.

- Agencies should also be given the broad authority to procure essential items and services for homeland security and, when appropriate, to waive normally applicable rules. This is also likely to be included in the DHS' powers, and most limitations and reviews should be eliminated.

- Congress should avoid creating funding inconsistencies and disincentives for IT necessary for national security. Congress has been too prone to give IT expenditures a low priority, and has refused thus far to support IT expenditures that are intended for multi-agency projects in part because its appropriations process does not support interagency acquisitions. This must change.

- Congress should support the training of a corps of IT acquisition specialists for assignment to each of the agencies needing sophisticated procurement advice. Current personnel are unable to utilize the flexibility that exists in the Federal Acquisition Regulation (FAR).

- To fully utilize its IT edge, the United States must find ways to tap existing capacities, to secure private sector support, and to provide government support for particularly promising projects. Recruitment of experts from the private sector, and training of existing personnel, have led to improved IT utilization, but in a slow, inconsistent, and unreliable manner. Research and development in IT within government has also been insufficiently productive. We support the proposal of the National Academy of Sciences' committee on technology and terrorism to create an Institute or similar institution to provide a vehicle by which government can derive advice and assistance on a range of issues from private sector experts. This non-governmental entity should not attempt to duplicate R&D functions already being provided by DARPA, the National Science Foundation, and existing national laboratories.

For a specific outline of how this Institute might work, see Illustration No. 4.

Illustration No. 4: A Research Institute for Homeland Security

The Institute should be available to the DHS Secretary and to other federal, state, and local agencies to assist on IT issues, and should be authorized by Congress to perform at least the following functions:

- Provide guidance in all its IT activities based on a customer orientation that maximizes operational effectiveness;

- Assist the DHS and its component agencies in developing their IT enterprise architecture;

- Provide solutions transfer support for all DHS agencies as well as other federal, state, and local entities, as necessary;

- Assist in developing protocols (but not rigid standards) for meta-data (interagency interface), data entry, security, and storage;

- Ensure that necessary testing is conducted to certify products from private vendors as meeting protocols;

- Establish a committee to screen proposals for research, development, or purchase of IT products from private sector companies;

- Provide advice and assistance to state and local governments and entities with regard to IT related issues;

- Assist through a committee designated for this purpose in recruitment of IT specialists, as well as in placing them with government agencies;

- Assist Chief Information Officers of federal, state, and local agencies in developing IT related plans for homeland security, and in certifying such plans as meeting relevant protocols and IT requirements;

- Establish and operate an IT clearinghouse for public and private exchange by IT experts and users of needs, capabilities, and experiences;

- Provide advice and assistance in developing methods for enhancing international cooperation and interface; and

- Engage with DARPA or other R&D entities in specific IT development initiatives designed to provide substantial and project-based federal government support to work with private firms in developing IT technologies or capacities that are recognized as urgently needed for national security purposes. Special efforts of this sort, such as the Manhattan Project and the Y2K initiative, successfully focused national resources in a highly productive way.

Examples of such projects include the creation and deployment of operative, consolidated watch-out lists; or designing a nationwide, Emergency Response Network on the Internet.

In addition, an entity should be created within the DHS to assist the Secretary and agency CIOs in providing effective IT training, planning, and implementation. This DHS entity should have the capacity, continuity, and authority to help satisfy the functional needs required to overcome recognized deficiencies that have resulted in inadequate IT exploitation.

- This DHS IT Center should be provided with multi-year budgetary support, including in particular funds to be used for interagency IT activities and for monetary awards to DHS agencies or departments that perform effectively in adopting IT recommendations. The Center should be required to review all IT infrastructure proposals made by or on behalf of any DHS entity, and to certify such proposals to Congress as warranting legislative support.

Finally, the DHS should join the CIA as a major sponsor and client of In-Q-Tel, using that firm as an effective, working vehicle that can tap cutting-edge expertise about new IT developments and help convert these ideas into usable, deployable products that can make America safer and freer.

Current drafts of legislation to create the DHS include the creation of entities that satisfy some of these requirements. But the entities created must provide roles for private sector experts that are assured, and not dependent on the discretion of the DHS Secretary or other government officials. In addition, these entities should be given functions and authorities that go well beyond those of a conventional federal advisory committee.