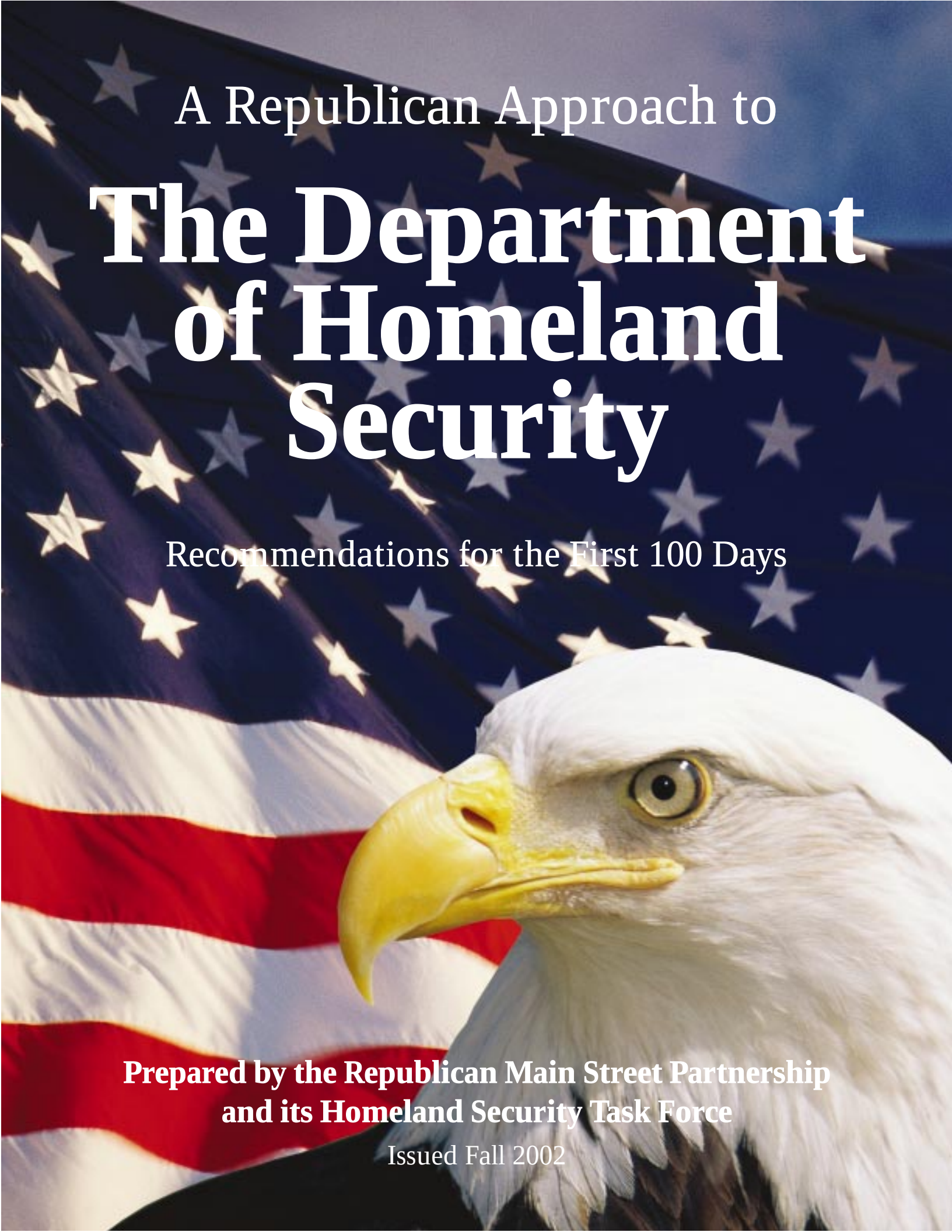


A Republican Approach to

The Department of Homeland Security

Recommendations for the First 100 Days

Prepared by the Republican Main Street Partnership and its Homeland Security Task Force

Issued Fall 2002

Homeland Security Task Force

Congressional Co-chairs:

Congressman Christopher Shays, CT
Congressman Doug Ose, CA
Congressman Rob Simmons, CT
Congresswoman Deborah Pryce, OH

Industry Co-chair:

David Zolet, TRW Inc

Task Force Members:

Sarah Chamberlain Resnick, Republican Main Street
Jason Foster, Republican Main Street
Darryl Fraser, TRW Inc.
Pete Perkins, TRW Inc.
Lauren Heller, TRW Inc.
Gina Bancroft, EDS
Marshall Williams, General Dynamics
Susan Phillips, Nortel Networks
Skip Roberts, SEIU
Robert Masciola, SEIU
Andy Mekelburg, Verizon
Helena Hutton, 3M
Thomas Spangler, ADA
Julie Scott, ADA
Frank Orlandella, Agilent
Elvia Morales, Agilent
Tom Moskitis, American Gas Association
Eileen Kean, Bond & Company
Andy Madden, Bond & Company
Michael Parr, Dupont
Thomas Bruderle, Health Underwriters
Larry Estrada, Hewlett Packard
Jay Spector, NAIOP

Republican Main Street Partnership Board

Honorable Mike Castle
Honorable Susan Collins
Honorable Amo Houghton
Mr. Donald Kendall
Honorable John McKernan
Honorable Alan Simpson
Honorable Olympia Snowe
Honorable Fred Upton
Honorable Doug Ose
Honorable Rick Lazio

The Task Force membership endorses the direction and basic themes of this monograph. Although individual Task Force members may disagree with some of the specifics contained in this report, all members recognize the importance of discussing such issues and setting priorities for the new Department of Homeland Security. No one member, nor his or her professional association, should be held responsible for any specific recommendation included in this report.

Acknowledgements

The Republican Main Street Partnership would like to thank all members of the Task Force, particularly our co-chairs, for their efforts in producing this document. We also want to extend special recognition to the White House Writers Group for their role in the preparation and editing of this report. We especially appreciate the long and patient efforts of the Task Force and its leadership to manage the many difficult and controversial issues pertaining to Homeland Security.

A Republican Approach to

The Department of Homeland Security

Recommendations for the First 100 Days

TABLE OF CONTENTS

Executive Summary 1

Chapter 1 - Information Integration 7

Chapter 2 - Identification and Authentication 13

Chapter 3 - Border Security 19

Chapter 4 - Public Health.....25

Chapter 5 - Science and Technology.....31

Chapter 6 - A Note on Human Capital 37

Afterword.....39

EXECUTIVE SUMMARY

The First 100 Days

"We are today a Nation at risk to a new and changing threat."

President George W. Bush
National Strategy for
Homeland Security
July 2002

The dramatic and heart-stopping attacks of September 11, 2001 catapulted a new and unexpected challenge to the top of the U.S. national priorities list: protecting the United States homeland from terrorist threats. With President Bush's announcement on June 6 of his plan to create a new Department of Homeland Security by merging 27 federal agencies, the formation of the new Department became a focal point for long-range homeland security efforts.

The task of creating the new Department will be monumental. It will have to be organized even while we are waging the war against terrorism, and possibly in the face of a conflict with Iraq - circumstances that could only heighten the threat and the challenges to the new Department. One way or another, there will be no "grace period" in which the new Department can correct false steps or right a faltering start.

In tackling the problem of homeland security, the United States in general - and the new Department of Homeland Security, in particular - face a number of paradoxes. One of the most fundamental is this: the very characteristics that make U.S. society unique (and uniquely attractive to immigrants from all parts of the world) - our openness and personal liberties - are the same characteristics that make securing our homeland especially challenging. A second, corollary paradox, is similar: as we move to secure our homeland from terrorist threats we must take special measures and special care not to compromise or undermine those freedoms and that openness. Otherwise, we will end up destroying what we are trying to protect.

Since the 9/11 attacks, government agencies, think tanks, business groups, scholars and others have written a small library of material on aspects of the homeland security challenge. A comparable, though somewhat smaller, outpouring has accompanied the President's plan for the new Homeland Security Department. Many of these efforts have analyzed the critical functions that need to be performed (securing the airways and other transportation modes; securing our borders, preventing and coping with chemical, biological or nuclear terrorism, etc.). Others have assessed our strengths, weaknesses and critical needs in important areas of capacity and capability. Still others have offered advice on the organization of the new Department - sometimes pushing the creation of specific offices or bureaus to address the advocates' pet concerns.

In deciding to make another contribution to the growing body of literature on U.S. Homeland Security, the Republican Main Street Partnership and its Homeland Security Task Force were motivated to do something different.

- We wanted to look beyond the creation of the Department of Homeland Security and focus on early questions and issues that will arise once the Department has been formally established through legislation.
- We wanted to focus on a limited menu of priority actions for the new Department's first 100 days of operation.

- We also wanted to approach this subject from a different angle. With the exception of the chapter on Border Security - a subject of overriding priority that intersects with many others - we have addressed the homeland security challenge in terms of tools and capabilities applicable across the spectrum of homeland security missions rather than in terms of the missions themselves.

We hope that this approach will be an asset to the new Secretary of Homeland Security and his or her subordinates as they work to forge a coherent agenda for the Department under conditions in which every priority will seem immediate.

Themes

Several themes run through the six sections of this report - Information Integration, Identification and Authentication, Border Security, Public Health, Science & Technology, and a note on Human Capital.

"SYSTEM OF SYSTEMS." President Bush's National Strategy for Homeland Security recognizes, and our report underscores, that in order for our efforts to be effective we must take a "systems engineering" approach to the homeland security challenge. What do we mean? In any emergency like the one that gripped the nation in the months after 9/11, there is a natural tendency to embrace specific solutions to evident vulnerabilities - pieces of equipment, a specific technology, a new procedure. The trouble is that if we think about it carefully, the 9/11 attackers succeeded by analyzing our systems - airline reservations and ticketing systems; systems of airport security; patterns of cross-country transportation; the operation of the air traffic control system; procedures for handling aircraft hijackings; etc. They analyzed our systems, found their weaknesses and exploited them to produce catastrophic consequences.

We can only hope to defeat future threats if we take a comprehensive view of how the different systems that are key to homeland security operate and how they relate to and interact with one another. As in other complex problems, focusing on individual "point solutions" will lead to sub-optimal overall results. Consequently, we need to see the homeland security challenge as the operation of a "system of systems" designed to thwart terrorists and that are continuously reviewed for weaknesses and exploitable vulnerabilities. We need to see it as a system where advances in one field - e.g., biomedical research on biometric identifiers - can contribute to breakthroughs in other fields - e.g., border security. Only this mindset will enable the responsible officials to have a sufficiently comprehensive view of the challenge to implement and upgrade systems of protection. As David Zolet, Vice President for Civil Systems of TRW Systems observed, "Homeland security demands a systematic approach involving the best of government, industry, academia and the American public all working together to protect the safety of our citizens and our way of life."

CHALLENGING TRADITIONAL PARADIGMS. In several areas we examined - but most notably in the area of identification and authentication of individuals - our homeland security challenge also gives us an opportunity to think outside of and transcend traditional paradigms. Too often in the past we have found ourselves locked in polarizing debates over whether the government's maintaining more personal data on individuals in the name of security is worth the loss of privacy and the erosion of constitutional freedoms that it might entail. Too often, as well, we find ourselves trying to make incremental improvements on admittedly faulty, patchwork systems - sometimes systems that were never intended to serve the purpose to which they are being put. Efforts to

improve upon and make more fraud-resistant state drivers' licenses, which are now often used as a sort of de facto national identification, fall in this category. Our examination leads us to conclude that we now have opportunities to pursue wholly different approaches to problems like individual identification and verification - approaches that neither concentrate more personal data on credentials individuals carry with them nor aggregate personal data in government or private databases. These approaches should be explored as a matter of priority for they could promise an early exit from paralyzing debates and enable us to reconcile conflicting interests.

TECHNOLOGY ASSESSMENT. In virtually every facet of the homeland security problem we examined, we found areas where promising technologies could make a major contribution. Considering the vastness and diversity of the homeland security field, it is evident that most of the technology that must be developed will be supplied by the private sector. One consequence is that the new Department needs to think of technology development in this field more in the context of a government-business partnership than as a wholly government directed effort. The Department will, therefore, need to determine what applicable technologies are "on the shelf," which are in development, or which are critically needed but not yet invented, and will need to set some priorities for their adaptation or adoption. This "technology assessment" challenge can be seen as a three-dimensional matrix. The dimensions of this matrix are the following.

1. Homeland security missions (transportation security, border security, protection against biological, chemical, radiological and nuclear terrorism, etc.)
2. Departments, agencies, and private sector entities that possess or offer relevant technology (e.g., the Departments of Defense and Energy, the intelligence community, the FBI and federal law enforcement communities, national laboratories, universities and other research centers, and private firms)
3. The maturity or availability of the technology (e.g., "on the shelf;" under active development; not yet invented).

Of course, technology development must be undertaken against a set of purposes and goals if it is to be useful. Consequently, side-by-side with our recommendations for early technology assessments in many fields by the new Department, we also call for development of a technology "road map" for specific functions - a desired security end-state and a time frame in which to achieve it.

ARCHITECTURES AND STANDARDS. An essential, early role for the new Department will be to define single integrated architectures for such key functions as communications and data systems that must be interoperable to achieve effective detection, prevention, and response. State and local authorities will turn to the new Department to set standards, both for the interoperability of equipment and data systems and for training and preparedness. The new Department of Homeland Security will face a formidable task in this area, again stemming from the diversity of activities, agencies, and current and candidate systems that require integration. But since interoperability and integration are the keys to success in the homeland security mission, the Department will have to rise to this challenge.

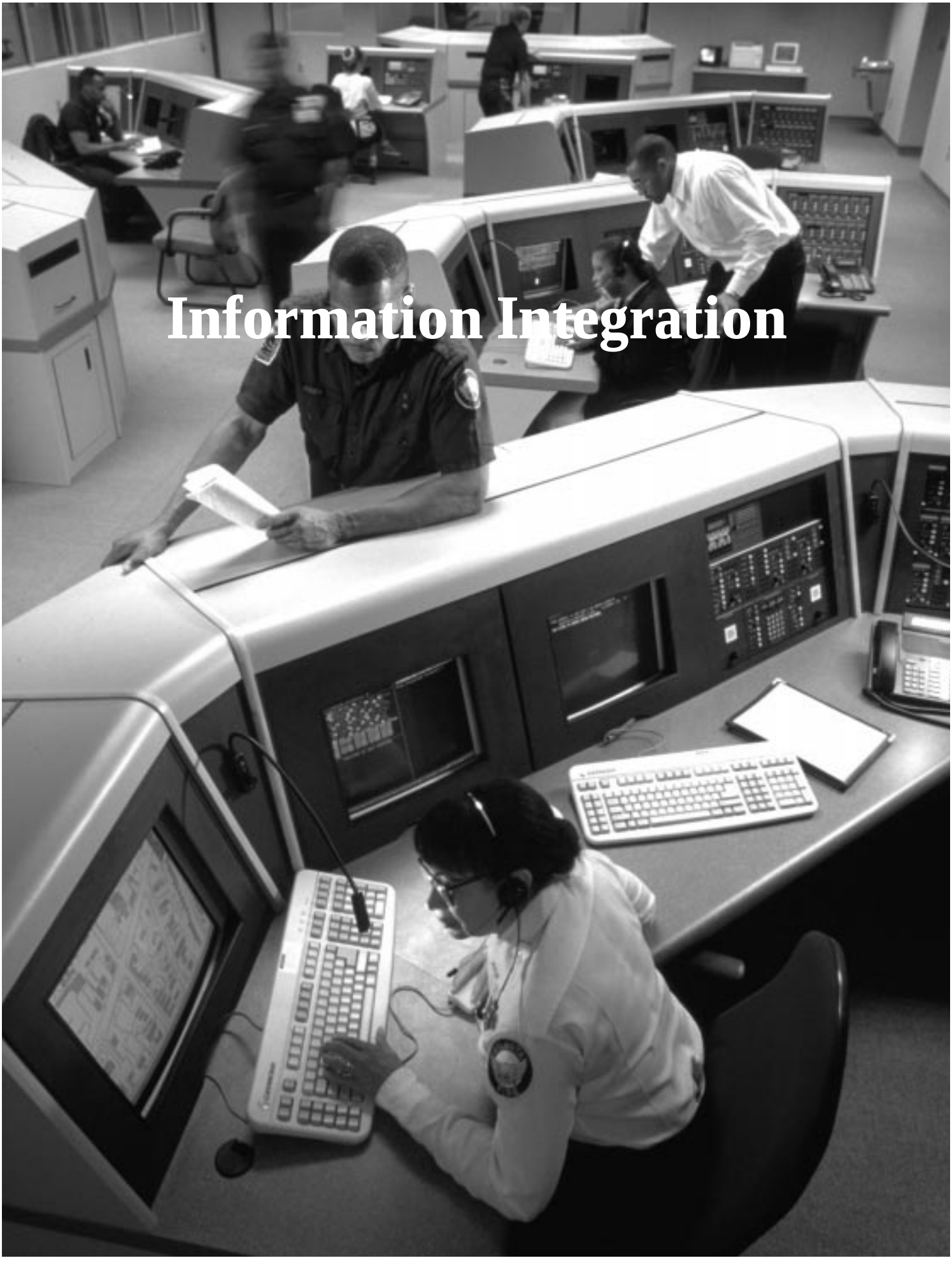
GETTING THE ORGANIZATION RIGHT. Fundamental to success in establishing architectures and standards and effectively assessing relevant technology is the challenge of getting the Department of Homeland Security off on the right organizational footing. This means different things in different fields. As discussed below, in the area of Science & Technology (S&T)

it means ensuring that the Department's Under Secretary for S&T wields centralized budget authority for technology research and development over all the component agencies of the new Department, backed up by a Chief Scientist and an outside scientific advisory board to prioritize the Department's research and development activities. In the area of public health, it means something different - working out a cooperative, collaborative relationship with the Department of Health and Human Services, which will maintain primary responsibility for these issues day-to-day, while carving out the new Department's specific responsibilities in the areas of threat monitoring, alerting, and developing new detection capabilities and new remedies.

As it approaches the formidable task of merging multiple agencies and disparate cultures, the new Department's managers would be well advised to draw on the experiences, lessons-learned, and best practices from corporate mergers. Many of the challenges that lie ahead for the new Department are analogous to those faced and surmounted – with differing degrees of success – by scores of companies in recent years. In so doing, however, the new Department's leadership should keep two key principles in the forefront. Where the new Department has the mandate to lead, it must organize itself to lead vigorously. Where the new Department can only succeed through cooperation and complementary efforts with other Departments and agencies, it must work from the first day to establish smooth collegial, non-competitive relationships.

LEADING THE PUBLIC DEBATE. Many measures required to tighten security at home have the potential to erode personal freedoms that we as Americans enjoy. Our wartime experience has shown that in the past, Americans have accepted reasonable and temporary limitations and inconveniences so long as they were manifestly necessary, clearly related to emergency needs, and explained and justified by officials through public dialogue. Key to achieving public acceptance of and cooperation with the new Department of Homeland Security's role will be for the Department to institute almost immediately on its inception channels of public communication and dialogue about the security challenges we face and the means to overcome them.

We hope that our task force's recommendations for the new Department of Homeland Security's first 100 days, outlined in the chapters that follow, aid the Department's senior managers as they embark on the most vital mission of our government today – protecting the safety of our citizens and the way of life that we enjoy as Americans.



Information Integration

CHAPTER 1
INFORMATION INTEGRATION

Scope of the Challenge

Fostering information integration - the interoperability of systems and sharing of data - is among the most important tasks of the Department of Homeland Security. Implicit throughout the President's National Strategy is the understanding that the federal government needs to vastly enhance its capacity to share appropriate information among departments, agencies, states and municipalities, and to establish standards that make data systems interoperable. The root of this need is fairly straightforward: the Departmental and agency structure of the federal government, and the separate structures of state and local governments, create a series of information "stovepipes." Within these agency structures, information tends to flow up and down much more easily than it does laterally to other agencies or to state and local authorities. As Rep. Christopher Shays (R-CT), remarked: "Bridging the gaps now limiting the effectiveness of federal, state, and local communications systems is a domestic security imperative." The President's National Strategy for Homeland Security recognizes this when it says, "We must build a 'system of systems' that can provide the right information to the right people at the right times. ... With proper use of people, processes, and technology, homeland security officials throughout the United States can have a complete and common awareness of threats and vulnerabilities as well as knowledge of the personnel and resources available to address these threats."

The task is both urgent and highly sensitive. In making it easier to access data and share information among law enforcement and public health officials, extra measures must be in place to assure the public that private information about citizens is not misused or that confidential intelligence or law enforcement material is not compromised. This aspect of the Department's work must always remain in the foreground.

Data sharing and interoperability are complementary activities, but they are not the same thing. Data sharing is a matter of policy. Interoperability is a matter of technology. The American people are looking to the Department of Homeland Security to address both aspects of this "information integration" challenge. The scope is large. Issues of data sharing encompass questions of law enforcement, foreign intelligence, interagency communication, public health, communication with state and local law enforcement and first responders, border security, and civic emergencies.

Beyond data sharing and systems interoperability, however, there is a further requirement. We need to be sure to invest in adequate analytical capability within the new Department to ensure that we can turn data – raw point observations – into information – interpretations and assessments that can serve as a basis for action by decision-makers and security personnel.

To cope with these challenges, what is needed is a "systems engineering" approach to putting in place the policies, adequate budgets, and the best technology to make the information we have more readily accessible to those who ought to have it.

In approaching this vast set of issues, the Department should focus on the following tasks during the first 100 days:

- *Assess the existing models* of data sharing already underway within the federal government and judge their efficacy.

- *Establish standards,* techniques, and protocols across the federal government to achieve a uniform policy on data sharing.
- *Improve spectrum allocation* to facilitate communication among federal, state, and local agencies.
- *Provide information* to government officials, public health and emergency coordinators, and the public about standards for data sharing and data sharing technology that should be adopted.
- *Improve data sharing* between state and local governments and federal agencies that deal with homeland security.
- *Distinguish between data that should be shared and that which should not be shared* with a focus on the protection of privacy and civil liberties.

Assess Existing Models

Interoperability and data sharing are already well-established, long-term efforts within the federal government - now prominently associated under the banner of "information integration." The Department of Homeland Security must not waste resources duplicating what has been tried and tested. At the outset of its work, the Department must assess how much data is currently shared between departments and agencies and the reasons why some data is not shared. It must also assess which data sharing programs are working, and why, and where failures and omissions occur, and why. This government-wide assessment is a necessary task to determine the priorities of the Department.

Similar assessments must also be initiated to determine the state of "vertical" data sharing between federal offices and state and local officials in both law enforcement and public health. As Rep. Rob Simmons (R-CT) has noted, "Our information systems stand as a critical link to the timely and effective coordination and communication between all levels of government. Accordingly, we must improve our "vertical" and "horizontal" communication and data sharing for our law enforcement, immigration, intelligence and public health surveillance enterprises, as well as ensure that state and local first responders use compatible communications equipment." Currently the federal government has both the information and technology to disseminate vital information (the location of hospitals or laboratories, for example) that could prove critical if it could be accessed in real time by local officials during their response to public emergencies.

In addition to these assessments, the Department should immediately examine the ongoing data sharing and interoperability models currently established in the federal and state governments and with private industry. The Department of Defense, for example, has already established procedures across the Department for information management, architecture standards, and intelligence handling. The Department of Homeland Security must first examine these systems to see if they can be expanded across the federal government. Similarly, the Centers for Disease Control and Prevention are in the final stages of launching a health alert network. This type of data sharing may be the basis of further enhancements in public health data sharing. There are also ongoing data sharing programs between the Department of Defense and the state National Guards, and between the Justice Department, the U.S. intelligence community, and local law enforcement. These programs must be candidly assessed for their strengths, weaknesses, and applicability to the Department's mission.

The complex issues confronting the Department of Homeland Security require the Department's leaders, the President, and his White House

advisers to make difficult and equally complex policy choices. There are trade-offs between the widespread sharing of information, even at different levels or compartments of sensitivity, and the risks of compromising intelligence assets or methods, law enforcement operations, or prosecutorial information. One important focus of the Department's effort should be to concentrate on technologies that can simplify policymakers' choices on these trade-offs. The Department should look for technologies that more effectively compartmentalize and protect information to be shared, and approaches that minimize the risk of compromising information, techniques or operations when data is shared or information systems are integrated.

Establish Standards

Exercises in data sharing are stymied when there are no common standards, techniques, or protocols to be used by various information gathering systems in government. It should be the primary responsibility of the Department's Chief Information Officer to begin establishing those standards on how information is handled, identified, and managed. These standards, often known as "meta-data" standards, exist in private industry and within federal departments and communities of interest. These must be reviewed to determine the best practices and their possible application to a broader set of federal activities.

Similar standards are needed for the technology that is used. The Department should take the lead, with the cooperation of the Departments of Defense and Justice, the intelligence community, and other relevant departments and agencies, in developing a single federal architecture for voice, data, and imagery sharing among federal departments and agencies - the goal of today's Integrated Wireless Network (IWN) program. One fruit of this effort should be establishing a single common format for packaging and transmitting data to facilitate communication across departments and among state and local officials. A further result should be the identification, for replacement or elimination, of redundant or outmoded communications and data systems across the relevant federal departments and agencies. Yet another outcome should be the already mandated completion of secure video and voice links between federal authorities and state and local governments. Obviously, this effort must balance the imperatives of effective information sharing to detect, prevent, and respond to terrorism emergencies with the necessity of safeguarding sensitive information from compromise.

Improve Spectrum Allocation

One of the key requirements of enhancing Homeland Security is to ensure that law enforcement, Federal security services, first responders, and other key personnel have access to adequate, clear radio frequency spectrum to do their jobs. Increasingly, key portions of the relevant spectrum are becoming crowded and subject to intense competition from commercial users. The impending battles over frequency spectrum allocation will be key for determining whether federal, state and local agencies can count on having the needed communications in times of emergency - or even day-to-day.

While frequency spectrum allocation is the responsibility of the Federal Communication Commission - not the Department of Homeland Security - other agencies (the Defense Department, the FBI and law enforcement, NASA and the satellite operating community, etc.) enjoy long-established "places at the table" when debates and negotiations about spectrum allocation take place. As a newly formed entity - albeit one comprised chiefly of long-established subordinate agencies -

the new Department of Homeland Security will need to make establishing its "place at the table" for these negotiations a high, early priority. It will also need to review and establish a clear picture of the frequency spectrum needs of the Department, its subordinate agencies, and the state and local agencies with which it must operate and be in a position to make an effective case for those requirements. The stakes in this negotiation could hardly be higher, since so much of the effectiveness of our homeland security response depends on communications.

Provide Information

The creation of a highly functional, interoperable data sharing program within the federal government is a long-term project. In the near-term, the Department of Homeland Security ought to become a clearinghouse of information on interoperability standards that all government agencies at every level can access. This could be as simple as informing state and local law enforcement agencies of the appropriate communications technology they should select in order to become interoperable with larger, relevant federal data bases. The purpose here is to use the broad assessment and survey powers of the Department to create a central dissemination point of information about leading practices, standards, protocols, and technologies even before final data sharing policies are in place.

Improve Data Sharing

The Department should regard the sharing of data between the federal government and state and local officials as a top priority. This should become a more accessible two-way communication channel that allows federal government agencies to share data with officials at the local level and permits those same officials to communicate readily with the federal government. The events of September 11th highlighted the difficulties of the various law enforcement systems communicating with those used by first responders. As Rep. Fred Upton (R-MI) remarked: "It is important that first responders have all the right tools. One way to do that is through communication."

Efforts now underway within the Treasury Department to create a fully integrated communications network capable of serving the highly diverse needs of its multiple subordinate agencies may provide a useful model for federal government-wide efforts in this field.

The key to any such government-wide effort will be establishing a single national architecture that can support parallel planning and implementation.

Protect Data

As the federal government moves to share data more widely and fluidly among departments and agencies for terrorism prevention, it is imperative that dramatic and publicly visible steps be taken to assure the public that civil liberties and personal privacy will not be compromised through this effort. One important step in this direction - one that the new Secretary of Homeland Security could begin work on immediately upon assuming office - would be the development of a draft Executive Order for the President's signature promulgating guidelines governing privacy protection as wider information sharing is implemented. Issuing clear guidelines prominently, backed up by the establishment of regular channels of communication with the public about this sensitive area, would be extremely valuable in allaying public concerns.

Recommendations for the First 100 Days

- Fully fund the Department of Commerce's Critical Infrastructure Assurance Office's Technology And Evaluation Program - funding for which is in jeopardy in the pending appropriations process.
- Assess existing data sharing programs within the government, academia, and private industry, identifying areas for significant improvement within the federal government and between it and state and local levels, with particular focus on shortcomings and needs in emergency situations.
- Establish a single national architecture for voice, data, and imagery sharing to be used by federal authorities and with state and local governments (including completing a secure video conferencing capability between federal and state and local officials).
- Clarify guidelines and protocols for information sharing that promote the freer interchange of information while safeguarding information that cannot be shared.
- Establish an information clearinghouse on interoperability standards and technology now in use.
- Develop a draft Executive Order specifying guidelines to protect personal privacy and civil liberties as federal agencies pursue expanded anti-terrorism information sharing; establish a regular program of communicating with the public.
- Ensure that the Department of Homeland Security has a "place at the table" to advocate for the frequency spectrum requirements of law enforcement, security services, first responders, and other emergency personnel based on a thorough assessment of their future communications needs.

Identification and Authentication

CHAPTER 2
IDENTIFICATION AND AUTHENTICATION

Scope of the Challenge

Identification and authentication are the foundation of not only law enforcement efforts aimed at enhancing homeland security, but also of virtually all non-law enforcement activities relating to security. Thorough and accurate identification procedures permit us to determine whom a person is and if they are who they say they are. Such questions are essential in dealing with U.S. citizens, legal visitors, illegal aliens, and any foreign national who arrives at our borders seeking entrance.

The role of the Department of Homeland Security in identification and authentication issues is highly complex. There are already dozens of identification programs and technologies used every day in the United States - from terrorist watch lists at borders to drivers' licenses, agency identification badges, and building access control devices. Clearly there is a need to harmonize some of these systems so that it is possible to more easily determine whether someone flying on a plane, crossing a border, purchasing a weapon, attending a school, or entering a government building might be doing so under a false ID.

Yet the precise role and activities of the Department on this front needs to be clarified. Is the Department a forum for policy discussion about ID programs? Is it an implementer or incubator of new technology? Is it a keeper of data? Is it a coordinator for federal agencies? What role does it play in setting policy in this arena?

In determining what role it will play, the Department should focus on the following points immediately since they will help determine the policies and initiatives the country pursues to enhance its identification and authentication capacities:

- *Assess existing technology* used at every level of government and in the private sector to determine and authenticate identity.
- *Establish a long-term architecture* for identification technology and standards to permit interoperability and enhance effectiveness of current "stovepipe" identity systems.
- *Establish a long-term technology* program to make the best use possible of new and existing technologies.
- *Lead public discussion* about identification policies and establish safeguards against the abuse of personal data and identification material.
- *Strengthen procedures for identification of foreign citizens* seeking to enter the United States.

Assess Existing Technology

The focus of this assessment should be to determine how vulnerable the existing identity and authentication methods are to being subverted by domestic or foreign terrorists. When coupled with a threat assessment, this provides a roadmap to the most critical areas of the nation's overall identity infrastructure.

The federal government, along with state and local law enforcement, use dozens of independent

methods for determining someone's identification. From drivers' licenses to company ID cards, there is no uniform method of confirming an individual's identity, nor is there any method by which one agency or office can authenticate an identity when someone might be using false documents to disguise themselves. In approaching this plethora of documents that today are commonly used for identification, authorities are broadly confronted with two major choices.

- First, whether to concentrate on incrementally improving today's "patchwork quilt" of different identity documents and data (drivers' license records, Social Security Numbers, and the like) or to pursue an alternative paradigm that avoids the vulnerabilities and limitations of trying to link these disparate databases; and
- Second, whether to concentrate effort on "hardening" identity documents themselves and encoding them with more privacy-sensitive data to improve verification, or to rely more on verifying document information against separate, secure identification registries.

The Department of Homeland Security needs to immediately assess the various methods for authenticating identification. It should examine the existing use of biometric identification and the areas where its expansion is needed. It should also catalog the existing technologies used at every level and assess their ability to be improved and their capacity for interoperability. The Department needs to weigh the advantages of creating a new, backbone system that could be used as a source of authentication by ID-granting offices in any location as an alternative to pursuing isolated, incremental improvements in today's "patchwork quilt" of identification mechanisms.

Establish a Long-Term Identity Architecture

The single greatest obstacle to the creation of a highly reliable identification system is the absence of an overarching architecture and a set of standards that could be used by federal agencies, local law enforcement, and private organizations that grant ID documents. Today's "identity infrastructure" is best described as a set of "stove piped" systems, each representing a point solution for the specific needs of the sponsoring organization.

The Department needs to assess alternative architectures that could enhance security via more integrated approaches. Central to this dilemma is the fact that, within the federal government, no single agency or office is actually "in charge" or responsible for the identity and authentication issue. Rather, individual issuing agencies - ranging from the State Department's passport office at the federal level to drivers' license bureaus at the state and local level - set their own standards, independently determine what underlying documentation will authenticate an application for a credential, and maintain their own data bases of document-holders. The Department of Homeland Security should be designated to lead the federal effort to sort out and systematize the thicket of identity documents recognized and used in the U.S. Far from establishing a national identity card - a neuralgic subject that inevitably excites concerns about privacy protection and undue government surveillance or intrusion into individuals' lives - the Department should instead concentrate on solutions that would "bring order out of chaos" in the issuance and recognition of identity documents. To this end, the Department should convene commercial and government agency representatives and quickly develop a plan for this effort.

The range of alternatives extends from the current "stovepipe" approach to a highly centralized national identity system to a far more distributed system that allows existing systems to reference a common registry of birth data. For example, without replacing the multiple identity mechanisms that are in use today, and without creating a much-feared central government database that aggregates significant amounts of private information, a registry database of birth certificates could be created (either centrally or via linked state databases) that includes biometric information and provides a method by which the existing identity mechanisms could be made uniformly more secure.

Such a registry would not be a "national ID file" actively collecting personal information about citizens. Rather, it could be an incremental improvement on existing birth records via the collection of biometric data such as thumbprints or fingerprints that (1) matches names and birth records with biometric ID material and (2) supports one-to-many comparisons of that biometric data to ensure that people are registered only once in existing databases.

Such biometric data is already widely used in law enforcement and has been mandated for use at border crossings. But to have an effective homeland security strategy, the Department must begin shaping the architecture of such a system so that authentication solutions could be built around it. Today there are simply too many competing databases of information that are not interoperable or that contain surplus personnel data that is unnecessary for homeland security purposes.

Establish a Long Term Technology Program

Any identity solutions created today will have to adapt to the realities of continued technology advancement. This advancement must be considered in determining the best long-term architecture for identity solutions, and it must be assessed on a regular basis to determine areas of potential vulnerability. The Department must assess its role in such a technology program. Will it conduct research and assessment activities directly? Is it the sponsor of research in this arena? Is it a facilitator (for instance, by sponsoring public databases of test data that stimulate technology development)? How much core competence is required within the Department and how much can be reasonably outsourced? The Department must either lead this effort or appoint a subordinate agency to be the organization responsible for carrying out the above tasks.

Regardless of the role the Department plays in any research efforts, it must assess the probable range of future technology capabilities and incorporate such forecasts into today's policy decisions.

Lead Public Discussion

The goal of any identity technology - biometric or otherwise - is that it be (1) low cost; (2) fast; and (3) accurate. We must recognize, however, that an identity technology regime that is free, instantaneous and perfect still may not be embraced in the face of public distrust and opposition that is not intelligently and sensitively addressed by the sponsoring government agency. This engagement is not optional. In fact, we would go so far as to suggest that the path the nation is now on in the area of identity management is neither sustainable nor practicable, in the face of public opposition to current approaches to identity management on the scale envisioned for homeland security applications.

Discussion of a national system of identification understandably and rightly concerns citizens who may fear that, in the name of homeland security,

the new Department is collecting excessive information on individuals and increasing its accessibility. Though that is a valid concern, it is not the purpose or role of a central ID authentication system. The Department of Homeland Security has an obligation to lead a national discussion about new and promising technologies for ID, how they might used, and how various organizations (both commercial and government) might be limited from collecting, analyzing, or distributing detailed information about U.S. citizens. Providing safeguards against abuse of identity systems could become the responsibility of the Department on an ongoing basis.

Procedures for Identification of Foreign Citizens

Every day thousands of foreign nationals enter the United States legally. The methods of identifying these people range considerably. Paramount in addressing this issue is determining how the U.S. will interact with other countries in the identification process. For example, what identifications standards will the U.S. accept based on the concept of reciprocity? The Department of Homeland Security should quickly establish which documents are to be accepted for entry into the United States and under what circumstances. Passports, visas, border crossing cards, and driver's licenses are in use now and none check a biometric beyond a photograph.

Systematizing documentation for foreigners' entry into the United States is fundamental to fulfilling the mandate of the Department of Homeland Security's Immigration and Naturalization Service to implement an entry-exit tracking system at the borders, with the initial phase to be in place by the end of 2003. This phenomenally complex task can be accomplished - and the resulting system can function reliably - only if we have clear and consistent requirements for identification at the border, and have set those requirements with an eye to ensuring effective authentication and minimizing fraud.

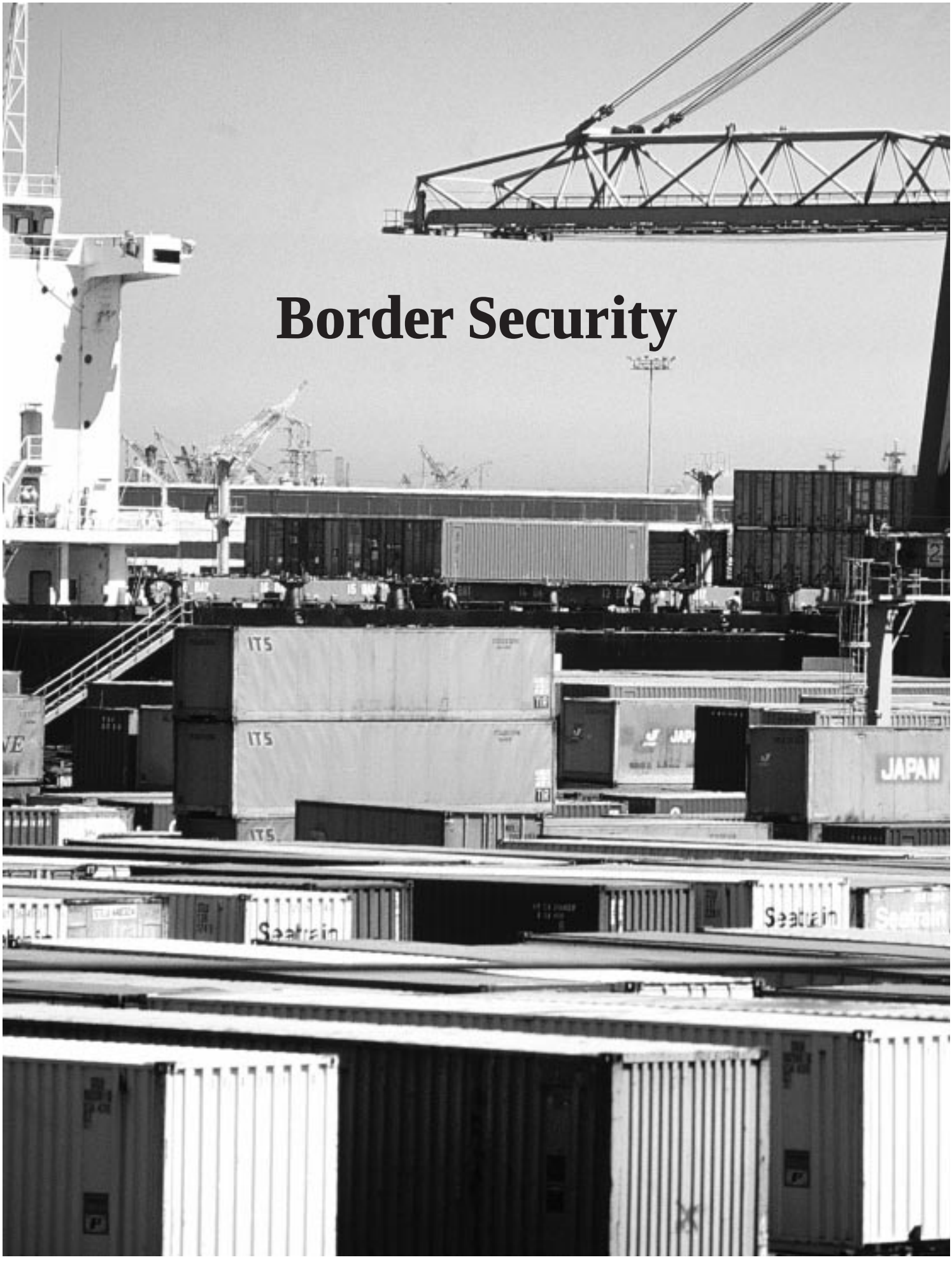
The effort to systematize immigration documentation for foreigners involves wider issues. For example, how will we reconcile our need for stricter, standard information on foreign entrants to the United States with our "visa waiver" program that exempts visitors from most Western, developed countries from obtaining visas before entering as tourists? How will we reconcile our information ambitions about foreign visitors with the realities of political asylum-seekers, who may arrive with little or no proper documentation? What is the U.S. willing to demand of other countries in terms of standardized data, given the potential economic impact if countries are removed from the visa waiver list? Also, what degree of law enforcement cooperation can the U.S. expect from other countries (e.g., searching of visa applicants' fingerprints against the host nation's criminal database)? Finally, will the U.S. take an active role in helping other countries to establish identity databases in those host countries as a means of upgrading U.S. security? The cumulative impact of these questions and others will force a reexamination and revamping of the visa waiver program now in effect for many advanced, developed countries to ensure that it does not become a "back door" for terrorists.

The issue of identity authentication is one of the most perplexing, yet critical, issues we must address if we are to improve our homeland security. The issues of reciprocity and speed and convenience of international travel are far reaching and complex, and the issues of personal respect and sensitivities to procedures like fingerprinting (associated in most peoples' minds with criminal investigations) are formidable and important. Work is currently underway at the National Institute of Standards and Technology (NIST) to

determine relevant standards for using fingerprint or other biometric data to verify foreigners' identities. Pending the completion of this work, and in order to begin building comparable data on foreign travelers to the U.S., the State Department should begin to collect fingerprint data from all persons granted visas to enter the U.S. These steps will, in turn, put a premium on adequately equipping, training and funding U.S. consulates abroad to cope with these heightened screening requirements.

Recommendations for the First 100 Days

- Establish the proper role for the Department in identification and authentication issues.
- Assess all current technology in identification, its limitations, and the possible scenarios of technology advancement.
- Establish a set of standards and a technology architecture that would be interoperable with existing systems of providing and verifying identification.
- Create a public forum where citizens can understand new technologies and be assured that the system cannot be abused.
- Direct the State Department to begin taking fingerprints of everyone who is granted a visa.



Border Security

CHAPTER 3
BORDER SECURITY

Scope of the Challenge

Of all the issues that comprise Homeland Defense, border control poses perhaps the most significant challenge not simply to U.S. security, but to our Nation's vision of what it means to be an open society. Securing our borders, while at the same time preserving the maximum degree of freedom of movement and travel, will require the focused efforts of the Department of Homeland Security, in coordination with all other security agencies of the U.S. Government. As Rep. Doug Ose (R-CA) observed, "Keeping our borders secure from terrorists is a top priority to ensure homeland security. To achieve this we will need better intelligence, international cooperation, and the right tools in the hands of law enforcement to be able to apprehend those who try to enter our country illegally." In addition, Governor John Hoeven (R-ND) noted, "As we work to build our borders of the future to ensure greater security we must also ensure border operations are efficient and meet the needs of our travelers and industry."

With the world's longest undefended borders (over 7,500 miles for Canada and Mexico combined), over 95,000 miles of shoreline and navigable waterways, more than 500 million people crossing U.S. borders each year - more than 60% of whom are non-citizens - and more than 58,000 cargo containers entering the U.S. each week, securing the United States' borders is a formidable task. To compound the challenge, the U.S. maintains relatively open borders with 37 international airports and dozens of seaports, while offshore outposts in the Caribbean and the Pacific, once entered, ensure unfettered onward access to any domestic destination in the U.S.

Policing the entry of people and products at the physical borders of the U.S. provides little room for error, given the challenges that face the U.S. Government in effectively following the movements of people and, to a lesser degree, products, once they have entered the United States.

This chapter will argue that border security can be enhanced in four general ways:

- *Employ a "forward strategy,"* by initially monitoring the movement of people and goods entering the U.S. at foreign locations - thereby lengthening the time border authorities have to assess/evaluate potential threats.
- *Enhance systems integration* to improve real-time information sharing, which in turn implies a greater standardization of policy, practice and protocols in information-collection between U.S. government agencies at all levels, and with friendly foreign governments.
- *Deepen targeted tracking capabilities* for watch list individuals while in the U.S., networking various public agency and private/commercial databases to flag behaviors inconsistent with the stated purpose of an individual's visit.
- *Improve the means and methods used at ports of entry to screen people and cargo.*

In addressing each of these priorities, the border security challenge must be met with due appreciation to key values associated with the movement of people (privacy, security of personal

information, ease of transit) and products (commercial efficiency, speed and reliability).

Technology constitutes a common thread running through all aspects of the border security challenge. Given the ways technology advances can drive security improvements, the new Department must commit to a continuous technology assessment effort, measuring existing systems against new capabilities, with the aim of migrating superior technologies into an integrated border security architecture.

Forward Strategy: Border Extension

Potential border security problems can be sharply reduced if U.S.-bound travelers and cargo are screened well before arriving at physical U.S. borders.

In terms of the movement of people, border extension will require enlisting the cooperation of friendly nations to strengthen the security screening process at departure points for U.S.-bound flights and ships.

In terms of the movement of products, extending our borders will require strengthened screening processes at non-U.S. cargo loading areas for inbound goods. The U.S. Customs Container Security Initiative, which focuses on strengthening screening efforts at the top 20 "mega ports" that account for two-thirds of all U.S.-bound sea container traffic - and allows the stationing of U.S. Customs screening agents at participating international ports - is a strong first step in this direction.

Border extension does more than shift the task of "information capture" abroad; it effectively lengthens the time U.S. authorities have to assess the information they collect. Given the volume of border traffic in terms of both people and products, time can be a critical tool in deterring terrorism.

Enhanced Systems Integration

In our post-9/11 world, U.S. border control authorities are faced with the challenge of securing borders, while maintaining an efficient flow of low-risk travelers and commercial trade. In each instance, improved information sharing and improved security measures will be key to processing inbound people and products in ways that ensure security, with minimal adverse impact on ease of transit. Governor John Engler (R-MI) noted that already, "Our strong relationship with Canada has resulted in significant border security improvements. These changes have improved homeland security and will continue to result in faster border crossing times."

One step the new Department of Homeland Security should take is to do a quick review of the best practices of foreign governments – for example, Israel's – in terms of screening arriving people and goods, looking especially at how these nations get their agencies to coordinate effectively.

In terms of the movement of products, U.S. authorities should focus on standardizing cargo manifest data, and integrating that data into the larger shared-information system. Given that goal, the use of new technologies to screen cargo and seal containers, both abroad and at our borders, will be vital to improved security. As a complement to enhanced procedures, increased penalties for shipping infractions could serve to incentivize private-sector compliance with new security regimes. In any case, any new initiatives would need to gain private-sector support by contributing to the timely movement of goods across international lines. In this regard, the new Department should move to capitalize on industry associations, trade unions and other stake-holders who could make a valuable contribution in setting priorities and achieving "buy-in."

In terms of the movement of people, there are currently many categories of travelers bearing multiple documents that allow entry to the U.S. Various kinds of visa holders, for instance, are processed for entry by U.S. authorities. These individuals are subjected to screening, but the extent of this screening is very much in question. We have individuals who arrive unannounced from visa waiver countries, with only their home country's identity or travel documents - in most cases, a passport. We have individuals who are refugees that arrive with little or no documentation. We have daily workers or business people with or without border crossing cards. We have individuals that are citizens of Canada or Mexico that enter with national identification alone. We have individuals and illegal entrants that arrive or are apprehended at our border with no form of identification. We have a tiny number that enter via the INS's "Trusted Traveler Program," called "INPASS".

Much of the work of validating travelers could be pushed back to the travelers' home governments, by either imposing and enforcing standardized travel documents for entry into the U.S. or by signing agreements with various countries to agree to use the same standardized documents. When a traveler reaches the U.S. border with a document adhering to these standards, the border security task is one of authentication - ensuring that the traveler is who he says he is - rather than trying to establish identification. The need to have a standard document, with some form of biometric, is key to making this verification work.

The objective for visa waiver countries should be a "trusted traveler program," with the following characteristics: voluntary enrollment, to alleviate privacy concerns; a strong enrollment process to ensure that only those who are truly entitled become part of the program; and continuous clearance, to ensure that those enrolled do not subsequently become part of a watch list. For all other countries, a combination of a "trusted traveler program" and a visa with verifiable biometrics should become the standard.

Congress has imposed new requirements to accurately register all entries and exits from the U.S. by persons traveling on foreign passports and travel documents. Information-sharing should include initiatives aimed at strengthening *exit controls*, with expanded information-collection and information-sharing between the U.S. and Canada, Mexico and the Caribbean countries in particular, which collectively account for a large percentage of visitors to the U.S.

Targeted Internal Tracking

Just as security is enhanced by a forward strategy of border extension, so too, is security advanced by expanding the ability to track the movement of goods as well as targeted individuals once they have been granted entry into the U.S. Together, border extension and internal targeted tracking move the U.S. away from the concept of a brittle border, a one-dimensional "firewall" that - once breached - allows goods and travelers free and unmonitored movement within the country.

In terms of the movement of products, technology and systems that strengthen cargo tracking to destinations deep within the U.S. would deliver significant security benefits. A fully articulated internal tracking system would require advanced systems integration with major transportation modes and the private and public entities that oversee movement of goods via rail, road, inland waterways and inter-state air freight in the U.S.

In terms of the movement of people, the key challenge in evolving targeted internal tracking capability is one of systems integration: Creating a "network of networks," comprised of both public and private/commercial databases, that would flag

certain types of transactions (credit card purchases, car rentals or hotel accommodations, for instance). While policies to protect privacy should govern the use of such tracking technologies, the use of such capabilities in tracking targeted watch-list individuals would significantly enhance U.S. security.

Improved Screening Means and Methods

Clearly, advanced technologies can play a critical role in enhanced border security, provided the new Department maintains an ongoing technology assessment effort that can integrate advances into the nation's existing border security architecture.

In terms of the movement of people, for instance, the use of biometrics in traveler identification - particularly more sophisticated forms such as iris scanning or DNA matching - can be used to make a one-to-one match of an individual against a biometric marker contained in a traveler's ID card or travel document. A focused effort in technology assessment should scour the technological landscape for new means and methods to identify and authenticate travelers seeking entry into the U.S.

In terms of the movement of products, consider the impact on cargo screening and security of a new technology that allowed positive identification of a shipping container, and verification that its contents were unchanged from a previous point of examination. Our security architecture must be open to incorporating such quantum leap advances, not wedded to prevailing legacy systems that permit only marginal improvements.

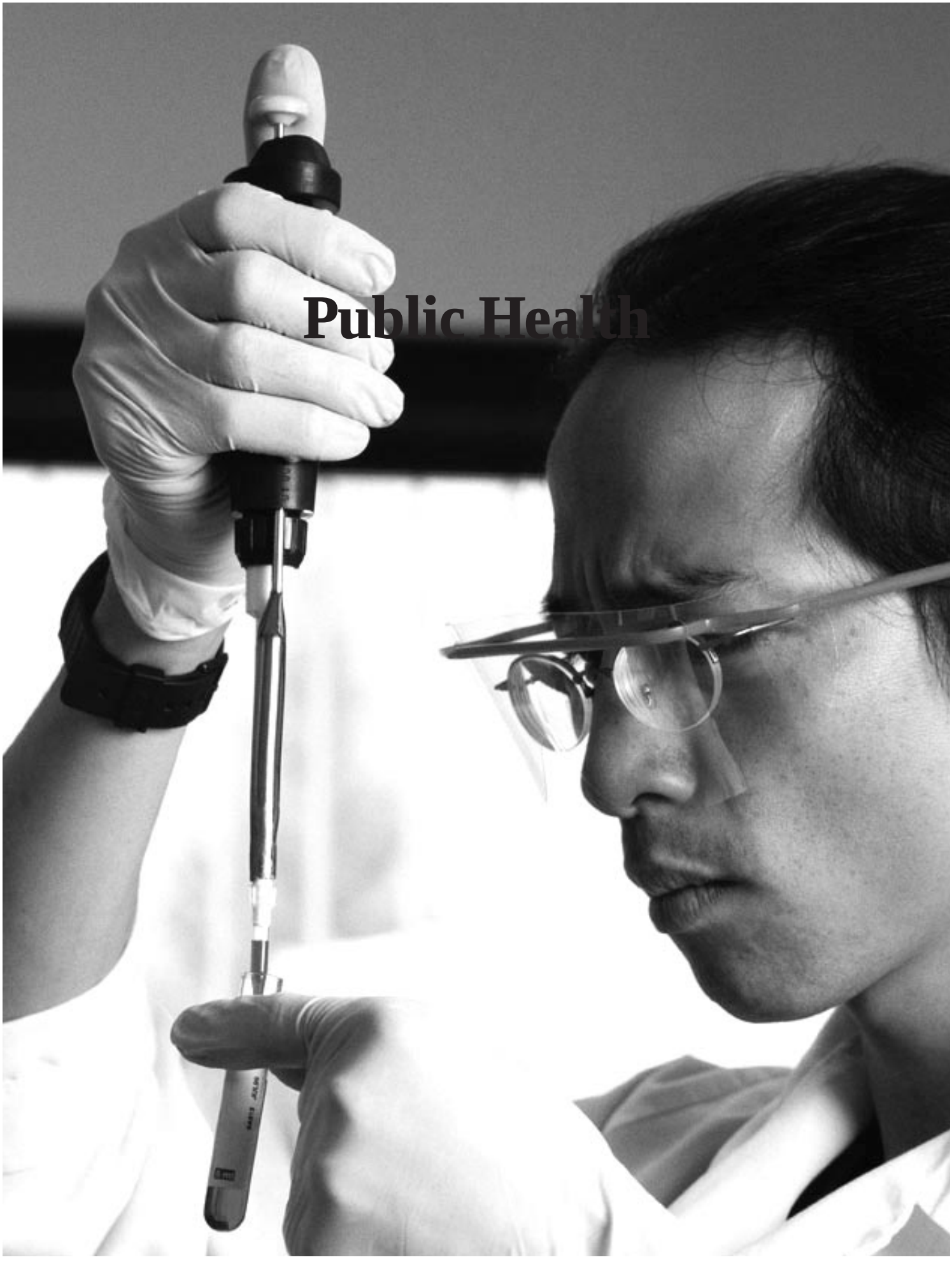
Recommendations for the First 100 Days

For the Department's first 100 days, we recommend:

- Establishing a plan to craft a *systems integration architecture* capable of evaluating border threats as presented by both the movement of people and products.
- Establishing a technology assessment plan, based on rigorous use of prevailing standards to ensure ***full interoperability*** of all information systems involved in border security, and
- Establishing a process for prioritizing *resource allocation* based on the highest threat scenarios.
- Examine the best practices of foreign governments in screening arriving people and cargo for lessons applicable to the U.S.

Longer-term, the Department should advance the view that U.S. funded and enforced programs be used for "border extension," to prevent unwanted travelers/high-risk cargo from reaching physical U.S. borders. The Department should also support as priority policies 1.) the establishment of minimum standards for non-forgeable travel documents/cargo manifests for entry to the United States;
2.) initiatives using biometrics to screen potential U.S. entrants; and
3.) initiatives expanding a targeted tracking capability for the movement of watch list individuals once within the U.S.

Public Health



CHAPTER 4
PUBLIC HEALTH

Scope of the Challenge

The 9/11 attacks and the anthrax attack that followed highlighted U.S. vulnerability to terrorism using chemical or biological agents or simply the release of infectious diseases into the U.S. population or its food or water supplies. As Rep. Christopher Shays (R-CT) put it, "Our nation has lived through the horrific consequences of a biological attack, as evidenced by last year's anthrax attacks. These attacks exposed our vulnerability to chemical and biological agents - vulnerabilities that place our food and water supplies at risk as well."

The specter of such a threat confronts public health authorities at all levels - and those responsible for homeland protection - with unprecedented challenges. Universally, public health systems have been geared to identify, contain, treat, and eliminate accidental outbreaks of infectious disease and to prevent them through vaccination. Water, sanitation, and food safety systems operate on similar premises. None of these systems - in the U.S. or abroad - has ever been designed to cope with an organized effort to systematically and deliberately introduce disease or contamination to cause maximum, widespread casualties. This is the new dimension of threat to public health in the U.S. brought by international terrorism.

Last year's anthrax attacks in Washington, New York, Florida, and Connecticut underscored additional dangers: specifically, that domestic criminals, cultists, deranged people, or extremist conspirators can also exploit the vulnerabilities of our open society to spread terror and economic disruption through disease or contamination. Measures effective against foreign terrorists should also protect against these criminal threats.

The very characteristics that make U.S. society unique - and uniquely attractive to immigrants from all parts of the world - are the same characteristics that make these public health challenges extremely difficult to meet. Adding to the porousness of our borders highlighted previously, the U.S. is characterized by:

- An open society with essentially complete freedom to relocate or travel within U.S. territory, including to wide open rural areas where the care and safety of livestock and food stocks rests in the private hands of individual farmers and commercial companies;
- A high degree of openness in our public facilities and widespread (though recently somewhat curtailed) information about critical infrastructure systems (e.g., water systems);
- Numerous facilities in society - akin to the postal system - that permit low cost, relatively anonymous access that could be misused to spread disease or contaminants.

The opportunities and risks are almost too numerous to mention - and the consequences of epidemic outbreaks of known diseases or newly synthesized agents are almost too gruesome to contemplate.

Our national health care system, as well as our animal health and food and water safety systems,

reflect the basic structure of U.S. society. These systems are highly distributed and dependent on local and state level institutions and private operators. They are predicated on the basic goodwill (as opposed to presumed malevolent intent) of virtually everyone. Although incorporating a preventive focus - particularly through childhood vaccination programs - the system is designed to react to reported incidents of illness, and it depends on higher-level state and federal authorities to correlate reported incidents and determine whether patterns indicate a wider public health consequence. In this system, a multiplicity of state and federal agencies share different areas of responsibility:

- 50 state public health departments (along with the District of Columbia, several large metropolitan areas, and the US territories);
- The Department of Health and Human Services (particularly its Office of Public Health Preparedness (OPHP), the Centers for Disease Control and Prevention, elements of the National Institutes of Health, the Health Resources and Services Administration (HRSA), and the Food and Drug Administration);
- The Department of Agriculture's Inspection Services and state-level agriculture departments (responsible for livestock health and meat safety);
- Municipal, county, and regional water authorities - as well as the Army Corps of Engineers - operating in conformity to Environmental Protection Agency Standards.

The list goes on.

It is into this thicket that the new Department of Homeland Security will enter as a new actor - one with a vital role of ensuring a higher level of public protection against an unprecedented - indeed, an unheard of - threat. But while the new Department will have a significant measure of responsibility in this area, its efforts will have to complement those of the Department of Health and Human Services, which will continue to have primary responsibility for the critical public health and food safety functions involved. What, then, should be the role and contribution of the Department of Homeland Security in the public health dimension of protecting Americans from terrorist threats? And what steps should the new Secretary and the Department take to begin performing that role in their first 100 days?

Lead Agency - But Without Primary Responsibility

In approaching the public health challenges of homeland security - particularly against terrorist attacks - the Department of Homeland Security will have to proceed differently than in the areas of its primary responsibility - transportation security, border security, nuclear incident and emergency response, and information sharing and detection. It will have to proceed with the recognition that:

- Unlike in these other areas, it neither has the primary responsibility nor the operational control over the relevant agencies and assets;
- Much of the public health response will be borne by local health care providers (e.g., the increasingly overloaded and under-staffed emergency departments of local hospitals), with most of this capability lying in the hands of private companies or religious or charitable organizations; and that

- It is entirely appropriate that the Department of Homeland Security not exercise primary responsibility in this area since the mission of public health is driven more by broader societal and human welfare concerns than by security.

Fostering Cooperation and Coordination

Consequently, the Department's role will need to be one of fostering cooperation, supplementing and improving existing channels of communication in areas of public health, food and water safety, setting (or catalyzing the setting) of new standards and procedures, and the like. The Department will have important missions in disseminating alerts and warnings to other federal departments and agencies, and state and local authorities, and in receiving, correlating and assessing information flowing up from state and local organizations. It will also be responsible for research and development of drugs and vaccines against bioterrorism and improved detection and screening technologies.

Bringing Political, Budgetary, and Technology Assets "to the Table"

In order to have the required "clout" among a set of federal, state and local institutions in which it will not be the dominant player, the new Department of Homeland Security must be in a position to "bring something to the table." Among the things it could bring are:

- A high-level, White House or Congressional mandate to perform assessments, to modify and augment existing public health communication and coordination channels, to set standards and establish new organizational linkages, and the like;
- Funding (i.e., grant-making and contracting capability) for new drugs and vaccines, communications capabilities, detection and screening technologies, training, and exercises - perhaps especially directed at the state and local levels;
- Capabilities, technology, and techniques for alerting and response that would otherwise not be available to the public health infrastructure.

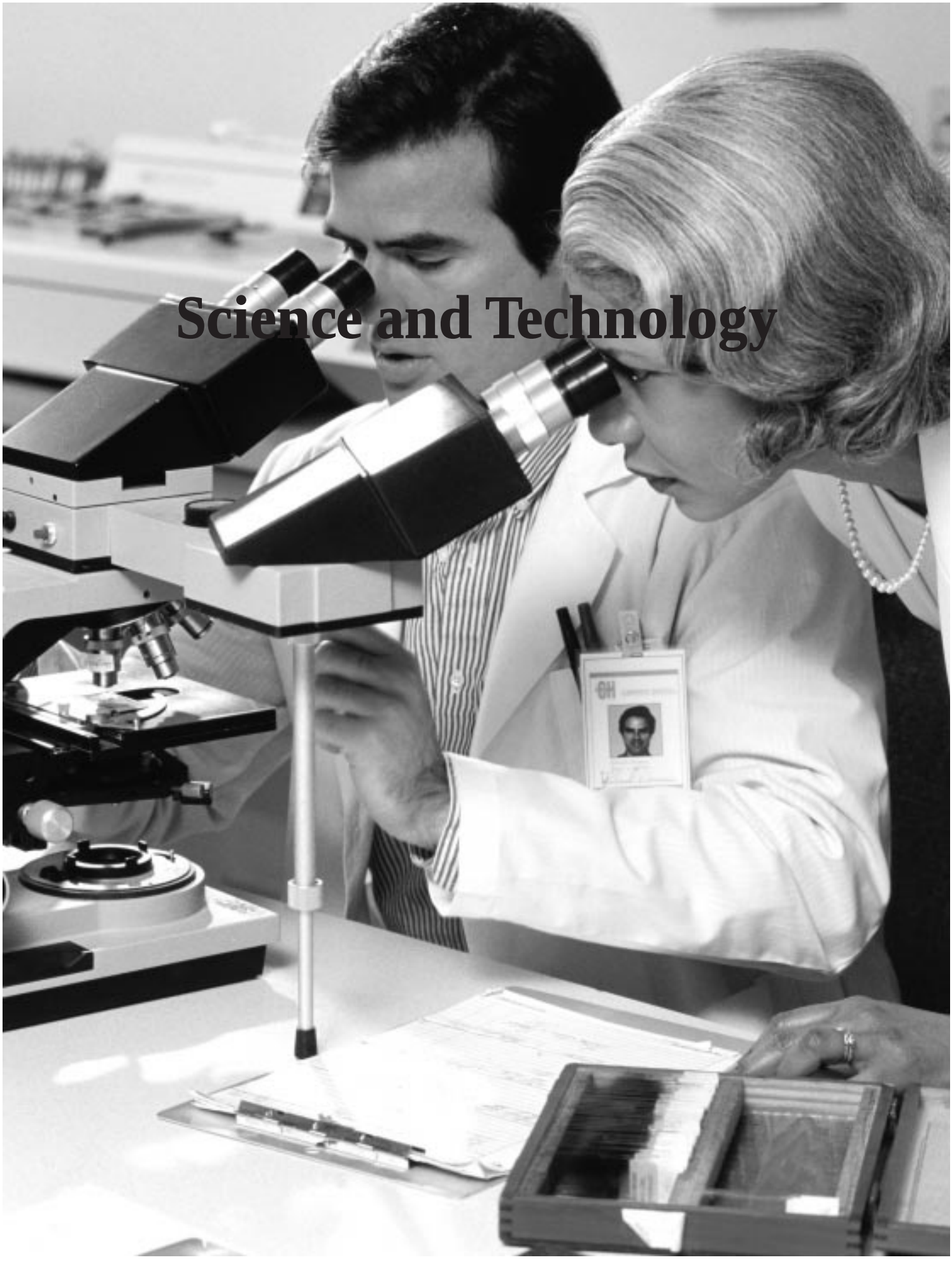
Recommendations for the First 100 Days

To carve out its role and responsibilities in the public health arena, this task force recommends the following actions for the new Department of Homeland Security in its first 100 days of operations.

- Establish a cooperative, collaborative relationship with the Department of Health and Human Services (with particular attention to OPHP, CDC, NIH, HRSA, and FDA), and with the Department of Agriculture's and EPA's relevant components, predicated on supporting and supplementing, not usurping, those agencies' primary responsibilities in this field.
- Determine how the new Department will organize its internal efforts on public health-related issues and whom within its structure will be in overall charge of these functions.
- Develop standards, particularly targeted at state and local levels, to correct deficiencies. The Department should employ systems engineering solutions to adapt existing, standard practices for homeland security ends and finding better ways to "mine" and rapidly share available data on emerging public health threats.
- Augment existing public health communications capabilities, particularly in a few key areas. This needs to occur regionally, between hospital emergency rooms and between individual physicians' offices and state health authorities, and between the DHS and its correspondents in OPHP, CDC, NIH, HRSA, and FDA, as well as between the CDC and the military's medical establishment.
- Work with HHS to "speed up its clock" - since the urgency of response increases dramatically when terrorists are trying to create maximum fatalities through infection or contamination. Working with HHS, the Department should ensure that epidemic symptoms reports are as fast and responsive as current MedWatch reports on drug reaction alerts.

In the longer run, of course, the Department of Homeland Security can expect to play a role, again in collaboration with HHS, in fostering new technology to shorten the diagnosis and response time and assess the degree of infection and contamination quickly - such as the development of instantaneous blood-based tests. In this respect, research in the biomedical field could yield benefits for other components of the homeland security challenge. Among other possible applications, for example, INS could effectively employ such technology during port of entry screenings.

Science and Technology



CHAPTER 5
SCIENCE & TECHNOLOGY

Scope of the Challenge

The President's National Strategy for Homeland Security correctly identifies science and technology as a critical advantage for the United States and its allies in the war against terrorism. It is a foundation of efforts to protect American citizens. No other country in the world is as well equipped to pursue new research questions in technology that can heighten American security in many ways. Such research is not new. It is a well established activity inside and outside of government: the Department of Defense, the National Institutes for Health, the Centers for Disease Control and Prevention, and our national laboratories are just some of the places where the federal government already has a deep commitment to science and technology research that has direct relevance to national security and the protection of public health. There is also an equally vibrant research activity in American industry and in our universities and research centers. As Rep. Doug Ose (R-CA) has put it, "Our nation's preeminence in science and technology will be critical in the coming years as we introduce new systems and solutions to thwart future terrorist attacks. We must combine the strengths of our scientists, cutting-edge technology, and private sector innovation."

The Department of Homeland Security must embrace this large swath of activity, coordinate the federal components, reach out to relevant research projects in the private sector, and identify the highest priorities for science and technology. The sheer scope of research in science in technology can be seen in the fact that the President's National Strategy identifies 11 major science and technology initiatives ranging from biological warfare countermeasures to applying biometrics technology to identification devices.

Because the range of activities in this area is so large, the most pressing task of the Department of Homeland Security during its first 100 days is to assess which among the vast array of research activities is most relevant to securing America's homeland and then how such activities can be coordinated and accelerated. In the process, the new Department has the opportunity to set the priorities of its science and technology initiatives to overcome the bureaucratic "stovepiping" noted previously in many areas related to homeland security.

Specifically, the science and technology agenda should be pursued in five key ways:

- *Establish an organizational structure* for science and technology research within the Department of Homeland Security that is capable of interacting with all departments that now conduct security-related research and with industry.
- *Assess current research* activities both inside and outside of the federal government to help identify duplication and significant research gaps.
- *Establish a coordination plan* for homeland security research projects of various departments and agencies aimed at minimizing duplication and capitalizing on synergies among these efforts.
- *Organize outreach activities* with private sector research companies whose work can be quickly assessed.

- *Commence a process to identify long-term projects* that might have the greatest payoff for homeland security

Organizational Structure

The Under Secretary of Science and Technology must coordinate the research and development (or science and technology) activities of all the component agencies of the Department of Homeland Security. However, the Office of the Under Secretary must also be equipped to identify the immediate research needs of the homeland security community, as well as work with science and technology experts to identify long term projects not yet in the research pipeline. To help achieve these goals, the Department should establish the Office of the Chief Scientist, who can assess the specific projects underway in each research area.

It is also critical that the Under Secretary for Science and Technology coordinate activities relating to the budget process for all relevant research that takes place within the Department of Homeland Security and its component agencies.

The Department should also immediately undertake a review to determine how to most effectively coordinate its research and development efforts with those in other relevant departments and agencies - notably the Departments of Defense, Justice, Energy, Transportation, and the intelligence community. It should consider, in particular, how to maximize synergy with current technology development efforts at the Defense Advanced Research Projects Agency. If its charter legislation does not provide for the creation of a DARPA-equivalent organization within the Department of Homeland Security, the Department's leadership should determine whether this model could be usefully adapted to the homeland security mission and needs.

Assess Current Research

It should be an immediate task of the Department to assess, describe, and rank the major federal research projects now underway that are relevant to homeland security. Part of this assessment must be geared toward identifying duplicative efforts within the federal government and opportunities for joint or cooperative research. This will prove especially important in areas related to border security, identification, and detection, threat assessment, and countermeasures for chemical, biological, radiological and nuclear incidents - areas where research is now conducted in several locations. One of the other key tasks of this assessment must be to identify what areas require new or additional research. Once that assessment is in hand, the Department will be able to identify the most pressing new research projects and recommend funding for specific new projects.

As part of the assessment process, the Under Secretary for Science and Technology should establish a Scientific Advisory Board, including state and local government representatives. This board would serve to identify promising technologies applicable to homeland security challenges, overcome parochial bureaucratic resistance to promising technologies, and provide an independent outside assessment of technology development projects. Among its early tasks could be the above-mentioned assessment and ranking of current Federal homeland security-related research projects according to their perceived effectiveness and utility.

Establish a Coordination Plan

While integration of federal activities (and cooperation with private efforts) is clearly one of the overall goals of the Department, science and technology research needs to be closely monitored and coordinated so that its benefits can be directly

applied to security issues. The Department should set a timetable for reporting to Congress on how it has integrated existing federal research efforts relevant to homeland security. The Department must also establish a process in which research conducted for the Department of Defense is assessed for its homeland security benefits and integrated with other ongoing research.

Organize Outreach Activities

The Under Secretary for Science and Technology needs to establish a process to identify and assess relevant research activities underway in the private sector, academia and other research institutes. Rep. Deborah Pryce (R-OH) noted, "The Department will need to reach out to all sectors of our nation, from Federal, state and local governments to universities, to businesses, even to individual citizens. Working together, we can help the Department of Homeland Security achieve our common goal of a safer America." A channel must then be set up to encourage private enterprise to interact easily with federal officials. The goal should be to allow ongoing innovations in the security and public health fields to be promptly presented for review and assessment by federal officials.

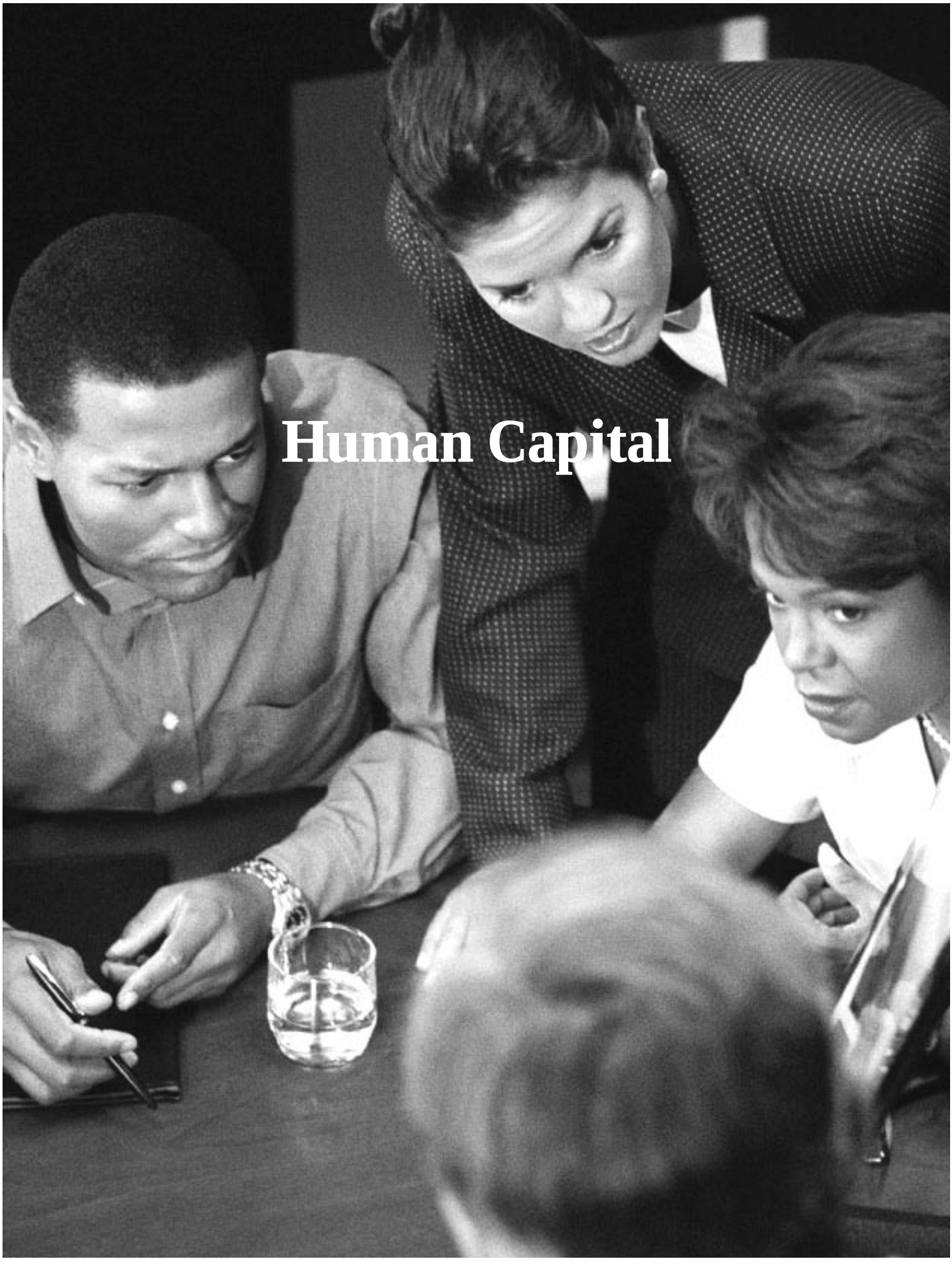
High Return Research Projects

In addition to the eleven priorities outlined in the National Strategy, the Under Secretary for Science and Technology must establish a process for considering longer-term research projects that, if successful, would provide a high return on the research investment. These might include research on vaccines, assessment of unfamiliar threats, biometrics, and tools for first responders.

Recommendations for the First 100 Days

- Grant the Under Secretary of Science and Technology centralized budget authority over all Department of Homeland Security research and development activities.
- Establish a rolling, multi-year budgeting process for the Department's technology development efforts, predicated on an explicit threat assessment and geared to the achievement of specific capabilities against projected threats by specific timeframes.
- Establish a technology road map that identifies long-term development objectives based on an assessment of available technology.
- Appoint a Chief Scientist and a scientific advisory board (including representatives of state and local governments and the private sector). The mandate of the Chief Scientist and the advisory board would be to advise the Under Secretary and Secretary on the most promising research projects and technology approaches, to provide independent assessments of vendor proposals, and to overcome parochial resistance to new concepts.
- Establish a clearinghouse within the Department of Homeland Security to evaluate private sector technologies and solutions for near-term implementation.

In the longer run - beyond the first one hundred days - the Department of Homeland Security will face a number of additional organizational challenges and opportunities in the science and technology field. It will need to prioritize funding for specific projects in each of the 11 science and technology areas identified by the President's National Homeland Security Strategy. It will require processes and mechanisms for identifying and pursuing longer-range research projects focused on core homeland security tasks: data sharing, border security, threat detection and response, and public health. It will also require mechanisms for evaluating the Federal government's analytical capacity to process future flows of threat information. Among the choices the Department will consider will be whether a new national laboratory focused on homeland security technology is needed to supplement our current national laboratories or whether to adapt the organizational model of DARPA to the new Department's technology incubation efforts.



Human Capital

CHAPTER 6
A NOTE ON HUMAN CAPITAL - A CRITICAL REQUIREMENT

Scope of the Challenge

In the quest for Homeland Security, technology can never obscure the critical need for human capital - particularly personnel with the skill-sets needed to integrate disparate information, intelligence and experience into a single, "systems-view" of the security challenge.

While the President's National Strategy for Homeland Security does not specifically address the "human capital" challenges of ensuring homeland security, these are obviously fundamental. Homeland Security functions will be no more effective than the people responsible for them. As different portions of the President's Homeland Security Strategy point out, the "human capital" problem has many layers.

On the federal level, human capital considerations will greatly influence:

- Intelligence
- Investigative efforts and law enforcement;
- Border security, port security, and immigration;
- Rail, road, and air transportation safety;
- Critical infrastructure protection and continuity of operations;
- Public health, disease control, and immunological functions;
- Food and water safety functions;
- Nuclear safety and security

On the state and local levels, where the largest number of responsible officials and personnel are to be found, human capital will prove a critical factor in the effectiveness of:

- Police and other public security personnel;
- Firefighters, rescue squads, and other first-responder units;
- Civil defense and other disaster response efforts;
- Hospital and clinic staffs, EMS squads, and public health officials;
- Records and licensing bureau personnel.

Beyond the governmental dimensions of the human capital issues, it is important to recognize the contribution of private sector personnel to the homeland security challenge; more than 1 million people are employed in private security currently and millions more are involved in safety and security related functions ranging from data systems protection to building engineering. The Department of Homeland Security can promote the further professionalism and proficiency of these services by conditioning its state and local grant-making to the State adoption of professional training and certification standards for private security functions.

In approaching the human capital dimension of the homeland security problem, we suggest that the Department of Homeland Security be guided by these themes:

- Organizational development programs that identify, for example, all the personnel responsible for different facets of the border security problem, regardless of the agency or organization to which they belong, and then integrating their culture so as to instill a sense of shared mission and goals;
- Professional development programs that identify skill gaps and help to upgrade the skills of the existing workforce to meet new and emerging threats;
- Training and simulation programs that enable personnel to better anticipate potential problems and function more effectively in high-stress, extraordinary, and/or unfamiliar situations;
- Identification and establishment of organizational structures and personnel practices that will best promote innovation and creative solutions to existing problems;
- Fostering respect for homeland security providers and their missions - an indispensable prerequisite for the public patience, understanding and cooperation necessary to thwart future attacks and capture would-be terrorists.

AFTERWORD

As we write these words in the weeks following the anniversary of September 11, the memories of that horrible morning sharpen the sense of responsibility we feel, as Members of Congress, to strengthen this Nation's capacity for homeland defense.

We fully support President Bush's plan to create a single, central agency entrusted with homeland security, with the authority and assets adequate to perform that task. Yet, while the passage of the bill creating the new department marks a major milestone in our efforts, it also signals the start of a new and critical phase: the challenge of shaping the mission and the mandate of this new agency in ways that best serve the security of the American people.

By identifying select elements in the homeland security challenge - from border security and public health, to issues of interoperability, identification and authentication and science and technology as well as the critical constant of human capital - the Republican Main Street Partnership offers this report not as the final word on the evolution of the new department. Rather, it is our contribution to the ongoing debate that will shape our homeland security efforts, particularly in the new department's all-critical first 100 days. Positioned as we are, not only at the center of the political debate but at the center of the political spectrum, we also offer the reflections and recommendations contained in these pages as a bridge between a Congress and an Administration that may differ on details, but agree entirely on the need to provide for homeland defense.

September 11, 2001 underlined for every American the dangers we face from the enemies of freedom. The days since then underline the need for this Nation to do all it can to detect, deter and defeat our enemies, and preserve the American ideals we hold dear. With that objective as our aim, we offer this report to be "read into the record" of the critical considerations to come.

Representative Christopher Shays

Representative Rob Simmons

Representative Doug Ose

Representative Deborah Pryce

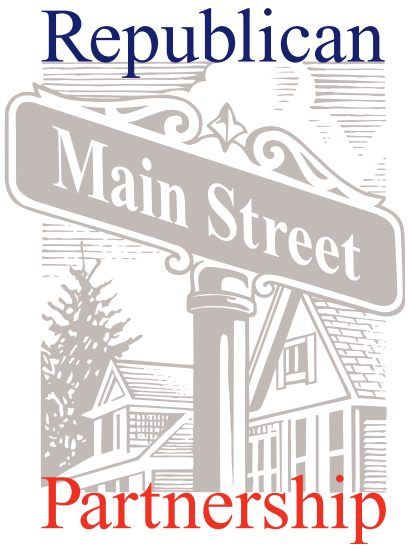
David Zolet
TRW Inc.

Republican Main Street Partnership Congressional Members

Sen. Lincoln Chafee, Rhode Island
Sen. Susan Collins, Maine
Sen. John McCain, Arizona
Sen. Pat Roberts, Kansas
Sen. Gordon Smith, Oregon
Sen. Olympia Snowe, Maine
Sen. Arlen Specter, Pennsylvania
Sen. Ted Stevens, Alaska

Rep. Charles Bass, New Hampshire
Rep. Doug Bereuter, Nebraska
Rep. Judy Biggert, Illinois
Rep. Sherwood Boehlert, New York
Rep. Ken Calvert, California
Rep. Dave Camp, Michigan
Rep. Shelley Moore Capito, West Virginia
Rep. Michael Castle, Delaware
Rep. Thomas Davis, III, Virginia
Rep. David Dreier, California
Rep. Vernon Ehlers, Michigan
Rep. Philip English, Pennsylvania
Rep. Michael Ferguson, New Jersey
Rep. Mark Foley, Florida
Rep. Rodney Frelinghuysen, New Jersey
Rep. Greg Ganske, Iowa
Rep. Paul Gillmor, Ohio
Rep. Wayne Gilchrest, Maryland
Rep. Benjamin Gilman, New York
Rep. Porter Goss, Florida
Rep. Kay Granger, Texas
Rep. Jim Greenwood, Pennsylvania
Rep. David Hobson, Ohio
Rep. Steve Horn, California
Rep. Amory Houghton, New York
Rep. Johnny Isakson, Georgia
Rep. Nancy Johnson, Connecticut
Rep. Timothy Johnson, Illinois
Rep. Sue Kelly, New York
Rep. Mark Kirk, Illinois
Rep. Jim Kolbe, Arizona
Rep. Ray LaHood, Illinois
Rep. Steven LaTourette, Ohio
Rep. Jim Leach, Iowa
Rep. Jerry Lewis, California
Rep. Frank LoBiondo, New Jersey
Rep. Jim McCrery, Louisiana
Rep. Connie Morella, Maryland
Rep. George Nethercutt, Washington
Rep. Tom Osborne, Nebraska
Rep. Doug Ose, California
Rep. Thomas Petri, Wisconsin
Rep. Deborah Pryce, Ohio
Rep. Jack Quinn, New York
Rep. Jim Ramstad, Minnesota
Rep. Ralph Regula, Ohio
Rep. Michael Rogers, Michigan
Rep. Marge Roukema, New Jersey
Rep. E. Clay Shaw, Jr., Florida
Rep. Christopher Shays, Connecticut
Rep. Robert Simmons, Connecticut
Rep. Fred Upton, Michigan
Rep. Greg Walden, Oregon
Rep. James Walsh, New York
Rep. Curt Weldon, Pennsylvania
Rep. Jerry Weller, Illinois

Gov. Jim Geringer, Wyoming
Gov. Bill Graves, Kansas
Gov. George Pataki, New York
Gov. John Rowland, Connecticut



Republican Main Street Partnership

The Republican Main Street Partnership is a gathering of leaders from government, business and education who share a commitment to conservative, pragmatic approaches to business in a global context, to compassion in our communities and character in our national leaders.

Unlike other organizations, we are focused on governing and on providing research, issue discussion and policy development from the Republican center to promote wise and thoughtful governance.

Our agenda is far-reaching - we're addressing the environment, education and urban policy to name a few. And our doors are open to people of differing views, backgrounds, and approaches.

We are the Republican Main Street Partnership. And we invite you to join us for the future of the party - and of the Nation.

Republican Main Street Partnership
1350 I Street NW, Suite 560, Washington, D.C. 20005
P: 202.682.3143 F: 202.682.3943