

# Creating a Trusted Information Network for Homeland Security

SECOND REPORT OF THE MARKLE FOUNDATION TASK FORCE

December 2003

*A Project of*

The Markle Foundation  
New York City

*In Alliance with*

The Brookings Institution  
Washington, DC

Center for Strategic and International Studies  
Washington, DC

# MARKLE FOUNDATION

## TASK FORCE ON NATIONAL SECURITY IN THE INFORMATION AGE

### *Chairmen*

**Zoë Baird**  
Markle Foundation

**James L. Barksdale**  
The Barksdale Group

### *Executive Director*

**Michael A. Vatis**  
Markle Foundation

### *Members*

**T. Alexander Aleinikoff**  
Georgetown University Law Center

**Robert D. Atkinson**  
Progressive Policy Institute

**Stewart Baker**  
Steptoe & Johnson

**Eric Benhamou**  
3Com Corporation

**Jerry Berman**  
Center for Democracy and Technology

**Robert M. Bryant**  
National Insurance Crime Bureau

**Ashton B. Carter**  
Harvard University

**Wesley K. Clark**  
Wesley K. Clark & Associates

**G. Wayne Clough**  
Georgia Institute of Technology

**William P. Crowell**  
Security and Intelligence Systems

**Sidney D. Drell**  
Stanford University

**Esther Dyson**  
EDventure Holdings

**Amitai Etzioni**  
The George Washington University

**David J. Farber**  
Carnegie Mellon University

**John Gage**  
Sun Microsystems, Inc.

**Slade Gorton**  
Preston, Gates & Ellis

**Morton H. Halperin**  
Open Society Institute

**Margaret A. Hamburg**  
Nuclear Threat Initiative

**John J. Hamre**  
Center for Strategic and International  
Studies

**Eric H. Holder, Jr.**  
Covington & Burling

**Arnold Kanter**  
The Scowcroft Group

**Michael O. Leavitt**  
Governor of Utah

**Tara Lemmey**  
Project LENS

**Gilman Louie**  
In-Q-Tel

**Judith A. Miller**  
Williams & Connolly

**James H. Morris**  
Carnegie Mellon University

**Craig Mundie**  
Microsoft

**Jeffrey H. Smith**  
Arnold & Porter

**Abraham D. Sofaer**  
Stanford University

**James B. Steinberg**  
The Brookings Institution

**Paul Schott Stevens**  
Dechert LLP

**Rick White**  
TechNet

**Philip Zelikow**  
Miller Center of Public Affairs  
University of Virginia

*Participating Experts  
(non-government)*

**Bruce Berkowitz**  
RAND

**Robert Clerman**  
Mitretek Systems

**James Dempsey**  
Center for Democracy and Technology

**Mary DeRosa**  
Center for Strategic and International  
Studies

**Lara Flint**  
Center for Democracy and Technology

**Lauren Hall**  
Microsoft

**Jeff Jonas**  
Systems Research & Development

**James Lewis**  
Center for Strategic and International  
Studies

**Terrill D. Maynard**  
Consultant

**Mary McCarthy**  
Center for Strategic and International  
Studies

**Patrick J. Sullivan, Jr.**  
Cherry Creek Schools

**Winston Wiley**  
Booz Allen Hamilton

### *Associate Director*

**Mary McKinley**  
Markle Foundation

### *Task Force Staff*

**Nancy Boursiquot**  
Administrative Assistant

**Todd Glass**  
Director, Public Affairs

**Caroline McCarus**  
Assistant to the President

**Jennifer Obriski**  
Administrative Assistant

**Stefaan Verhulst**  
Chief of Research

# Table of Contents

## Acknowledgements

## Overview

## Part One: The Task Force Report

<b>Achieving a networked community for homeland security</b> .....	1
<b>Assessment of government progress toward a trusted, decentralized network</b> .....	2
Information sharing and analysis .....	2
Utilizing privately held data.....	5
<b>Building a networked community for homeland security</b> .....	8
Vision and objectives .....	8
<i>Exhibit A: Action plan for federal government development of the SHARE network</i> .....	9
Closing the gaps between agencies .....	11
Scenario-based concept of operations.....	13
Designing a robust architecture for the future .....	13
<i>Exhibit B: Weaknesses in the current information-sharing system</i> .....	14
<i>Exhibit C: Authentication technology</i> .....	15
<i>Exhibit D: Attributes of the SHARE network</i> .....	17
Participants in the network: organizational structure .....	18
The federal participants .....	18
<i>Exhibit E: Joint Terrorism Task Forces (JTTFs)</i> .....	20
Decentralized analytic nodes .....	21
The road to a culture of distribution .....	22
Measuring performance .....	24
<i>Exhibit F: Evaluating improvements in information sharing and analysis</i> .....	25
<b>Accessing private sector data</b> .....	30
Information available in the private sector .....	30
Identifying the private sector information the government needs .....	31
Guidelines for government use of private sector information.....	32
Acquisition and use of private sector data.....	33
Government retention of private sector data.....	34
Sharing private sector data with agencies not involved in counterterrorism .....	35
Accountability and oversight .....	35
<i>Exhibit G: Evaluating improvements in the government's use of private sector data while protecting civil liberties</i> .....	37
<b>Future work of the Task Force</b> .....	39
<b>Conclusion</b> .....	39
<b>Additional Papers</b> .....	40

## Acknowledgments

The Task Force issued its first report in October 2002. This initial report was seen as a useful contribution by a broad cross section of those concerned with the new environment for America's homeland security. We decided to continue our work and developed an agenda for further action. The Task Force began its second year in March 2003. Renewing its commitment to providing the government with practical recommendations informed by diverse perspectives, the Task Force organized several areas of work, leading up to a summer plenary meeting. At that meeting, Task Force members agreed that we should issue a second report by the end of this year, given the urgent need for our government to improve its ability to use information to protect our nation.

We organized two Working Groups. Working Group I, ably led by Tara Lemmey and Bill Crowell, focused on how to construct a network for sharing and analyzing information among governmental entities at all levels and relevant private sector organizations. This Working Group's paper is included in Part Two of our report. Working Group II, equally ably led by Gilman Louie and Jim Steinberg, addressed the issue of how our government can more effectively utilize privately held data while protecting privacy and other civil liberties. This Working Group's paper, too, is in Part Two. We also convened a smaller subgroup, thoughtfully led by Amitai Etzioni, to consider the crosscutting issue of how to make forms of identification more reliable while protecting civil liberties. This paper is in Part Three.

The papers developed by the Working Groups and the subgroup, along with many other papers, including the selection of appendices found in Part Three, informed the Task Force's discussions, which took place in two plenary sessions, numerous meetings, and email and telephone exchanges. These discussions led to the Report of the Task Force as a whole, found in Part One.

We thank the leaders of the Working Groups and the subgroup for their devotion to our work and their high standards regarding what we together could achieve. On technology issues, Tara Lemmey, Gilman Louie, and Task Force associate Jeff Jonas made our work a central part of their daily lives, tirelessly researching and vetting papers,

drafting sections of our report, and informing our efforts with their knowledge and creativity. On policy and governmental issues, Jim Steinberg, Amitai Etzioni, Stewart Baker, and Task Force associates Mary DeRosa, Mary McCarthy, Winston Wiley, Terry Maynard, and Jim Dempsey developed innovative approaches, careful research, compelling ideas, and drafts of sections of the report. These people and the many other members and associates of the Task Force put in dozens of hours melding their expertise into a common understanding of the interplay between technology and policy. They attended meetings, reviewed documents, consulted one another via email or telephone, and sought advice and information from other professionals. We cannot adequately thank them here for their wisdom and dedication.

Eric Benhamou, among his other contributions, helped us chair our principal plenary meeting. Lauren Hall and a team at Microsoft—drawn together by Task Force member Craig Mundie—assisted Tara Lemmey in helping us think through how to create visual representations of our recommendations.

Stefaan Verhulst, Lara Flint, and Tanvi Madan provided valuable research assistance. Todd Glass handled our public education and outreach, and Karen Thomas provided an excellent platform on the Internet for the Task Force's work. Sharon Lucius and Caroline McCarus were important members of the team, as were Paulette Layton, Nancy Boursiquot, Jennifer Obriski, Brendan Lavy, and Linda Hutchins, who worked day to day to support the Task Force members and staff. Karen Byers provided sound financial management. Mila Drumke tirelessly edited our final product.

Finally, none of this would have been possible without the dedication and hard work of our Executive Director, Michael Vatis, and Associate Director, Mary McKinley. Michael thoughtfully managed the many different areas of activity that constituted this project and ultimately brought them together to form a valuable whole in this report. Mary again operated the daily activities, keeping them on course with professionalism and experience.

Zoë Baird

James Barksdale

## Overview

This is the second report of an extraordinary task force we have been privileged to co-chair. This remarkable and diverse group has come together to serve our nation by doing the hard work of considering how we can create an information network that prevents terrorism and protects the security of our homeland, while preserving the civil liberties that are a fundamental part of our national values.

In the Task Force's first report, we stressed the importance of creating a decentralized network of information-sharing and analysis to address the challenge of homeland security. We emphasized the need to form that network around presidential guidelines shaped by public debate on how to both achieve security and maintain liberty. We also set forth principles for capitalizing on our society's strengths in information technology. In this second report, we reaffirm those principles and provide greater detail on how to implement our approach.

The network we envision would be created with the following key elements, which reflect the character of the distributed, asymmetric threat we confront:

1. The handling of information should be decentralized, and should take place directly among users, according to a network model rather than a mainframe or hub-and-spoke model.
2. The network should be guided by policy principles that simultaneously empower and constrain government officials by making it clear what is permissible and what is prohibited.
3. Our government's strategy should focus on prevention.
4. The distinguishing line between domestic and foreign threats is increasingly difficult to sustain. Thus, in its approach, our government should avoid creating blind spots, or gaps between agencies, that arise from this distinction. At the same time, though, our government needs urgently to define new rules—rules to replace the old “line at the border” between domestic and foreign authorities for information-collection and use—to

ensure that agencies do not infringe on our traditional civil liberties.

5. The network should reflect the fact that many key participants are not in the federal government, but rather in state or local government and the private sector.
6. The network should make it possible for the government to effectively utilize not only information gathered through clandestine intelligence activities and law enforcement investigations, but also appropriate information held by private companies. This should happen only after clear articulation by the government of the need for this information and the issuance of guidelines for its collection and use.
7. Combating terrorism is a long-term effort that is designed to protect our way of life and our values along with our security. Therefore, the policies and actions undertaken need to have the support—and trust—of the American people. Privacy and other civil liberties must be protected.

What do these principles mean in practice?

First, our government should give greater priority to sharing and analyzing information. In the Cold War intelligence architecture, the government placed a premium on the security of information. It developed a system that tightly controlled access to information by requiring that every individual have a demonstrable “need to know” certain information before he could see it and by allowing the agency that initially acquired the intelligence to restrict further dissemination of that intelligence. This system assumed that it was possible to determine *a priori* who needed to know particular information. And it reflected the judgment that the risk of inadvertent or malicious disclosure was greater than the benefit of wider information-sharing.

This architecture and the underlying assumptions are ill suited to today's challenges. The events of September 11, 2001, have starkly demonstrated the dangers associated

with the failure to share information, not only within the federal government, but also between the federal government, on the one hand, and state and local governments and the private sector on the other. Therefore, the government should open up the system to state and local agencies and officials and, in some circumstances, to private sector actors, providing access not just to information but to technology and money as well. Our government should reengineer operational processes where needed and build the technology architecture and tools that will facilitate two-way sharing and interoperability. Our government should also take into account the needs of the users, as well as the agency that originally developed the information, in deciding whether or how to control where the information goes. This should take place in an environment in which the need to protect both the security of sensitive information and individual civil liberties is consistently addressed.

Furthermore, our government should effectively utilize the valuable information that is held in private hands, but only within a system of rules and guidelines designed to protect civil liberties. Our nation can never hope to harden all potential targets against terrorist attack. Therefore, we must rely on information to try to detect, prevent, and respond to attacks. The travel, hotel, financial, immigration, health, or educational records of a person suspected by our government of planning terrorism may hold information that is vital to unveiling both his activities and the identities and activities of other terrorists.

But until the government devises consistent guidelines for controlling when and how such information is accessed and used—and until those guidelines are publicly debated—the public’s concerns over potential privacy infringements will continue to hamper the necessary development of new technologies and new operational programs to use that information.

The need to create the network we envision is more urgent than ever. Terrorism remains a continuing threat around the world. And the potential for terrorists to use weapons of mass destruction raises the stakes considerably. Building the technical architecture, changing agency cultures, establishing new rules and procedures, and securing the necessary funding all take time. It is therefore imperative that the steps we recommend receive immediate attention. We urge the Executive Branch and Congress to implement the measures necessary to create the proposed Systemwide Homeland Analysis and Response Exchange (SHARE) Network—which would empower all participants to be full and active partners in protecting our security, and which would be governed by guidelines designed to protect our liberties.

Zoë Baird

James Barksdale

PART ONE

# The Task Force Report

## Achieving a networked community for homeland security

---

In October 2002, the Markle Foundation Task Force issued its first report, *Protecting America's Freedom in the Information Age*. In that report, we expressed our belief that the threats to America at home from terrorism and weapons of mass destruction could be met only if we developed first-rate information collection, analysis, communications, and sharing. The nation could never sufficiently harden all potential targets against attack, so the government should instead develop the means to obtain advance warning of terrorist intentions through better intelligence, and use that intelligence to interdict terrorist plans and focus our protection resources on the most likely terrorist targets. It should also use information to enhance our response capabilities. We proposed a national strategy for using information and information technology in a robust decentralized network and for strengthening the processes for collecting data and turning it into actionable information. These new capabilities, we stated, could be achieved in a manner that protects our rights to privacy and other traditional civil liberties. In fact, any government undertaking to build such an information network would not be sustainable if the government did not build public trust by embedding protection of well-established civil liberties throughout that system.

We expressed our belief that our nation must capitalize on its leadership in information technology and on our citizenry's commitment to have both security and civil liberties. Thus, the recommendations in our first report provided a roadmap for the development of new networks and relationships among government agencies and officials at all levels. We also provided a framework for considering how the government might make most effective use of data residing in the private sector, while preserving liberties and avoiding the imposition of undue costs on businesses.

In our first report, we emphasized the need for a next-generation homeland security information network that would empower local participants to contribute, access, use, and analyze data, while also allowing them to identify, access, communicate with, and assemble other participants in both the public and private sectors. We argued against a

centralized mainframe system in Washington, DC, and stated that “most of the real frontlines of homeland security are outside of Washington, DC,” and that “likely terrorists are often encountered, and the targets they might attack are protected, by local officials” (page 10). In addition, we said that “the government will need access to public and private sector data for national security” and called for the Department of Homeland Security (DHS) to “develop innovative service-delivery models for using information held within and outside government” (page 37).

In this report, we reaffirm the principles of our first report and offer greater detail on how we believe the government should create networks for information collection, sharing, analysis, and use across federal, state, and local agencies and the private sector, while preserving—and even enhancing—privacy and other civil liberties. The network we envision consists not just of the technological architecture, but also of the people, processes, and information that must go hand-in-hand with the technology, and the rules that should govern how all of these elements interact. We repeat our call for the President to issue guidelines for government collection and use of information. As we said in our first report, “Only the President can establish and be accountable for the proper balance between development of domestic intelligence and preservation of liberty” (page 2). And only with such guidelines and attendant public discussion can the government hope to engender and maintain the trust of the people in its efforts, which is vital to implementing the network we envision.

## Assessment of government progress toward a trusted, decentralized network

---

Since we issued our first report, the federal government has made some progress in fostering the development of the network we envisioned. Both the Executive Branch and Congress appear to have a greater understanding now of the need for more information sharing and for networks that break down agency “stovepipes.”<sup>1</sup>

But our nation’s efforts continue to suffer from the absence of the national vision and public discussion called for in our first report. Progress thus has been ad hoc and sporadic at best. The government also has not yet developed guidelines to govern the collection, use, and retention of information in conducting the war on terrorism and issued them as a presidential directive. As a result, each agency is making its own decisions, and this is undermining public confidence—which in the long run limits the prospects for successful implementation of the necessary information-gathering and analysis efforts. It is critically important that guidelines be established before another major terrorist incident occurs. If public debate were to take place in the shadow of another major national tragedy, it could lead to rushed and poorly conceived initiatives that not only fail to solve the underlying problems, but also have a detrimental impact on civil liberties.

---

<sup>1</sup> The new *Attorney General’s Guidelines for FBI National Security Investigations and Foreign Intelligence Collection* (effective 31 Oct. 2003), for instance, stress that “information should be shared as consistently and fully as possible among agencies with relevant responsibilities to protect the United States and its people from terrorism and other threats to the national security, except as limited by specific constraints on such sharing” (page 24). Available at [http://www.cdt.org/security/usapatriot/031031nsiguide\\_lines.pdf](http://www.cdt.org/security/usapatriot/031031nsiguide_lines.pdf) (last visited 11 Nov. 2003). These guidelines move the government forward on considering how it will share information, and we intend to look more closely at this issue. However, the guidelines do not appear to reflect the comprehensive effort that we encourage to openly develop policy principles and tools that can help implement guidelines for use when both privacy and security interests are implicated by the collection of information domestically.

## Information sharing and analysis

Steps have been taken at the federal, state, and local levels to broaden the sharing of terrorist-threat data among government agencies at all levels and to improve analysis of terrorism-related information.<sup>2</sup> To date, however, the government is still a long way from the creation of the dynamic, distributed network for sharing and analysis that we envision. The sharing of terrorist-related information between relevant agencies at different levels of government has been only marginally improved in the last year, and remains haphazard and still overly dependent on the ad hoc “sneaker net” of personal relations among known colleagues. It is not the result of a carefully considered network architecture that optimizes the abilities of all of the players.

At the federal level, the President announced, in January 2003, the creation of the Terrorist Threat Integration Center (TTIC), an interagency center created by the CIA and the FBI, with participation of the DHS, the Department of State, the Department of Defense (DoD), and the intelligence community. The TTIC reports to the Director of Central Intelligence. The Executive Branch established the TTIC to perform many of the analytical functions that Congress had assigned to (and that our initial report recommended be performed by) the DHS and its Intelligence Analysis and Infrastructure Protection Directorate. Thus, the White House announced that the TTIC would close the gap between analysis of foreign and domestic intelligence on terrorism. According to the White House, the center will do the following:

- *Optimize use of terrorist threat-related information, expertise, and capabilities to conduct threat analysis and inform collection strategies,*

---

<sup>2</sup> One example is the Antiterrorism Information Exchange (ATIX), a network being developed by the Justice Department and the FBI to provide law enforcement agencies and public safety, infrastructure, and homeland security groups access to “Sensitive But Unclassified” homeland security information. ATIX is also intended to serve as a means to deliver security alerts to public officials and private sector groups and to allow users to create collaborative bulletin boards where they can exchange information. See Wilson P. Dizard III, “First Responders Get Homeland Security Network,” *22 Government Computer News* 9 (28 Apr. 2003), at [http://www.gcn.com/22\\_9/news/21878-1.html](http://www.gcn.com/22_9/news/21878-1.html) (last visited 11 Nov. 2003).

- Create a structure that ensures information sharing across agency lines,
- Integrate terrorist-related information collected domestically and abroad in order to form the most comprehensive possible threat picture,
- Be responsible and accountable for providing terrorist threat assessments for our national leadership.<sup>3</sup>

While the TTIC's personnel are working hard to build an integrated analytical capability and are apparently considering innovative ways to analyze and disseminate information,<sup>4</sup> the very fact of the TTIC's creation has caused confusion within the federal government and among state and local governments about the respective roles of the TTIC and the DHS.

Moreover, we understand that the TTIC is presently focused mainly on only one part of its assigned mission—"providing terrorist threat assessments [such as the President's Terrorism Threat Report (PTTR)] for our national leadership," including the President, the National Security Council, and other senior officials in Washington, DC. While this is obviously an

<sup>3</sup> White House Fact Sheet: *Strengthening Intelligence to Protect America* (Jan. 2003), available at <http://www.whitehouse.gov/news/releases/2003/01/20030128-12.html>. For more information on how the TTIC was formed and is intended to operate, see testimony by Winston P. Wiley, Chair, Senior Steering Group, Terrorist Threat Integration Center, and Associate Director of Central Intelligence for Homeland Security, before the Senate Governmental Affairs Committee (as prepared for delivery) 26 February 2003, available at [http://www.cia.gov/cia/public\\_affairs/speeches/2003/wiley\\_speech\\_02262003.html](http://www.cia.gov/cia/public_affairs/speeches/2003/wiley_speech_02262003.html) (last visited 8 Nov. 2003).

<sup>4</sup>For instance, over 2,000 government users have access to "a TTIC-sponsored classified website providing terrorism-related information. This website... is currently being updated to include expanded need-to-know access with rich content available at varying classification levels, from "Top Secret" to "Sensitive-But-Unclassified"...[and to] enable users to search across disparate data sets in many different ways. The website will increasingly include products tailored for the needs of state and local officials, as well as private industry" for dissemination by the DHS and the FBI. Statement for the Record of John O. Brennan, Director, TTIC, on "The Terrorist Threat Integration Center and its Relationship with the Departments of Justice and Homeland Security," before the House Judiciary Comm. and the House Select Comm. on Homeland Security (22 July 2003), available at <http://hsc.house.gov/files/Testimony%20Brennan.doc> (last visited 12 Nov. 2003).

important function, the TTIC's almost single-minded focus on this one aspect of its mission has prevented it from addressing the urgent intelligence needs of operational entities throughout the government and serving as a key locus for intelligence fusion and sharing. As an intelligence community official told one Task Force member, "As good as the PTTR is, it won't save anyone's life."

Meanwhile, the DHS also does not appear to have taken the necessary steps to build the communications and sharing network required to deal with the threat, or to begin producing regular, actionable intelligence products for other agencies. Indeed, the DHS has yet to articulate a vision of how it will link federal, state, and local agencies in a communications and sharing network, or what its role will be with respect to the TTIC and other federal agencies. The Department instead seems to be focused on building a new information-technology infrastructure to support and unify its 22 components.<sup>5</sup> This is an important step, but one that should be grounded in a plan for the whole system.

Moreover, neither the TTIC nor the DHS has gotten very far in putting in place the necessary staff or framework for analyzing information and sharing it broadly among the relevant federal, state, and local agencies. Government at the federal level thus remains very much in need of an overarching decentralized framework for building an information sharing and analysis network.

Many state and local governments have grown increasingly frustrated at the perceived lack of progress at the federal level in sharing information, at the dearth of actionable intelligence coming from federal sources, and at the lack of transparency and feedback regarding how the information they provide is being utilized. Some have responded by developing their own ideas for information sharing and analysis networks.<sup>6</sup>

<sup>5</sup> See, for example, Dibya Sarkar, "DHS Still Working on Info-Sharing Plans," FCW.com (7 Nov. 2003), available at <http://www.fcw.com/geb/articles/2003/1103/web-dhs-11-07-03.asp> (last visited 11 Nov. 2003).

<sup>6</sup> For example, the 10 northeastern states, from Delaware to Maine, have formed a consortium to combine their homeland security efforts and develop information sharing strategies. See Testimony of James Kallstrom, senior advisor to New York Governor George Pataki for Counter Terrorism, before the House Select Comm. on Homeland Security, Subcomm. on Intelligence and

However, without an overall framework that links regional or local networks with one another and with federal entities, the full potential of state and local governments will never be realized. Moreover, without broad national agreement on how state and local government programs should function, and when and how they should access and use private sector data, they run the risk of being shut down in the same way federal programs that would have used private sector data have been.<sup>7</sup>

In August 2003, the General Accounting Office (GAO) issued a study that found that the poor coordination of information sharing efforts might cause critical clues of impending terrorist attacks to go unnoticed.<sup>8</sup> Although the Homeland Security

---

Counterterrorism (24 July 2003) at pages 4-5, available at <http://hsc.house.gov/files/Testimony%20Kallstrom.doc> (last visited 11 Nov. 2003). In addition, Pennsylvania, New York City, and Washington, DC, have formed a model project—primarily with local funding—that would link existing law enforcement, public safety and justice systems across jurisdictions to provide real-time data sharing over the Internet. See “The Shield Pilot,” available at <http://www.search.org/integration/pdf/ShieldPilot.pdf> (last visited 11 Nov. 2003).

<sup>7</sup> For example, several states now participate in the Multistate Anti-Terrorism Information Exchange (MATRIX) project, a data mining effort run by a private company for the participating states and aided by the federal government. MATRIX, started by police in Florida, combines law enforcement and court records with commercially available information about individuals, and purportedly allows officials to look for patterns and linkages among people. See Robert O’Harrow, Jr., “U.S. Backs Florida’s New Counterterrorism Database,” *Washington Post*, page A1 (6 Aug. 2003), available at <http://www.washingtonpost.com/ac2/wp-dyn/A21872-2003Aug5?language=printer> (last visited 4 Nov. 2003). Privacy concerns have reportedly caused several states to reconsider their initial decision to participate and have prompted criticism and questions from civil-liberties groups. See, for example, Kristen Wyatt, “Georgia Decides Against Crime Database,” Associated Press (21 Oct. 2003) available at <http://www.bayarea.com/mld/mercurynews/business/7068004.htm> (last visited 8 Nov. 2003); American Civil Liberties Union, “What is the Matrix? ACLU Seeks Answers on New State-Run Surveillance Program,” (30 Oct. 2003), available at <http://www.aclu.org/Privacy/Privacy.cfm?ID=14257&c=130> (last visited 4 Nov. 2003).

<sup>8</sup> See GAO, Homeland Security Highlights, “Efforts to Improve Information sharing Need to Be Strengthened” (Aug. 2003), available at

Act of 2002 requires the DHS to share information with state and local authorities, representatives from states and cities told the GAO that the current system is close to failing. One of the major obstacles cited in the GAO report is the federal government’s belief that the fight against terrorism remains its responsibility alone. In addition, GAO investigators said many federal officials expressed concern about sharing national-level intelligence information with state and local agencies.

Furthermore, since many states and localities are presently enduring serious financial difficulties, most of these efforts are in need of federal funding to make any significant advances. A 50-state study released by the U.S. Conference of Mayors in September concluded, for instance, that 90 percent of cities have not received funds from the country’s largest federal homeland security program, designed to assist local officials, police, fire chiefs and other first responders to prepare for terrorist attacks.<sup>9</sup> Though we do not believe that all cities need significant federal funding—because all are not equally likely to be terrorist targets—this is nevertheless a telling statistic. We must ensure that local officials are neither overwhelmed by, nor without adequate resources to deal with, what is expected of them, because they are important players in the overall system. Moreover, their participation is important for creating deep and lasting public trust.

Another recommendation of our first report was that the government create virtual consolidated watch lists to allow agencies to check individual names against the many different lists maintained by various parts of the federal government. We also called for guidelines and procedures that would determine how individuals get put on a list, and how they can be removed from it. Some progress is apparently being made here. In particular, the government is creating the Terrorist Screening Center (due to become operational on December 1, 2003), which is supposed to

---

<http://www.gao.gov/highlights/d03760high.pdf> (last visited 21 Nov. 2003).

<sup>9</sup> See “The United States Conference of Mayors, U.S. Conference of Mayors Announces: 90 Percent of Cities Left Empty-Handed Without Funds from Largest Federal Homeland Security Program” (17 Sept. 2003), available at [http://www.usmayors.org/uscm/news/press\\_releases/documents/homelandfunding\\_091703.pdf](http://www.usmayors.org/uscm/news/press_releases/documents/homelandfunding_091703.pdf) (last visited 21 Nov. 2003).

consolidate the many existing watch lists.<sup>10</sup> But it remains to be seen how successful this center will be in practice. Also, to date, no government-wide guidelines have been issued concerning how individuals get placed on—and removed from—a watch list; how accuracy is maintained and errors are corrected across lists; or on how information on the lists is shared among agencies and with private companies.<sup>11</sup>

## Utilizing privately held data

Government access to, and use of, privately held data remains a vexing problem. On the one hand, as we pointed out in our first report, there is a great deal of readily available private sector data that can expose patterns, identify terrorists, and save lives. In our initial report, for example, we showed how the September 11 terrorists could have been identified from airline reservation systems and searches of public-record data starting with the information that two individuals on terrorist watch lists had bought airline tickets using their real names (page 28). These individuals were linked by common past addresses, common phone numbers, and frequent-flyer numbers. On the other hand, government efforts to collect information on Americans without a demonstrated, compelling government need have been met with outcries of invasion of privacy and repeatedly have been shut down.<sup>12</sup>

---

<sup>10</sup> See Homeland Security Presidential Directive/Hspd 6 (16 Sept. 2003), available at <http://www.whitehouse.gov/news/releases/2003/09/20030916-5.html> (last visited 7 Nov. 2003).

<sup>11</sup> In April 2003, the GAO issued a report on federal watch lists, finding that 9 agencies maintain 12 different watch lists, that the lists contain overlapping but different information, and that the agencies had different policies governing when and how information on the lists is shared with others. It also found that sharing is constrained by the watch lists' differing technological architectures. GAO, "Information Technology: Terrorist Watch Lists Should Be Consolidated To Promote Better Integration and Sharing" (Apr. 2003), available at <http://www.gao.gov/new.items/d03322.pdf> (last visited 9 Nov. 2003).

<sup>12</sup> In 2002, for example, Congress prohibited implementation of the Justice Department's "Operation TIPS" (Terrorism Information and Prevention System) after the media, public, and members of Congress expressed concern about infringements of privacy. Homeland Security Act of 2002, 6 USC 142, § 880. TIPS would have given workers in the transportation, trucking,

One major development since our first report has been the controversy over the Defense Department's Terrorist Information Awareness (formerly known as Total Information Awareness) program (TIA). The aim of this initiative, created by the Defense Advanced Research Projects Agency (DARPA), was to develop information-analysis and collaboration tools to enhance the government's ability to detect terrorist activity. Another aim was to develop software that would allow government officials to search for patterns across databases of transactional records (medical, financial, educational, travel, immigration, and communications, etc.) in order to detect potential terrorist activity. The TIA faced vocal opposition from the public and Congress, in part because of shifting explanations of how the TIA's proposed technology (described as, among other things, "data-mining" or "knowledge discovery" tools) would operate. For instance, the TIA left ambiguous whether its technology would be used to search transactional data only for information about specific subjects of terrorism investigations or to find suspicious patterns that matched analysts' hypotheses of how potential terrorists might launch an attack, and thereby identify individuals requiring further scrutiny. Similarly, it was never clear whether the TIA envisioned technology that would allow the government to

---

shipping, maritime, and mass-transit industries (and, originally, mail carriers and utility workers as well) a formal mechanism for reporting and sharing information about suspicious, publicly observable activity possibly related to terrorism.

In 1999, the Federal Deposit Insurance Corporation withdrew a proposed "Know Your Customer" regulation that would have required certain state banks to develop programs to determine the identity of their customers, the customers' sources of funds, and their "normal and expected transactions"; monitor their account activity to identify transactions inconsistent with those normal and expected transactions; and report any suspicious activities to the government. The regulation, which was intended to "protect the integrity and reputation of the financial services industry" and assist in combating money-laundering and other illegal activities, was withdrawn in the face of widespread opposition from industry and the public. "The overwhelming majority of commenters were individual, private citizens who voiced very strong opposition to the proposal as an invasion of personal privacy." FDIC, "Minimum Security Devices and Procedures and Bank Secrecy Act Compliance," 12 C.F.R. Part 326, Fed. Reg. vol. 64 no. 59, p. 14845 (29 Mar. 1999), available at <http://www.fdic.gov/news/news/financial/1999/FIL9934b.pdf> (last visited 11 Nov. 2003).

aggregate private sector data into one centralized government database, or technology that would allow the government to search across private sector databases while leaving the data in private hands.<sup>13</sup> Moreover, the TIA's defenders never adequately explained the extent to which transactional data of U.S. citizens would be searched using the agency's technology. In January 2003, Congress barred funding for domestic deployment of the TIA but allowed research to go forward.<sup>14</sup> Ultimately, in September 2003, Congress eliminated all funding for the TIA program and "any successor program."<sup>15</sup>

We are disappointed that Congress found it necessary to ban research and development of technologies that would make use of privately held data. Innovation in technology is an important part of our nation's competitive edge against terrorist organizations and the states that back them. Had the government, in developing the TIA, formulated policy principles and guidelines on the research and use of such technologies to access privately held data—and engaged in a public discussion of those policies—it would not have become so mired in the controversy that resulted in the banning of research by Congress. Policy guidelines like these are meant to empower government officials as well

---

<sup>13</sup> Compare, for instance, "Overview of the Information Awareness Office," remarks as prepared for delivery by Dr. John Poindexter, Director, DARPA Information Awareness Office, at DARPA Tech 2002 Conference, Anaheim, Calif. (2 Aug. 2002) ("One of the significant new data sources that needs to be mined to discover and track terrorists is the transaction space. If terrorist organizations are going to plan and execute attacks against the United States, their people must engage in transactions and they will leave signatures in this information space... *The relevant information extracted from this data must be made available in large-scale repositories with enhanced semantic content for easy analysis to accomplish this task.*" [emphasis added]) with Terrorist Information Awareness Program, *Guide to the Report to Congress* (20 May 2003) ("the TIA Program is not attempting to create or access a centralized database that will store information gathered from public or privately held databases" [emphasis added]).

<sup>14</sup> Omnibus Appropriations Act for Fiscal Year 2003, H.R.J. Res. 2, Amend. 59, 108th Cong. (2003).

<sup>15</sup> H.R. Conf. Rep. No. 108-283 (2003) (Conference report on H.R. 2658, Department of Defense Appropriations Act, 2004), (24 Sept. 2003), available at <http://thomas.loc.gov/cgi-bin/query/R?r108:FLD001:H08501> (last visited 21 Nov. 2003).

as limit them, and Congress and the Executive Branch should share a common commitment to both objectives.

Yet, even though the TIA has been shut down, other still-extant governmental efforts—both research and operational activities—raise many of the same issues. For instance, the National Security Agency's (NSA) Advanced Research and Development Activity (ARDA) is pursuing research programs in "Novel Intelligence from Massive Data" (aimed at "focusing analytic attention on the most critical information found within massive data—information that indicates the potential for strategic surprise"<sup>16</sup>) and "Information Exploitation" ("the process of extracting, synthesizing, and/or presenting relevant information from vast repositories of raw and structured data"<sup>17</sup>). Meanwhile, the CIA reportedly is implementing a data-mining program called Quantum Leap that "enables an analyst to get quick access to all the information available—classified and unclassified—about virtually anyone."<sup>18</sup>

Similarly, if implemented, the Transportation Security Administration's (TSA) Computer Assisted Passenger Prescreening System (CAPPS II) would check passenger-provided data against commercial databases, government databases, and a watch list of suspected terrorists and people wanted for violent crimes to determine if specific passengers should receive further checkpoint scrutiny or be barred from boarding planes altogether.<sup>19</sup> However, following the revelation that

---

<sup>16</sup> "Advanced Research and Development Activity, Novel Intelligence from Massive Data," at [http://www.ic-arda.org/Novel\\_Intelligence/](http://www.ic-arda.org/Novel_Intelligence/) (last visited 31 Oct. 2003).

<sup>17</sup> "Advanced Research and Development Activity, Information Exploitation Thrust," at <http://www.ic-arda.org/InfoExploit/index.html> (last visited Oct. 31, 2003).

<sup>18</sup> See Bill Powell, "Inside the CIA," *Fortune* (29 Sept., 2003), available at <http://www.fortune.com/fortune/articles/0,15114,490641,00.html> (last visited 7 Nov. 2003). The CIA's deputy chief information officer reportedly stated that the program's technology is "so powerful it's scary," and that in the wrong hands, it "could be Big Brother." The MATRIX program, discussed above at note 7, is another example of an ongoing data-mining effort.

<sup>19</sup> According to testimony from DHS officials: "CAPPS II is intended to identify terrorists and other high-risk

JetBlue Airways turned over to a DoD contractor the names and addresses of 5 million passengers, which were then used for a data-mining study on airline-passenger risk assessment, Congress has stalled the implementation of CAPPs II pending a GAO review of the program's effectiveness and potential effects on privacy.<sup>20</sup>

Thus, while various government agencies pursue efforts to utilize privately held data, those efforts continue to provoke controversy because of the lack of a systematic effort to consider the privacy implications of the proposed programs or to develop an overall policy framework that would govern the deployment of new technologies. Here, too, then, the principle of establishing clear policies and guidelines for the acquisition, use, and retention of private data laid out in our first report has not been adequately implemented.

---

individuals before they board commercial airplanes. CAPPs II will conduct a risk assessment of each passenger using national security information and information provided by passengers during the reservation process—including name, date of birth, home address, and home phone number, and provide a risk score to the TSA. The risk score includes an authentication score provided by running passenger name record (PNR) data against commercial databases to indicate a confidence level in each passenger's identity. CAPPs II will be a threat-based system under the direct control of the federal government and will represent a major improvement over the decentralized, airline-controlled system currently in place." Testimony of Stephen J. McHale, Deputy Administrator of the TSA, et al., before the Senate Comm. on Commerce, Science, and Transportation (5 Nov. 2003), available at [http://www.senate.gov/~commerce/hearings/testimony.cfm?id=985&wit\\_id=2785](http://www.senate.gov/~commerce/hearings/testimony.cfm?id=985&wit_id=2785) (last visited 8 Nov. 2003).

<sup>20</sup> See Department of Homeland Security Appropriations Act, 2004, 108 Pub. 90 (1 Oct. 2003), Title VI, § 519; Judi Hasson, "Congress Demands Study of CAPPs II," *Federal Computer Week* (26 Sept. 2003), available at <http://www.fcw.com/fcw/articles/2003/0922/web-capps-09-26-03.asp> (last visited 21 Nov. 2003).

## Building a networked community for homeland security

---

We developed this second report through a rich, multilayered process that involved a diverse group of Task Force members with vast experience in federal, state, and local government; intelligence; law enforcement; defense; the technology industry; computer science; sociology; law; medicine; and privacy protection. We consulted with government officials in Washington, DC, and across the country so that we could better understand the current state of governmental activity—the successes achieved and barriers encountered to date. We also consulted broadly with technology experts and businesses to learn the state of technology development.

We approached our task by considering concrete situations in which the government would need to obtain, analyze, share, and act on certain information in order to learn about and prevent terrorist activity. This process of scenario-based envisioning allowed us to evaluate the following: (1.) how such information would be analyzed and shared today; (2.) where current roadblocks exist that prevent or impede necessary information sharing; (3.) what additional players should be getting the information in order to activate all the sensors in the system and increase the intake of relevant information; (4.) what procedures should be developed so that sensitive information (such as intelligence sources and methods) can be protected from unauthorized disclosure but actionable information can be routinely and quickly disseminated throughout the network; (5.) what process changes and new technologies can enhance analysis and information sharing; and (6.) how the government can avoid flooding the system with noise while ensuring that potential signals of terrorist activity are distinguished from the noise and shared widely.

To this end, we developed a set of information vignettes (see Appendix D) that served to inform the Task Force's discussions and our ultimate recommendations. Our goal was to discover where the present homeland security initiatives are optimized to achieve the dynamic and decentralized network required to take on the challenge of distributed and complex threats, and where more work is needed. We looked at whether existing networks were created to maximize the

potential contribution of all of the participants, including those at the state and local levels. And we sought to identify how the government could utilize the enormous volumes of potentially significant data in private hands while protecting precious liberty interests. This process has grounded our recommendations in reality, thus allowing us to see more clearly the very real impediments to change and to make recommendations that can help the government work through those obstacles more effectively.

### Vision and objectives

The networked community that we envision would protect national security by drawing on the best talent and technology available and by fostering a robust sharing of information and ideas. Collectively, this community could provide the public with confidence that the government was doing everything reasonably possible to prevent and respond to terrorist attacks on the homeland. The network we recommend would be guided by a practical set of policy guidelines that would simultaneously empower and constrain government officials by making clear what collection, analysis, sharing, and uses of information were permissible and what were not. And it would focus on eliminating the gaps between government agencies. All players in this network—including those at the edges—would be able to create and share actionable and relevant information. The focus of the network itself would be to get information into the hands of people who could analyze and act on it, and to leverage information from private data holders within a system of rules and guidelines. The objective of this network would be to enhance the government's "sensemaking" ability—that is, its ability to discern indicators of terrorist activity amid overwhelming amounts of information, and to create more time for all of the actors to make decisions and to prevent or respond to terrorist acts more effectively.

This is government acting in new ways, to face new threats. And while such change is necessary, it must be accomplished while engendering the people's trust that privacy and other civil liberties are being protected, that businesses are not being unduly burdened with requests for extraneous or useless information, that taxpayer money is being well spent, and that, ultimately, the network will be effective in protecting our security.

Building the networked community presents enormous challenges. It requires changes in

policies, processes, and the use of technology. And it requires fundamental changes in the harder intangibles of cultures and attitudes, which have impeded the creation of the sort of network we envision. Leadership is emerging from all levels of government and from many places in the private sector. What is needed now is a plan to accelerate these efforts, and public debate and consensus on the goals. This report attempts to contribute to paving that path.

Using the principles outlined in this and our previous report, and building on the information sharing initiatives around the country, the federal government should create an interagency, public-private group, led by the DHS and comprising representatives of all the relevant network players, to develop a national strategy and architecture for the homeland security network. Because of the

daunting political, organizational, and technical challenges, it is impossible to conceive of designing and building this network all at once. It will be necessary to grow capabilities in pieces, building on existing systems and incorporating new systems and technologies over time. To do so will require an architecture that is flexible and adaptable. Such an effort could render a working plan within a year, one that could guide investment and network development for both the short and long term.

Throughout this report, we recommend actions the government should take to begin creating the Systemwide Homeland Analysis and Resource Exchange (SHARE) Network we envision. In Exhibit A, we summarize the principal steps that should be taken by the federal government in the near term to begin this urgent undertaking.

#### **Exhibit A Action plan for federal government development of the SHARE network**

##### **The President should issue an Executive Order that does the following:**

1. Sets the goal of creating a decentralized network along the lines set out in this report
2. Sets forth specific and clear objectives for improved analysis and information sharing, which each federal agency should be required to meet by December 31, 2004
3. Establishes guidelines for agencies' collection, use, and dissemination of information, including private sector information
4. Establishes a process for Executive Branch review of agencies' performance in improving analysis, information sharing, and utilization of private sector information, to take place after December 31, 2004
5. Designates the DHS as the lead agency of an interagency, public-private process to establish the concept of operations for the network, directs other agencies to offer their full assistance and cooperation, and establishes a timeframe for implementation
6. Clarifies the respective roles of the DHS, the TTIC, and other federal agencies in information sharing and analysis.

##### **The President should also issue a second Executive Order or other directive that does the following:**

1. Establishes guidelines governing the authority of the TTIC and other intelligence, defense, and security agencies to receive, retain, and disseminate information gathered in the U.S. about U.S. persons
2. Establishes guidelines governing intelligence agencies' ability to set requirements for (or "task") domestic collection of information
3. Creates within the TTIC appropriate institutional mechanisms to safeguard privacy and other civil liberties.

The contents of the Executive Order should be unclassified to the maximum extent possible and put out for notice and comment. In addition, the President should consider introducing legislation to codify the appropriate scope of the TTIC's use and dissemination of information about U.S. persons.

**Exhibit A (Continued)**

**Action plan for federal government development of the SHARE network**

**The DHS should do the following:**

1. Convene an interagency, public-private group to design a strategy and concept of operations for the decentralized network we describe, which should render a working plan within a year
2. Work with state, local, and private sector entities to create decentralized analytical centers, foster their ability to communicate with other players in the network, and establish standards for digitization, retention, and communication of information
3. Establish clear mechanisms for responding to requests for threat and vulnerability information from local officials
4. Establish a process for ensuring that as much information as possible is being shared among network entities, including a dispute resolution mechanism to resolve disagreements among agencies about how much information can be shared
5. Establish a process for overseeing federal agency development and implementation of guidelines governing the acquisition, use, retention, and dissemination of private sector information and the creation of methods for ensuring oversight and accountability
6. Work with state, local, and private sector entities to institute information-sharing and analysis objectives for these entities, and establish a process with them for jointly evaluating their performance after December 31, 2004, and thereafter on an ongoing basis

**The FBI should do the following:**

1. Establish mechanisms for sharing information with state and local law enforcement agencies, and for encouraging those agencies to share directly with other players in the network
2. Establish clear mechanisms for responding to requests for threat and vulnerability information from local officials

**All government agencies with homeland security intelligence responsibilities should do the following:**

1. Set up mechanisms to produce more information that can be readily disseminated to other players in the network, including unclassified information
2. Identify specific categories of private sector information they need, using a scenario-driven process that considers the types of situations they might confront in investigating or seeking to uncover terrorist activity
3. Institute guidelines governing the acquisition, use, retention, and dissemination of private sector information, and establish methods to ensure oversight and accountability

**Congress should do the following:**

Undertake to review the performance of federal agencies in improving analysis and information sharing along the lines set out in this report, and in utilizing private sector information while protecting civil liberties. This review should take place after December 31, 2004.

## Closing the gaps between agencies

One of the biggest challenges we face is the reduction of information gaps that exist between our various federal and state agencies, between intelligence and law enforcement, and between government in general and the private sector. In 1947, President Truman created the Central Intelligence Agency (CIA) to help eliminate the intelligence gaps that existed between government agencies before World War II. The National Security Act of 1947 charged the CIA with coordinating our nation's intelligence activities and correlating, evaluating, and disseminating intelligence.<sup>21</sup>

**One of the biggest challenges we face is the reduction of information gaps that exist between our various federal and state agencies, between intelligence and law enforcement, and between government in general and the private sector.**

Today, if anything, the gaps between different agencies are even broader and more numerous than in the Cold War years. This is particularly true in the context of counterterrorism, where important information or analytical ability resides not just in the 14 intelligence components of the federal government and federal law enforcement and security agencies, but also with the 17,784 state and local law enforcement agencies,<sup>22</sup> 30,020 fire departments,<sup>23</sup> 5,801 hospitals<sup>24</sup> and the millions of

<sup>21</sup> See *Central Intelligence Agency Factbook on Intelligence 2002*, "The Genesis of the CIA," at <http://www.cia.gov/cia/publications/facttell/genesis.html> (last visited 31 Oct. 2003).

<sup>22</sup> See DOJ—Office of Justice Programs, Bureau of Justice Statistics, *Law Enforcement Statistics Summary Findings (2000)*, available at <http://www.ojp.usdoj.gov/bjs/lawenf.htm> (last visited 12 Nov. 2003). There are approximately 800,000 full-time sworn law enforcement officers in the United States, including federal, state, and local agencies.

<sup>23</sup> See DHS, FEMA, U.S. Fire Administration, *Fire Data (2001)*, at <http://www.usfa.fema.gov/inside-usfa/nfdc/nfdc-data9.shtm> (last visited 12 Nov. 2003). There are 1,078,300 firefighters in the U.S.

first responders who are on the frontlines of the homeland security effort. Add to this the thousands of private owners and operators of critical infrastructures, who are responsible for protecting potential targets of terrorist attacks, and the many more private companies that may have information in their databases that could lead to the prevention of terrorist activity. Communication, collaboration, and sharing across the gaps between and among these actors are critical to countering terrorism because we cannot predict where the first sign of a potential terrorist threat will come from—a communications intercept from the National Security Agency (NSA), a human source of the CIA or the FBI, an investigation by a local police department, or an observation by an alert private security guard or emergency room nurse.

The decentralized nature of the terrorist threat thus leads to exponentially more—and widely scattered—information to process and share. The reality is that every hour of every day, our intelligence and law enforcement agencies, health care providers, private companies, and numerous other players receive information that might be relevant to uncovering a terrorist plot and preventing an attack.

Attempting to centralize this information is not the answer because it does not link the information to the dispersed analytical capabilities of the network. Centralization could also lead to information becoming obsolete, since a centralized analytical entity would not have the ability to keep up-to-date much of the information collected from dispersed

**Every day our intelligence and law enforcement agencies, health care providers, private companies, and numerous other players receive information that might be relevant to uncovering a terrorist plot and preventing an attack.**

<sup>24</sup> See Hospitalconnect.com, Advancing Health in America Resource Center, "Fast Facts on U.S. Hospitals from 'Hospital Statistics'" (10 Dec. 2002), available at [http://www.hospitalconnect.com/aha/resource\\_center/fastfacts/fast\\_facts\\_US\\_hospitals.html](http://www.hospitalconnect.com/aha/resource_center/fastfacts/fast_facts_US_hospitals.html) (last visited 12 Nov. 2003).

sources. But making all the information available to everyone in the network is not the answer either, because this could increase the threat to civil liberties, heighten the risk of a leak of sensitive information, cause uncoordinated action by different agencies, and simply overwhelm the recipients. Indeed, the sheer volume of data would create such a high degree of noise that it would be extremely difficult for analysts to make useful correlations or for local agencies to take meaningful protective action.

The network we envision therefore would enable participants to distinguish useful signals of potential terrorist activity from useless noise.<sup>25</sup> It would utilize the expertise of all the participants in the network, and address their need to collect, update, and understand the information that is important to their primary functions, without flooding them with extraneous information they cannot use.

**The network we envision would enable participants to distinguish useful signals of potential terrorist activity from useless noise.**

Moreover, the threat today requires unprecedented speed in the way we collect, share, and act on information. Unlike in the Cold War, we are not trying to discern the size or movements of distant armies or the goings-on within a foreign government. Rather, we are trying to detect and thwart potentially imminent attacks that could take place at any time against what are often soft, civilian targets. What's more, the potential modes of attack—sniper attacks, suicide bombers, truck and car bombs, airline hijackings, weapons of mass destruction (chemical, biological, nuclear, and radiological) as well as mass disruption (cyber attacks)—are as varied as the imaginations of those who wish to do us harm. To detect, thwart, and respond to these types of threats, time is of the essence. And information needs to be tailored to facilitate decision-making and action at all levels—not only by the President, but also by police officers on the street.

<sup>25</sup> One potential model for thinking about this problem stems from an analogy to the functioning of our bodies' immune systems. See Appendix C.

Our Task Force's fundamental objective, then, is to identify the technological tools and infrastructure, the policies, and the processes necessary to link these different communities, so that important information can be shared among the people who need it, and as rapidly as possible. Information sharing itself is not the goal; rather, it is the means by which we can maximize our ability to make sense of the information available. And it is also the means by which we can give all participants more time to make the right decisions and take more effective actions to prevent terrorist attacks.

**Information sharing itself is not the goal; rather, it is the means by which we can maximize our ability to make sense of the information available.**

For our envisioned network to work, rules are needed to define the following: (1.) how decisions are made about what information might be useful; (2.) who has what responsibilities for creating potentially useful information for the system; and (3.) who is authorized to have access to information and what uses of the information are permissible. There must also be rules to ensure oversight and public accountability.

Finally, guidelines covering how information is collected, used, and shared among the relevant actors are critical for several different but complementary reasons. First, they are vital to preventing the misuse of information that is gathered and shared in the network. A robust sharing of information must only be pursued consistent with civil liberties interests. Second, they are needed to empower government officials who, not knowing what the rules are, or fearful of public criticism, may refrain from taking legal and necessary action that might uncover a terrorist plot or thwart an attack. Third, guidelines are needed to ensure coordination by the participants in the network; if participants feel that they do not know what will happen with information they share with others, they will simply refrain from sharing regardless of how many directives are issued to mandate it. Finally, guidelines are needed to engender the public's trust in what the government is doing when it acts across the specifically defined boundaries of agencies in the network. That is, the public must understand, to the fullest extent possible, why the government needs information and what the government will do with it. The

public must also have confidence that the information—and individuals' rights—will not be abused. It is not enough to write the code that operates the network; we must also write the code that governs the network.<sup>26</sup>

## Scenario-based concept of operations

To build the network, we must start with a concept of operations that is based on a realistic understanding of the ways in which information comes into the system and the means employed for turning it into useful knowledge. The concept of operations must be scenario-based, and derived from the needs of the users across the network rather than from central authorities in Washington, DC. Thus, the government should generate realistic terrorist-threat scenarios that agencies might confront and then conduct exercises against them in order to understand the required information and communication flow, collection requirements, data sources, analytical requirements, decision processes, responder needs, and response timetables. The concept of operations that the government derives from these scenarios should be a living framework that is regularly updated based on new threat assessments and evolving user needs.

The creation of a concept of operations would provide a better understanding of the gaps, single-point dependencies, and bottlenecks in the network architecture that exists today, and of what we need to do to move toward the network we envision. The concept of operations should define the most efficient and effective information workflow as well as the minimum acceptable bandwidth, connectivity, storage, and sharing requirements for every required connection path on the network. It should also allow individual agencies to better plan their internal information-technology acquisition plans and workflow-improvement programs. And it should help to establish benchmarks for response time, data-sharing requirements, information-quality standards, responsibility, and authority for each node on the network. The information vignettes that our Task Force has developed (see Appendix D) are helpful for understanding how information flows today, and how it needs to flow

---

<sup>26</sup> See Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books, 1999), for a discussion of how code embedded in software and hardware and code found in laws and regulations enacted by the government both serve to regulate behavior on the Internet.

to optimize the capabilities of the players at the edges of the network.

The network should be decentralized, of course, but someone needs to be responsible for designing, building, and maintaining it. Consistent with the recommendations in our first report, we believe the DHS should take the lead by convening the relevant players, collaboratively designing the network, and securing the funding necessary to build it. We firmly believe that an agency with domestic jurisdiction, rather than a foreign intelligence agency, would be the most trusted federal entity to lead the creation of a network that is sustainable when privacy concerns are raised. Furthermore, Congress has established internal oversight mechanisms within the DHS, including a privacy officer and a civil rights and civil liberties officer, which would help give the DHS credibility.<sup>27</sup>

## Designing a robust architecture for the future

Many agencies are enhancing their internal information and communications infrastructures in an effort to improve their ability to perform analytical tasks and respond to customers. Various agencies are adopting data and communication standards for sharing information. We see this as a positive first step, but more work needs to be done.

Agencies' current information-sharing efforts tend to focus on sharing data laterally and narrowly—federal agency to federal agency, law enforcement to law enforcement, and state government to state government. Work needs to be done to enable a network in which data moves across all the gaps, and analysis occurs at multiple nodes rather than only in a few centralized locations. This section outlines some of the technical design elements of such a network, which we call the Systemwide Homeland Analysis and Resource Exchange (SHARE) Network.

---

<sup>27</sup> See Homeland Security Act of 2002, 6 USC 142, §§ 221, 705 (2002).

**Exhibit B**  
**Weaknesses in the current information-sharing system**

**There are multiple weaknesses in the current system that need to be fixed:**

1. The system is susceptible to single points of failure for both analysis and communication of information.
2. The system is designed mainly to flow information up, to senior officials, and not down, to operational entities, and out, to the edges of the network.
3. The system does not adequately support real-time operations.
4. Many critical information repositories are not compatible with the analytic tools, and many still are air-gapped and not accessible online to analysts.
5. There is a lack of trust between federal, state, and local agencies.
6. It is difficult to sort the important signals of potential terrorist activity from the noise. Analytic tools are outdated and incapable of dealing with the current volume of data.
7. State, local, and commercial information is not well leveraged.
8. Many people are concerned about potential misuses of private information.
9. Information that is disseminated to first responders typically is not actionable. That is, relevant information does not enter into the everyday workflow of first responders.
10. Clear lines of authority and responsibilities for information sharing and analysis have not been established.
11. The system has not been well tested to see how it meets potential terrorist threats.

Essential to an effective network that links disparate players is a set of directory services that help each actor to find what he or she is looking for. We need directory services for information about locations (such as critical infrastructure assets, landmarks, and geographical references), people, organizations, terrorist methods, and other

topics; and pointers to experts on various subjects. Directories would also help people find others working on similar problems. Fortunately, this is one of the areas in which existing technology can make a significant contribution. Automated directories with appropriate security and access controls can be deployed to solve these problems. These directories can be structured to give originators of information control over what can be shared, and where it can be routed. Directories also can be updated automatically through real-time monitoring, synchronization, and profiling of the skills and interests of the network users.

Another important element of the network is the separation of data from data applications in order to foster interoperability. Data sets are often not directly interoperable because they are constructed for different purposes, use different standards, contain different terminology, and were not intended for integration with other data sets. But through the combination of data directories, metadata standards,<sup>28</sup> and commercially available exchange standards such as Extensible Markup Language (XML), a user can identify what data exists in other agencies and then contact those agencies to obtain the underlying data (assuming the user has the requisite authority). XML organizes information by allowing categories of data to be tagged with agreed upon names for each field, and thus can enable different organizations to share information more efficiently. To an extent, this process can also be automated: software tools (“agent technologies”<sup>29</sup>) can be used to search for and identify data at the edges of the network, collecting only directory-level information without actually moving and consolidating the underlying data into a centralized database. Directories can also enable ad hoc collaboration and sharing, so that groups of players across levels of government can come together on matters of mutual interest and, by doing so, not only inform one another, but also collectively enhance the network analysts’ ability to make sense of the huge volumes of data flowing through the system. To

---

<sup>28</sup> “Metadata” is essentially data about data. A common example of metadata is a library catalog, which contains information (metadata) about publications (data).

<sup>29</sup> An agent is “a program that performs some information-gathering or processing task in the background,” thus allowing the technology user to multitask. “Typically, an agent is given a very small and well-defined task.” Webopedia, “Agent,” available at <http://www.webopedia.com/TERM/a/agent.html> (last visited 3 Nov. 2003).

achieve this, the network needs to be a part of every user's workflow. For the reasons discussed above, a centralized, consolidated repository of information in Washington, DC, is impractical and vulnerable. We must therefore operate from a distributed model of interconnected databases that are made available to users through the directory services described above. The network, therefore, needs to take advantage of tools that can federate the data for analysis (that is, draw on appropriate information from various sources in the network).

Moreover, the network must allow users to move large amounts of data easily and in any form (such as written reports, photographs, video, and biometric data). Participants in the network must also be able to share across all levels of security, from "Top Secret/Code Word" to "Sensitive But Unclassified" and vice versa.

If we expect various agencies to share, then the network also needs to have strong data protection, including the ability to restrict access privileges so that data can be used only for a particular purpose, for a finite period of time, and by people with the necessary permissions.<sup>30</sup>

Thus, the network also needs access control, authentication, and full auditing capability. Data protection is critical to preventing unauthorized disclosures and to preserving traditional civil liberties. A variety of new technologies has increased the capacity for online identification and authentication, which are prerequisites for providing permission to the right people to use the network for the right reasons. These technologies can enhance the security of the network, permit multiple users to interact and trade information in a trusting environment, and allow effective oversight

<sup>30</sup> In technical terms, a permission is "[a]n access privilege (for example, read, write, execute) associated with a file or directory. Depending on the operating system, each file may have different permissions for different kinds of access and different users or groups of users." InstantWeb Online Computing Dictionary, "Permission," available at <http://www.instantweb.com/foldoc/foldoc.cgi?permission> (last visited Nov. 4, 2003).

of systems to prevent or detect misuse. These technologies include smart cards with embedded chips, tokens, biometrics, and security circuits. Many identification systems are being developed in conjunction with new data-anonymization technologies and strategies that can ensure that privacy objectives are achieved. Having these protections in place would not restrict information sharing. The protections would actually encourage sharing by engendering trust in the network and in the rules by which information is shared.

### Exhibit C Authentication technology

While authentication technologies are improving, no single approach can provide high assurance on its own. There are no smart cards or tokens that cannot be cracked, biometrics are not 100 percent reliable, and high-quality passwords are difficult to remember, manage, and enforce. With all of these technologies there are also people and process issues (such as enrollment procedures and audit trails) that can undermine their integrity. Therefore, a multifactor system is a preferable approach. Multifactor authentication typically combines a password with a token or smart card and can include other forms of authentication including biometrics, challenge codes and questions, and profile access matching. Authentication is strongest when part of the information resides with the user, a part with the token or smart card, and a part in the network. Credit card companies, good users of multifactor authentication, rely on tokens (credit cards), passwords (PIN), challenge questions ("What's your mother's maiden name?"), and profile matching ("Is this a typical charge for this individual?").

Information rights management technologies (such as those being developed for the next generation of personal computers, operating systems, and document applications) can also protect data at the document level and may be key enablers for policy management systems.<sup>31</sup> Rules about who can have access to particular documents and when documents expire can be created. High-speed encrypted storage systems are also being developed to protect the data at rest.

<sup>31</sup> We use the term "information rights management" rather than "digital rights management" to refer not just to the specific technologies used by the music and movie industries to protect their products against piracy, but to all technologies that protect and control access to and use of information. Information rights management allows individuals or organizations to specify who can access and use documents or portions of documents, and helps prevent sensitive information from being printed, forwarded, or copied by unauthorized people.

Immutable audit (the ability to maintain tamper-resistant logs of user activity on the network) and tracking are also important capabilities for building trust. The ability to trace the origin of a piece of information, who has accessed it, and how it has been used facilitates accountability.<sup>32</sup> Audit technology also facilitates tracking and monitoring to improve security and to prevent inappropriate access and use. Security watch centers can employ tools that constantly monitor data use and notify watch officers of potential violations of policy and out-of-profile usage that might warrant a call to the user. These tools also allow the originator of information to track where the information is flowing, employing technologies similar to those used for tracking express mail.

Another benefit of having strong audit and tracking is the improved ability to understand the factual dependency of information. For example, if several pieces of analysis are dependent on a single data point, and that data point is later found to be wrong, the government can trace the noted dependencies on that data point in various analytical products and then notify analysts and other users that the data is inaccurate. An example of a wrong data point is the report that a white panel truck was associated with the 2002 sniper attacks in the Washington, DC area. This wrong data point diverted the police's attention from other, truly relevant data points. As a result, the public was on the lookout for the wrong type of vehicle.

Since the network itself will be a target for both inside and outside threats, and because the information on it could also be misused, the security of the network (from both physical and cyber attack) and of the information within it must also be a priority. This requires not only new technology, but also rules and procedures for building an environment of trust. For without trust, no one will share. The system must constantly be screening for potential insider threats and misuses of the information, and should have

---

<sup>32</sup> A system with immutable audit capabilities would, for instance, immediately and permanently record who authored, changed, or accessed information; who posed queries to the system, what the queries were, and what the responses were; and who shared information with whom, and when. This means no individual could inappropriately access information or query the system and then hide the fact from an after-the-fact audit. Inspection of the audit logs can also be controlled in a way that would require multiple parties to unlock the logs, so as to make those logs tamper resistant as well.

access controls and multifactor authentication built in. In short, security and information assurance must be designed directly into every element of the network. They cannot be grafted on.

The network, too, must not only enable users to push information to others, it must also enable users to pull it on demand, or at least give each user pointers to a person who can determine whether the user is authorized to access the information. The network must support the bi-directional sharing of information between public agencies, and between agencies and private data holders and transaction processors. Users should be able to make data requests, publish and subscribe information, perform directory searches and federated queries across databases, and examine and integrate information from other portals, all from their own work environment.

In addition, the network itself must be aware. Too many of our existing analytical tools are based on the query model, and assume that analysts can ask every smart question every day. This is especially difficult because most of the information that analysts obtain is processed sequentially, in the order received. The network should constantly screen, without the need for human direction, for information that matches government watch list data and for new patterns that indicate potential terrorist activity.

Because we cannot realistically expect a new architecture to be built overnight, or ask that the federal government require all players to upgrade their operational systems to comply with sharing requirements, legacy systems will inevitably be part of the new architectures. Moreover, legacy data pertinent to the mission will still have to be accessible and shareable in the new architecture. The government should therefore have the capability to take information in any form, transform it into a useable format, perform quality assurance, and publish it on the network for access and use by the appropriate players.

With all of this information being shared, however, comes the risk of flooding the system with too much data, thereby causing the meaningful signals to be lost amid the noise. Some existing tools can help ameliorate this problem. For example, automatic personalization, extraction and categorization tools can allow users to select what sorts of information they want from the network according to their individual needs. The government also could place sensors throughout the network, which would look for information

about specific threats or individuals and only report matches. These sensors could be updated electronically so that they are always current and reporting relevant information.

#### **Exhibit D**

##### **Attributes of the SHARE network**

**The Systemwide Homeland Analysis and Resource Exchange (SHARE) Network we envision would have the following attributes:**

**1. No single points of failure**

- a. Support for redundant or complementary analyses in numerous locations
- b. Multiple and redundant communication pathways

**2. Loosely coupled architecture**

- a. Implemented in a decentralized, peer-to-peer environment in which information flows without dependence on a central information broker
- b. Data repositories should be accessed through a common data layer and kept independent from applications to allow for easier interoperability
- c. Adherence to industry-standard data-exchange practices
- d. Ability to support on-demand as well as ad hoc information sharing

**3. Directory-based services**

- a. Ability to find pointers to all information relating to persons, organizations, locations, time, and methods
- b. Ability to support publish and subscribe models for information dissemination and to permit remote queries

**4. Support for real-time operations**

- a. Real-time dissemination, collaboration, and communication
- b. Leverages the edges of the network
- c. Gets information to and from users at all levels, and provides feedback

**5. Security and accountability to prevent abuse**

- a. Multifactor authentication and access control
- b. Strong encryption and data protection
- c. Immutable audit capabilities
- d. Automated policy enforcement
- e. Perpetual, automated screening for abuses of network and intrusions

## Participants in the network: organizational structure

The technical architecture described above is only part of what is required to develop a network that brings many disparate participants together. In order to create the sort of decentralized, coordinated network we envision, the government must also address the organizational structure of the players in the network.

### The federal participants

We need to begin with a structure at the federal level that makes the sharing of information among relevant federal agencies, and with state, local, and private sector entities, a central part of its mission. Although some agency officials have become convinced that this is the right direction for government investments, the federal government has not designated an organization to lead the creation of a decentralized network. We believe that the President should take steps within the Executive Branch to clarify this leadership role. We have expressed our preference for the DHS to be assigned the lead in designing the architecture of the network and overseeing its implementation with representatives of the other participants in the network. For this effort to succeed, the cooperation of all agencies must be ensured through a combination of Executive Order, organizational structure (for example, an interagency, public-private group), and incentives that ensure a clear assignment of responsibility, adequate resources, and accountability for outcomes. In addition, the President needs to set forth, in an Executive Order, guidelines that establish the principles for using this network to improve information collection, analysis, and sharing, while protecting civil liberties.

**The President needs to set forth, in an Executive Order, guidelines that establish the principles for using this network to improve information collection, analysis, and sharing while protecting civil liberties.**

It is also important that the President clarify, in an Executive Order, the roles of the TTIC and the DHS, and clearly delineate their respective responsibilities.<sup>33</sup> If the TTIC is to be a crucial, though not exclusive, locus for fusing and sharing information within the federal government and for eliminating the gap between foreign and domestic intelligence on terrorism, then it must begin placing more emphasis on producing analyses for intelligence consumers throughout the government, rather than devoting its attention almost entirely to serving the needs of the President and other senior officials as it currently does. Any agency will naturally adjust its activities to respond to requests for information from the Executive Office of the President, even if that necessarily means devoting less attention to other parts of its mission. Therefore, the President himself must call for this change. He should make clear that serving the needs of operational components of the network is a major priority for the TTIC. Failing the necessary presidential action, Congress should consider stepping in with legislation.

In addressing the needs of the other participants in the network, the TTIC should not serve as the centralized hub of a hub-and-spoke model for information sharing. That is, information should not have to pass through the TTIC in order to be shared with other agencies. Rather, the TTIC should be one important analytical node in a decentralized system in which the participants share directly with one another.

Moreover, the creation of the TTIC as an all-source intelligence fusion and analysis center—with access to both foreign intelligence and domestic intelligence and law enforcement information concerning U.S. persons—confronts us with the question of what will replace the previous “line at the border” that largely defined the distinctive rules for foreign and domestic intelligence. There has

---

<sup>33</sup> Indeed, while the President announced the concept of the TTIC in January 2003 in his State of the Union speech, and a subsequent presidential directive (Homeland Security Presidential Directive/Hspd-6) refers to the TTIC, there is to our knowledge no presidential order that actually created the TTIC. Rather, the TTIC’s roles and responsibilities are set out in Director of Central Intelligence Directive (DCID) 2/4 (effective May 1, 2003), which is classified. This exemplifies the lack of adequate public discussion attending the creation, mission, and authorities of this important new organization.

been no significant public debate on this fundamental question, and it is a critical area for presidential guidance. It is possible that the Executive Branch has radically changed the balance of liberties with this organizational move.

**The creation of the TTIC as an all-source intelligence fusion and analysis center confronts us with the question of what will replace the previous “line at the border” that largely defined the distinctive rules for foreign and domestic intelligence.**

Foreign intelligence agencies have traditionally operated abroad with relatively few constraints on their collection activities. Domestic law enforcement and counterintelligence agencies, on the other hand, traditionally have operated under much stricter rules designed to safeguard the rights and liberties of U.S. citizens and residents. Since at least the mid-1980s, with the growth of international terrorism and international narcotics trafficking, the activities of foreign intelligence agencies and domestic law enforcement and counterintelligence agencies have increasingly overlapped. As a result, the two communities have had to work more closely and share more information than ever before.

The creation of the TTIC, however, takes this coordination and sharing to a new level. It is therefore imperative that we have an open, public debate about what new rules are needed to replace the “line at the border.” At the very least, the President should set out in an Executive Order clear guidelines governing the authority of the TTIC—and any other agencies that have access to both foreign and domestic intelligence and law enforcement information—to receive, retain, and disseminate to U.S. and foreign intelligence agencies information gathered in the U.S. about U.S. persons.<sup>34</sup> The Order should also contain

---

<sup>34</sup> Analogous issues are raised by the creation of Northern Command (NORTHCOM), the military’s unified command responsible for the defense of the U.S. and for support to civil authorities engaged in homeland security. In addition to concerns unique to the military (such as the restrictions on military involvement in law enforcement activity under the Posse Comitatus Act and DoD regulations), NORTHCOM’s mission raises

guidelines to govern the intelligence agencies’ ability to set requirements for (to “task”) domestic collection of information. These guidelines should, to the extent possible, be unclassified and put out for notice and comment so that the American public can have insight and confidence in the way domestic information is collected and used by the government. It may even be appropriate for the President to initiate this important public debate by introducing legislation to codify the appropriate scope of the TTIC’s use and dissemination of information about U.S. persons. In short, guidance is needed to empower the TTIC and other agencies’ analysts, as well as to constrain improprieties. Without it, agency personnel may be reluctant to share information that could prevent a terrorist incident.

Moreover, the Executive Branch should create within the TTIC the appropriate institutional mechanisms to safeguard privacy rights. When Congress passed legislation to establish the DHS, it was careful to include a privacy officer and a civil rights and civil liberties officer. If the TTIC is going to perform much of the analysis and information-sharing mission Congress had intended for the DHS, then it should have commensurate privacy-protection measures.

Even if the TTIC plays the role described above, we continue to believe that the DHS has a vital role to play as well. First, as noted above, the DHS should have the lead responsibility for developing the architecture for the SHARE Network we envision. Second, while we firmly believe that all federal agencies have a responsibility for sharing relevant information across all levels of government, the DHS should have the principal responsibility for facilitating and ensuring the sharing of information with state and local

---

question about what guidelines are necessary to govern the military’s access to information about domestic activities. As a Congressional Research Service report put it: “In order to defend the U.S. from attack, NORTHCOM has a strong rationale for access to information collected by various intelligence and law enforcement agencies. However, at a certain point, such access could create the perception—or the reality—that the military is spying on U.S. citizens. What type of access should NORTHCOM be given to various types of sensitive data? What types of safeguards need to be established to ensure that this data is used properly?” See CRS Report for Congress, *Homeland Security: Establishment and Implementation of Northern Command* (14 May 2003), at 5, available at <http://www.fas.org/man/crs/RS21322.pdf> (last visited 12 Nov. 2003).

governments and the private sector. Third, the DHS should focus its own analytical resources on the nation's vulnerabilities to terrorist attack and on matching those vulnerabilities with threat information from the TTIC and others to determine which targets are at greatest risk and what protective measures are needed.

The DHS's role in ensuring that information is shared with state and local governments should not preempt the FBI's unique role in sharing investigative information with state and local law enforcement agencies, since those agencies must often work jointly with the FBI on investigations. But the FBI should be more willing to share directly with state and local law enforcement agencies, and not just with the state and local representatives on the FBI-led Joint Terrorism Task Forces (JTTFs), who are precluded from sharing with their home agencies without the FBI's approval.<sup>35</sup> (See Exhibit E, below, for more information about the JTTFs.) Indeed, the FBI should see itself as part of the whole network, sharing appropriate information with all of the other relevant players, rather than viewing itself as the top entity in its own law enforcement stovepipe. Similarly, it should encourage its state and local law enforcement partners to share information directly with other players in the network, rather than actively discouraging such broad sharing.

Moreover, beyond pushing information to other players, both the DHS and the FBI should build the capability, and instill a culture of willingness, to respond to requests for information from state and local entities. Those entities have knowledge of their communities, and of vulnerabilities within and potential threats to their jurisdictions, and they need to be able to tap into the information held by the federal government in order to be effective. Accordingly, the DHS and FBI should establish

clear mechanisms for responding to requests from state and local officials for threat and vulnerability information, and these agencies should establish a culture that makes responding to such requests a priority.

Ultimately, these sharing mechanisms should be automated, allowing state and local officials to pull relevant information from federal databases. Automation would require the use of directories, data-transformation capabilities, and technology that identifies users who have permission to access certain information, as discussed above. It would also require the requisite security and auditing procedures and technology. Agencies should make such technology a procurement priority. In the short term, until the requisite technology is introduced, however, federal agencies should at least make clear whom state and local agencies can call to obtain information. This can be done by establishing online directories, which can then be built into automated systems over the long run.

#### **Exhibit E Joint Terrorism Task Forces (JTTFs)**

JTTFs are groups of state and local law enforcement officers, FBI agents, and other federal personnel who work jointly to investigate and prevent acts of terrorism, under the leadership of the FBI. These task forces are designed to tap the expertise of different agencies and facilitate the collection and sharing of intelligence.<sup>36</sup> The first JTTF was created in 1980, and the total number of task forces has more than doubled since September 11, 2001. Today, there are 84 JTTFs.<sup>37</sup> In addition, in 2002, the FBI created a National Joint Terrorism Task Force at FBI headquarters in Washington, DC. The National JTTF comprises nearly 30 intelligence, public safety, and federal, state, and local law enforcement agencies. It collects terrorism information and distributes it to the 84 JTTFs as well as to terrorism units within the FBI and partner agencies.<sup>38</sup>

<sup>35</sup> See, for example, Testimony of James Kallstrom, above at n. 6, at page 4 (stating that "important information [from the JTTFs] does not reach the officers responsible for patrolling the cities, towns, highways, villages, and neighborhoods of our country" and that the JTTFs have not sufficiently empowered state and local officers to act as "eyes and ears" by providing them with necessary information).

<sup>36</sup> See FBI, "War on Terrorism, Counterterrorism Partnerships," available at <http://www.fbi.gov/terrorinfo/counterterrorism/partnership.htm> (last visited 12 Nov. 2003).

<sup>37</sup> See FBI, Speech prepared for delivery by Director Robert S. Mueller, III, at 110th Annual Conference of the Int'l Ass'n of Chiefs of Police (24 Oct. 2003), available at <http://www.fbi.gov/pressrel/speeches/iacp102403.htm> (last visited 24 Oct. 2003).

<sup>38</sup> See FBI, "War on Terrorism, Counterterrorism Partnerships," available at <http://www.fbi.gov/terrorinfo/counterterrorism/partnership.htm> (last visited 12 Nov. 2003).

## Decentralized analytic nodes

There has been much debate about how best to achieve intelligence fusion and analysis. The discussion is often cast as a choice between centralizing this function in one agency or within several agencies in Washington, DC, and decentralizing analysis among all relevant players. In fact, this is a false choice. As our vision of the SHARE Network indicates, we need both centralized and decentralized analysis. Redundancy, or complementarity, of analysis is beneficial. We need, for example, an agency like the DHS or the TTIC that is capable of pulling together relevant intelligence and law enforcement information so that the government can put together as many pieces of the puzzle as possible and gain a full view of terrorist threats. But we also need other entities at the edges of the network that are capable of gathering pieces. Intelligence analysis is largely a matter of trying to assess the probabilities of connections among people or events from uncertain facts that are susceptible to different interpretations, and making predictive judgments about the future. Therefore, a system in which multiple analysts look at information from different points of view is more likely to reveal signs of potential terrorist activity. In addition, the reality is that the TTIC and a local or state agency might be working on different puzzles, or different parts of the same large puzzle. The TTIC might be looking at the activities of foreign terrorist groups and their plots against U.S. interests in general, while a local police agency might be looking at a specific criminal group that is only one small part of a terrorist group. We would not want, nor can we reasonably expect, a single entity to be responsible for performing both sorts of analyses. Moreover, different analytical entities produce different sorts of products for different audiences, ranging from a strategic intelligence analysis for the President or Cabinet officials to tactical leads for local police departments.

Currently, the FBI's JTTFs constitute one form of decentralized analytic nodes. Other, interdisciplinary analytical groups should also be encouraged, and these groups should be tied into the network and encouraged to communicate directly with one another as well as with the DHS and the FBI. In order for these decentralized entities to be a true part of a network rather than becoming their own stovepipes of information, it is critical that they adopt common (or at least interoperable) standards and formats for communicating and that they publish metadata about their information in integrated directories so

that their information may be easily located and shared quickly with others in the network. In addition, guidelines are needed that address not only how information should be shared, but also when it should be shared, and with whom. The DHS should work with state and local government entities to create additional decentralized analytical centers, and should foster their ability to communicate not only with the DHS and the FBI, but also directly with one another.

Beyond state and local government, private sector entities must also be brought into the network. To date, some industries have formed Information Sharing and Analysis Centers (ISACs) for the purpose of analyzing and sharing information among companies and between that industry and the federal government. These ISACs were originally formed to deal with cyber-security information. Since September 11, however, many have broadened their scope to deal with terrorism-threat information as well. But ISACs have a mixed record when it comes to the amount of information actually shared among companies or with the government. Moreover, existing ISACs are generally limited to critical infrastructure sectors (such as electrical energy, information technology and telecommunications, and financial services). As terrorists increasingly seek soft targets where they can take innocent lives without confronting tight security, it is important that the federal government have the ability to communicate quickly and broadly with non-infrastructure companies.

Thus, we believe the DHS should work with private companies to improve the two-way flow of terrorism-related information between government and industry. The DHS should help to expand the scope of all existing ISACs beyond cyber threats to include focus on terrorism-threat information, and it should encourage the ISACs to share more information with the government and with other industry ISACs. The DHS should also foster the creation of new ISACs or other mechanisms to bring together non-infrastructure companies that might be the target of attack or that might, in the course of their business, collect information related to terrorist activity. The DHS should also work with ISACs to establish information-sharing standards and, where necessary, provide seed funding.

The creation of such new analytical centers, of course, will only exacerbate the current shortage of qualified, trained analysts. It is therefore imperative that the government make training of new and existing counterterrorism analysts a priority—not

only at federal agencies, but at the state and local level and in the private sector as well. Such training would make these decentralized nodes more attuned to the kinds of information they should be looking for, and enable them to be more valuable participants in the network.

## The road to a culture of distribution

The biggest obstacle to implementing the best-designed systems in the world is often culture. Organizations, processes, and technologies can be changed, but unless fundamental changes occur in the culture of the participants in an existing system, progress is stymied. We have identified some critical vehicles for changing culture, which are discussed in this section along with the necessary processes and procedures to cement the change. We emphasize, however, that no vehicle will lead to change unless the leader at the top is completely clear about the objectives he or she seeks. Thus to implement our model, the President has to make absolutely clear that his objective is to create a decentralized network for robust information sharing and analysis that produces actionable intelligence.

Decisions about sharing intelligence in the government are still made largely in the context of a system of classification that was developed during the Cold War. Our collection efforts then were focused on maximizing collection, by human or technical means, against targets overseas. Agencies were organized around collection and had analytical units to help sort, analyze, and reduce the data to semi-finished intelligence reports. Analysis was designed to first serve a small number of senior policymakers (the President, Vice President, Secretary of Defense, Secretary of State, DCI, etc.) and second, to serve a larger but still small number of high-level decision-makers. In this context, classification was seen as an important tool to protect the sources and methods through which intelligence was collected, because access to information was limited to a small group of individuals. The government further limited access to information by imposing a requirement that any individual who wanted to see the information had to have a demonstrable “need to know,” and by establishing procedures that allowed the originating agency (the agency which first obtained the information) to strictly control the dissemination of that information within the government. This system assumed that it was possible to determine in

advance who needed to know particular information, and that the risks associated with disclosure were greater than the potential benefits of wider information sharing. The formal limits on sharing imposed by this system were exacerbated by the widely acknowledged problem of overclassification. That is, far more information was classified initially—and remained classified—than was necessary or appropriate.

This mind-set of classification and tight limits on sharing information is ill suited to today’s homeland security challenge. While certain information must be protected against unauthorized disclosure, the general mind-set must be one that strives for broad sharing of information with all of the relevant players in the network. The system must be designed to address the needs of the potential users of information, not just the security concerns of the collectors.

One of the principal reasons that federal agencies do not widely share information with one another and, especially, with state and local governments and with private sector entities is fear that the information would be leaked to the media and the public—and thus to our nation’s adversaries as well—thereby putting lives at risk, jeopardizing intelligence sources and methods, compromising law enforcement investigations or prosecutions, or violating individual privacy rights.<sup>39</sup> These are legitimate concerns. But these concerns can be ameliorated if federal agencies put in place regular processes for producing information in a way that allows it to be shared even if it comes from sensitive law enforcement or intelligence sources.

Government agencies currently rely on processes for “sanitizing” classified information so that it can be shared with other agencies. Sanitization involves removing from a report any sensitive information that the originating agency believes cannot be shared widely with other agencies without undue risk to sources and methods or some other legitimate interest, while still providing the gist of the information so that recipient agencies can take appropriate investigative or protective actions or utilize the information in their analyses.

---

<sup>39</sup> This is also true for state and local agencies. Private companies also often decline to share information, because of their concerns about disclosing information that is proprietary or that might cause public embarrassment or a loss of shareholder confidence.

Currently, some federal agencies sanitize some reports to remove source and method information. But the sanitized version is often still classified, and is usually designed for dissemination only to other federal agencies. Sanitization does not generally occur as a matter of course for many agencies, and no agency, to our knowledge, regularly produces a sanitized version of information that is unclassified and appropriate for wide-scale dissemination to state, local, and private sector entities. The sanitization process is also often slow and cumbersome.

**Instead of a culture of classification and occasional, post-facto sanitization of classified documents, we need a culture of distribution, in which the rewards go to those whose information has been found most valuable by people across the network.**

The process needs to be reversed so that distributable products are created at the outset.<sup>40</sup> That is, instead of a culture of classification and occasional, post-facto sanitization of classified documents, we need a culture of distribution, in which the rewards go to those whose information has been found most valuable by people across the network. We need to reward those who figure out exactly what information others in the distributed system need to see, and who make sure the other players get that information in a form they can use.

---

<sup>40</sup> To some extent, this can be seen as an expansion of the current approach of some agencies to producing “tear-line” reports, in which an agency produces a classified version of information with a less classified, or unclassified, version below a tear-line. In our approach, the production of such alternate versions would be commonplace and automatic. And it would be a top priority. For example, an agency would create a “Top Secret/Code Word” report that reveals the source of the information; a “Secret” version that would not reveal the source, but might give explicit detail on the threat; and a “Sensitive But Unclassified” version that might only contain the necessary action the recipient agencies should take given their specific roles in the network (for example, to be on the lookout for certain individuals or indicators of specific terrorist activity).

All federal agencies responsible for collecting terrorism-threat information also should see state and local government agencies and, in some instances, private sector entities, as regular consumers of their information. Thus, these agencies should produce unclassified reports of relevant information that may be disseminated to state, local and, in some instances, private sector entities. But one agency, the DHS, should serve as the backstop, the guarantor that as much information as possible is being shared. To do this, the DHS should establish a process for resolving disputes between originating agencies that want to prevent further dissemination and those agencies that need more information.

Technologies exist that can facilitate the sharing of sensitive information. For example, screening tools could be used to assist in the redaction process when moving information across security levels. Screening tools can automatically alert disseminators when potentially sensitive information is about to be transmitted, or when information may be about to be sent to parties that lack the requisite permission to receive it. Semi-automated systems could also suggest special-handling guidelines as well as who should be included on dissemination lists.

While such measures would foster the dissemination of actionable information to other players in the network, they would not entirely eliminate the risk of unauthorized disclosure and the harm that such disclosure can cause to both government counterterrorism operations and to citizens’ rights. Even when sources and methods or personally identifiable information is removed from a disseminated report, that report still could, if made public, reveal important clues about the government’s knowledge of a terrorist group or plot, or infringe on a citizen’s privacy if the missing pieces of data can be discerned from other sources. Moreover, as information is shared among agencies with overlapping jurisdictions, there is a risk that uncoordinated action by one agency in response to that information could impede or disrupt a sensitive counterterrorism operation by another agency. If one federal agency, for example, shares information about a terrorist group that it has been investigating clandestinely for a long period, and another agency then undertakes its own investigation of that group, the second agency’s actions could disrupt the first agency’s investigation and cause the loss of vital intelligence. Finally, a recipient of information that is not suitable for public disclosure (for example, information of uncertain credibility about a potential terrorist

threat to an infrastructure asset) could take action or make public statements that cause undue public alarm if the threat turns out to be unfounded. Additional measures must therefore be taken to minimize the risk of unauthorized disclosure of information and ensure coordination by recipient agencies before information is acted on.

While there is no easy solution to this problem, improvements can be made. Auditing technology, for example, could be deployed to track the flow of information to different players and to record how the information is used (whether, for example, it is printed, forwarded, or edited). This could help deter leaks. The auditing tools should use strong means of authentication that have forensic value (that is, they should be permissible in court to prove access). Information rights management technologies, when combined with digital certificates, can also help by allowing agencies to create self-enforcing rules about who can have access to particular documents, how they can be used, and how long the document can be viewed before access expires. Another possibility would be to make federal funding for information-sharing purposes contingent on the adherence to certain rules prohibiting unauthorized disclosure. Another improvement would be the establishment of “deconfliction” centers populated by representatives of relevant agencies, which would ensure the coordination and deconfliction of investigations and operations by multiple agencies. Finally, information could be accompanied by clearer, more specific handling requirements and dissemination limitations. While none of these measures is perfect, a combination of such efforts might reduce the chance of unauthorized disclosure or uncoordinated action, and thereby foster a healthy environment for the sort of broad communication that we envision.

Another issue that must be dealt with to foster more sharing among government agencies is digitization of data, both active data sets as well as certain important legacy data sets. As discussed above, because it is not always possible to distinguish signal from noise when information is first collected, we must ensure that even when information is not actively disseminated, or pushed, to other entities, it is registered in a directory so that it can be easily located later and pulled by analysts with the appropriate permissions. Given the vast amounts of data that are already in the system—and the vast amounts of additional data that will be collected—we cannot rely on analysts to remember information that seemed unimportant at the time it was collected, but that may be of use

later. Thus, to make the system work, information must be stored digitally, and retained long enough for it to be useful when other information comes to light. Standards should therefore be developed—under the leadership of the DHS, but with participation from experts in government, industry, nonprofit organizations and academia—to ensure that information in the network is digitized, stored, and retained, and that it is searchable at a later date.

## Measuring performance

Instituting these new processes and, more fundamentally, instilling a culture of sharing will not happen overnight. As we have said, it will require active engagement from the President himself, the National Security Council and Homeland Security Council, and the heads of agencies, as well as continual oversight from Congress to ensure follow-through. As part of the process, then, we believe agencies’ performance in meeting the information-sharing and analysis objectives should be evaluated after a reasonable implementation time. We therefore recommend that the President set forth specific and clear objectives for improved analysis and information sharing, based on the recommendations above, which each federal agency should be required to meet by December 31, 2004. At the conclusion of this period, the Executive Branch and Congress should evaluate how agencies have performed in meeting those objectives. If an agency has not performed adequately, the President and Congress should consider making any necessary changes. The government could also evaluate agencies’ performance by assessing how well they would do in meeting the information-sharing challenges set out in some of our information vignettes (see Appendix D).

We also think the DHS should include state and local government and private sector entities in a regular process for assessing how well information is being shared with them, akin to the process the intelligence community currently uses for having customers of intelligence evaluate collectors. Concomitantly, the DHS should work collaboratively with state and local governments and private sector entities to set analysis and information-sharing objectives for them to meet as well, and jointly evaluate their performance after December 31, 2004, and thereafter on an ongoing basis. See Exhibit F, below, for a set of metrics that we believe should be the basis for the Executive Branch’s and Congress’ evaluations.

## **Exhibit F**

### **Evaluating improvements in information sharing and analysis**

We have recommended that after December 31, 2004, the Executive Branch and Congress evaluate the progress of federal, state, local, and private sector entities in improving information sharing and analysis, consistent with the recommendations in our report. We set forth here some questions that Congress or others may ask to determine whether adequate progress has been made toward the goals set forth in this report. The questions reflect an ambitious, but realistic set of expectations. With issues as important as these, progress must be rapid. On matters that require significant organizational changes or new funding, however, it is not realistic to expect that the job will be completed in a single year. Therefore, some of the objectives embodied in the questions are interim steps that would represent reasonable progress toward satisfying the goals.

#### **Clarifying roles, responsibilities, and authorities**

For effective information sharing, the Executive Branch must clarify the respective roles, responsibilities, and authorities of the players responsible for homeland security information. The respective roles of the TTIC, the DCI's Counterterrorist Center (CTC), the DHS's Directorate of Information Assurance and Infrastructure Protection (IA&IP), the FBI and its JTTFs, and the Defense Department's Northern Command (NORTHCOM) are not clearly defined. As long as this remains true, there will be turf battles among agencies and, most significantly, gaps in information sharing and analysis. Moreover, regardless of how these entities' roles are defined, foreign intelligence agencies will continue to have greater access to information about U.S. persons (citizens and legal resident aliens) than in the past. This increased access blurs a line that has long been in place to reduce the risk of government abuse of privacy and other civil liberties of U.S. persons. Although increased information sharing among law enforcement and intelligence entities is critical to the counterterrorism mission, no clear government-wide direction has been established for appropriate handling of domestic information while protecting civil liberties.

#### **Question set 1:**

Are the federal government's homeland security agencies and players acting with clear guidance about their respective roles and responsibilities for information sharing, collection, and analysis? Which agency or agencies are responsible for communicating with state, local, and private sector players about homeland security intelligence, threats, and warnings? What are the respective analytic responsibilities of the players? Which intelligence entities have tasking authority over domestic collection, and how can that authority be exercised and coordinated?

#### **Question set 2**

Are homeland security agencies and players acting with clear guidance for the collection, handling, and dissemination of information about U.S. persons? Does this guidance permit the flow of information necessary to fight terrorism, but maintain the protection traditionally afforded U.S.-person information? Is the guidance, to the maximum extent possible, available to the public?

#### **Information sharing within the federal government**

Although there have been significant advances since September 11 in the ability and willingness of intelligence, law enforcement, and other agencies to share information relevant to countering terrorism, significant roadblocks remain. Thus, the Executive Branch must make greater and more rapid progress toward removing them.

#### **Question set 3**

Have the federal homeland security agencies taken significant and measurable steps toward adopting an information-technology architecture with the basic characteristics that the Task Force has described? Does each agency have sufficient guidance for procuring new technology so that it does not buy products incompatible with this architecture?

## **Exhibit F**

### **Evaluating improvements in information sharing and analysis (Contd)**

#### **Question set 4**

Are all terrorism-related watch lists in the federal government available for combined searching in real time, or at least for the matching of names and related information? Are there consistent standards regarding how individuals are placed on watch lists, how information about such individuals is managed, what types of data should be kept to enhance the government's ability to confirm identities of individuals, and the process for correcting errors and allowing innocent people to be removed from such lists?

#### **Question set 5**

Are terrorism intelligence and threat and warning information flowing efficiently and effectively through clear channels and with regular auditable procedures rather than through informal channels that are based on personal relationships and ad hoc judgments about who should receive information?

#### **Question set 6**

Have bureaucratic or other institutional roadblocks to sharing information—such as requirements for originator approval, inadequacy of facilities for storing classified information, and “paper only” intelligence products—been eliminated or minimized? Have positive incentives been developed to foster more information sharing, such as rewarding analysts who produce disseminable products that are of great value to others in the network?

#### **Question set 7**

Are FBI field offices producing intelligence reports—even from ongoing cases? And are they immediately and automatically sharing these reports with FBI headquarters and other appropriate recipients?

#### **Producing intelligence for a new customer**

Intelligence agencies often see their job as sending information up to the President and other senior officials. They do not always view operational entities—particularly those outside of the federal government—as their customers. Therefore, they are not accustomed to creating reports that are available or useful for these other entities. One of the principal reasons that homeland security threat information and other intelligence reports are not shared widely is that they are classified. An important step in creating the culture of distribution that the Task Force recommends is to increase the information that is available for distribution—that is, unclassified information.

#### **Question set 8**

Are intelligence agencies responding to the intelligence needs of their new customers? Is there regular, formal interaction between those responsible for preparing intelligence in the federal government and the state, local, and private sector players who need information? Does this interaction result in specific, substantive requirements for intelligence producers?

#### **Question set 9**

Has it become part of the culture of intelligence agencies to create unclassified versions of intelligence reports on terrorism? Are there reward and audit mechanisms to encourage this culture? Do automated report formats have required fields for an unclassified version? Are unclassified versions prepared for at least 80 percent of these reports? Is there a mechanism for a non-originating agency to seek further declassification? When used, does this mechanism result in further declassification a significant percentage of the time?

## **Exhibit F**

### **Evaluating improvements in information sharing and analysis (Contd)**

#### **Communicating with state and local governments and the private sector**

In addition to producing intelligence for these new customers, there are a number of steps the Executive Branch should take to promote a networked information architecture and improve communication with players outside of the federal government about intelligence, threats, and other information relevant to countering terrorism.

#### **Question set 10**

Has the federal government convened state, local, and private sector players to develop common standards for information sharing? Have the parties developed common or interoperable metadata formats and definitions, directory formats, and communications methods and protocols to facilitate information sharing by all players across the network? Have they developed common or consistent policies on retention, dissemination, and sharing of data? Has the government leveraged appropriate technologies (such as anonymization, information rights management, automatic policy enforcement, and immutable audit) that may enhance information sharing, protect sensitive information, and foster auditing and accountability?

#### **Question set 11**

Has the federal government coordinated and provided incentives for the digitization of data in state, local, and private sector systems? Is this data accessible online in a secure manner and in near real time? If not, have these parties taken significant and measurable steps toward adopting these system changes?

#### **Question set 12**

Has the DHS established up-to-date and updateable contact and profile directories that are available to all players in the homeland security network? Do those directories include contact and profile information for businesses and other entities that are potential targets or that might require threat information for other reasons; for experts in government, the private sector, and academia, who can be called upon for guidance or insight with regard to a particular threats; and for other specialists and entities that might either contribute or require information about homeland security threats or warnings? Is the DHS utilizing existing technologies to create and manage these profiles and ensuring that the profiles are current and relevant?

#### **Question set 13**

Are state and local law enforcement personnel able—quickly and automatically—to do a name match between federal terrorism watch lists and individuals they have in custody or under surveillance, and to obtain more information about those individuals from federal sources? Is that additional information sufficient to provide useful guidance to state and local authorities on how to proceed with that individual, and to reduce false positives (that is, to determine whether the person in custody or under surveillance is actually the same person as the one on the federal watch list)?

#### **Question set 14**

Does the federal government—in particular the DHS and the FBI—have clear, workable procedures for sharing intelligence and threat information with state, local, and private sector homeland security players? Do these nonfederal players understand these procedures, and if so, do they take advantage of them?

#### **Question set 15**

Is there regular and substantive communication between the federal government—particularly the DHS and the FBI—and nonfederal homeland security players about intelligence and threat information? Does the communication flow in both directions? Have federal entities established mechanisms to encourage and reward their employees' responsiveness to nonfederal players? Are the nonfederal players satisfied with this interaction? Can the federal entities effectively ingest and utilize information from state and local actors?

**Exhibit F****Evaluating improvements in information sharing and analysis (Contd)****Question set 16**

Have the parties developed mechanisms for communicating targeted requests for information from the federal government to nonfederal homeland security players, and if so, are these mechanisms in use? Can the DHS or FBI point to several specific examples of targeted requests for information that have generated thorough and useful responses from state, local, or private sector entities?

**Improving analysis**

It is critical to a homeland security information-sharing network that the information being shared is accurate and that its significance is understood. This requires analysis that combines substantive expertise and first-rate analytic tradecraft. In addition, analysis of threats to homeland security cannot all occur at the top—that is, in Washington, DC. To be effective, analysis must occur at all levels of the network.

**Question set 17**

Is there a federal government entity responsible specifically for producing long-term, strategic analysis of terrorist threats? Does that entity have the number and quality of analysts necessary to carry out that function? Is it actually producing a steady and useful stream of such intelligence?

**Question set 18**

Are federal government intelligence agencies producing analysis for the entire range of customers who need it, including operational entities, the DHS and nonfederal actors? Are agency analysts according equal priority to analyses directed primarily at customers other than the President and senior policy officials as they are to analyses for these high-level officials, such as the President's Terrorism Threat Report and the President's Daily Brief? Are federal agencies providing access to useful data sets to foster decentralized analysis at the nonfederal levels?

**Question set 19**

Is the DHS producing—as its authorizing statute requires—analysis of the nature and scope of threats and potential vulnerabilities? Do its analysts have sufficient training and expertise in important areas, such as target industries (the airline industry, for example) and threat categories (the energy sector, for example), to produce quality analysis? Is the DHS producing actionable intelligence?

**Question set 20**

Is analysis occurring in the field, including at JTFs and FBI field offices and in state, local, and regional analysis centers and organizations? Do these field analytical units have an understanding of broader analytical needs, and do they communicate regularly and effectively with other homeland security players? Are these field units receiving adequate training?

**Improving the capabilities of state, local, and private sector entities**

To be effective participants in the network, state, local, and private sector entities also need to take steps to increase their capacity to share and analyze information.

**Question set 21**

Have regional or state groups formed to promote information sharing and prepare for homeland security threats? Do these groups include representation from federal, state, local, and key private sector players in law enforcement, public health, and emergency preparedness? Are all 50 states, the District of Columbia, and U.S. territories participating in this type of group? Are state, local, and regional entities effectively sharing their information with each other and with the federal government?

**Exhibit F****Evaluating improvements in information sharing and analysis (Contd)****Question set 22**

Have law enforcement organizations in key localities that are the most likely targets of terrorist attack, or that have been the locus of terrorist planning and other activity (such as the New York metropolitan area; the Washington, DC, metropolitan area; Los Angeles, Chicago; Detroit; Phoenix; southern Florida; the Bay Area; Las Vegas; and Seattle) implemented information-system upgrades and digitization of metadata using common standards? Have additional jurisdictions taken steps toward implementation?

**Question set 23**

Have local or regional analytic centers been formed in key cities or regions such as the ones listed above? Have additional jurisdictions taken steps toward the formation of such centers?

**Question set 24**

Have ISACs or other government-industry groups been formed by key industries (including those not considered critical-infrastructure industries) for which no such groups currently exist? Are these groups effective at sharing threat and vulnerability information quickly (and preferably automatically), conducting analysis relevant to their industries, and communicating with federal, state, and local agencies?

## Accessing private sector data

---

Today, the private sector is on the frontline of the homeland security effort. Its members are holders of data that may prove crucial to identifying and locating terrorists or thwarting terrorist attacks, and stewards of critical infrastructure and dangerous materials that must be protected. Thus, the private sector is the source of information that is essential to counterterrorism. We therefore start from the premise that the government must have access to that information, which is needed to protect our country, and that through a combination of well-crafted guidelines, careful articulation of the types of information needed for identified purposes, and effective oversight using modern information technology, it will be possible to assure that the government gets that information in a way that protects our essential liberties.

### Information available in the private sector

In the past decade, we have seen an explosion in the quantity of personal information held by the private sector. Transactional data—such as point-of-sale data, credit card records, travel records, and cell phone call logs—increasingly makes it possible to track in minute detail, and sometimes in real time, the activities of individuals. (See Appendix H for a description of the many types of data available.) Access to this sort of data can be critical to a government agency’s ability to investigate and understand the intentions of a suspected terrorist.

The challenging policy issue comes when the government tries to use private sector data to detect signs of potential terrorist activity by people it does *not* already have reason to suspect. Although using data in this way can be beneficial (see Appendices D and E for illustrations of how privately held data might help agencies understand the significance of suspicious activity by previously unknown entities), it raises serious civil liberties concerns.

Internet technologies, such as cookies, potentially allow (if linked with other information) access to some of the most private indicators of personal behavior and interest. And the exponential increases in both computing and storage capability at exponentially diminishing costs have made it possible—and inexpensive—to collect and exploit

petabytes of data on virtually every aspect of our lives. For example, supercomputer performance can now be obtained at desktop prices by clustering 64-bit processors with terabytes of storage. This can be both a benefit and a threat. It can, for example, allow government authorities to examine transactional information that a terrorist believes is effectively beyond government scrutiny, and thus help those authorities to uncover a plot in progress. But it can also allow for intrusion into the personal lives of individuals whom the government has no cause to suspect of criminal activity.

All of this data is collected not under government mandate, but as a consequence of the more or less voluntary decision of citizens to avail themselves of services that require (or allow) private companies to collect information on their activities. In other words, customers appear willing to give up a certain amount of privacy in exchange for better service. For example, an online bookseller uses a customer’s profile of past purchases to suggest new titles that may be of interest; a credit card company alerts a customer to unusual purchasing patterns that may indicate a stolen credit card or identity theft.

Often, however, information collected by private sector entities is used for purposes other than those for which the customer provided it. In fact, a great deal of information sharing takes place for commercial purposes without the knowledge or express consent of the consumer. This seems to be tolerated by consumers in part because it has led to an expansion of the commercial services available to them. Moreover, the standards for technologies like cookies were established in technical organizations before many of the public policy issues involved had surfaced, and many consumers appear to accept them for the limited purposes to which they have been put to date.

Moreover, in recent years, the scale of information collection has been dramatically augmented by the rise of data aggregation companies that acquire data from individual collectors in order to create vast databases that allow users to cross-reference data from diverse sources (including, in some circumstances, public sector records such as driver’s licenses and property deed transfers). Collection sources as well as the algorithms used to create these data sets generally are proprietary. Data from aggregators has been used by companies for activities ranging from marketing to risk assessment, and by the government for law enforcement and to locate missing children.

Government agencies can readily buy these data sets from data aggregators, who can deliver the data to government users in any format necessary for immediate analysis. In addition, the aggregator can perform a certain amount of initial analysis, breaking down larger data sets into more focused collections of data called “data marts.”

Government agencies can then merge these data sets into other data sets that they routinely maintain or collect (for example, criminal records or intelligence information). Moreover, sophisticated data mining or “knowledge management” software, as well as technologies for profiling, pattern analysis, link analysis, and transactional fingerprinting, are readily available either as procurable hardware or software or as a service from the commercial sector. These technologies can allow agencies to analyze both structured (organized in a predefined, meaningful way) and unstructured data, allowing them to find patterns of activity or links among individuals and derive value from the sea of largely disorganized data available in various sources of transactional information. The result is a vastly richer data context, and thus more wide-ranging and, ultimately, effective analysis.

Much data is also available from open sources, such as the Internet. While much of that information can be valuable, it can also be of poor quality, come from questionable sources, and be easily manipulated. The government therefore needs to take special care when it integrates open source information into its data analyses.

Government agencies have always had access to certain kinds of privately held information. But historically, information requests to commercial organizations were made by government agencies on a case-by-case basis. Companies would either volunteer the information or fulfill a specific subpoena request from law enforcement. In some cases, the law might impose specific collection and reporting requirements (such as with financial services firms, which must submit Suspicious Activity Reports to regulatory agencies).

With the advent of data-mining and analysis tools and the increasing computational capability of computers and decreasing costs of storage, agencies at all levels of government are now interested in collecting large amounts of data from commercial sources. Such data might be used not only for investigations of specific people (for example, to help find associates of a suspected terrorist) but also to perform large-scale data analysis and pattern discovery in order to discern

potential terrorist activity by unknown individuals. Both uses of private-sector data, but particularly the latter, have raised a number of concerns from industry and privacy advocates, as well as from the broader public and Congress. Companies are concerned about both the cost of supporting ongoing data flows to the government and the potential damage to their reputations and businesses if their data is misused. Privacy advocates and many in the public are concerned that the government will have access to large repositories of personal identifiable information, which are often of questionable quality and which could be used inappropriately to profile U.S. citizens or legal residents and possibly result in the denial of services or infringement of civil liberties based on people’s race, country of origin, political views, or personal habits. Additionally, there is concern about potential mission creep: while the government may collect data today for counterterrorism purposes, once the government has the data, there are no guarantees that it won’t use the data for other purposes in the future. In fact, many responsible legislators advocate that collected data should, in fact, be used for other purposes. Contributing to all of the above concerns is the lack of transparency and accountability of the algorithms used by the government against large data sets to rate (or “score”) potential threats.

Another, more specific use of private sector data is to resolve, or confirm, identities. When a government agent is using a watch list, investigating a person, or tracing a phone number, he or she needs to be able to determine whether the person or thing being examined is, in fact, the intended object of inquiry. Without identity resolution, watch lists can be cumbersome and ineffective; use of them can generate many false positives and false negatives, and investigations can be led down blind alleys. The government needs access to appropriate identity resolution data and services, and private companies are the best source of those services. Moreover, with appropriate safeguards, effective identity resolution can also have important civil liberties benefits: it can help distinguish between those who should legitimately be the subject of scrutiny and those who should not.

## **Identifying the private sector information the government needs**

So the question is, how can the government best make use of the vast volumes of private sector data

while protecting civil liberties and avoiding the imposition of undue costs on industry? As we said in our first report, “Data mining can be a useful tool. But it is also a tool that invites concern about invasion of privacy.... 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” (page 31).

We believe the place to start is identifying concretely the information the government needs to carry out its homeland security responsibilities. The best way to do this is to consider realistic situations that the government might confront. To this end, the Task Force developed several scenarios in order to identify some kinds of privately held data that the government might need when confronted with certain situations (see Appendices D and F). In some of our scenarios, the government would start with limited information about the mode of a planned attack (for example, a scuba diver attack on a hazmat tanker ship) and might need information on the identities of people who have the capability or access to the means to carry out that mode of attack (such as certified scuba divers) and information on facilities where the means can be obtained (such as dive shops). In other scenarios, the government would start with particularized suspicion about specific individuals, and then might seek to identify the suspects’ associates by looking at records of common or related addresses, telephone and email accounts, financial transactions, and travel.

But our scenarios, and the resulting information categories, are purely illustrative. The crucial point is that this is the sort of approach that the government should take as a preliminary step, so that it can concretely identify its true information needs before launching controversial efforts to accumulate or mine large volumes of privately held data.

## **Guidelines for government use of private sector information**

The next critical step is for the government to establish guidelines to regulate access to, use, and sharing of private sector data among agencies. These guidelines would help the government to ensure that: (1.) information is used in ways that are consistent with core national values, including privacy, other civil liberties, and the functioning of an accountable democratic political system; (2.) investigatory resources are deployed in a cost-

effective manner to achieve priority goals, without wasting government resources or imposing undue costs on industry; and (3.) government personnel have clarity about what is permissible, so that they are not overly reluctant to engage in perfectly legitimate activity for fear of public or congressional backlash. For many, these goals are seen as contradictory, requiring trade-offs between security and liberty, or between government empowerment and individual liberties. But we believe these goals are in fact complementary. By focusing information strategies on high-priority uses and making the rules clear, the government could reduce the impact on privacy and related concerns, empower agency personnel to take the necessary steps to collect and analyze information, and enhance public support for those aspects of the information strategy that are truly essential.

Given the nature of the security problem, it is inevitable that some of the details of the guidelines will need to be classified. But that should not stand as a barrier to public discussion of the core issues discussed in this report. If the government is to sustain public support for its efforts, it must demonstrate that the information it seeks to acquire is genuinely important to the security mission, and that it is obtained and used in a way that minimizes the impact on privacy and civil liberties. The reason we seek to strengthen our homeland security effort is to protect our safety and our way of life. So the government’s approach must give the public confidence that the value of collected information is significant in relation to the potential impact that collection will have on civil liberties and other important interests.

**If the government is to sustain public support for its efforts, it must demonstrate that the information it seeks to acquire is genuinely important to the security mission, and that it is obtained and used in a way that minimizes the impact on privacy and civil liberties.**

In thinking about guidelines, the government should start with the basic architecture—what is the appropriate level of protection for different types of information, and what kinds of standards and procedures might provide that protection. The current legal framework governing access to and

use of privately held data is a patchwork quilt of different standards for information with similar sensitivity (such as wire, cable, and Internet communications) and inappropriate or nonexistent standards for other kinds of information.<sup>41</sup> The complexity of these rules, and the confusion they engender, may cause government officials to be reluctant to take lawful and necessary action to gather important counterterrorism information for fear of crossing a vague line. At the same time, these rules offer little assurance to the public that their rights are adequately protected. We do not think it would be realistic or desirable to replace this set of rules overnight. But we do think that greater clarity is needed, and that over time the government should seek greater consistency in the rules governing various forms of privately held information, and that it should develop guidelines that bear a closer relation to the fundamental interests at stake. New guidelines should, at a minimum, address: (1.) government acquisition and use of private sector data; (2.) government retention of the data; (3.) sharing of the data by the acquiring agency with other agencies for purposes other than counterterrorism; and (4.) accountability and oversight. Following are principles that the government should consider in developing guidelines to address these issues.

### **Acquisition and use of private sector data**

Rules governing access to and use of private sector data should be based primarily on two dominant considerations: the value of the information to the government, and the sensitivity of the information from the perspective of individual privacy and other civil liberties. Thus, for example, large data sets with information on individuals with no known connection to terrorism are of relatively low value to the government, while information on the whereabouts and activities of an individual who is credibly believed to pose a threat is of high value. With regard to the sensitivity of the information, non-personally identifiable information is the least sensitive; personally identifiable information that is generally available to the public (such as through a Google search) is more sensitive; personally

identifiable information not generally available to the public (such as information provided to a vendor on the condition that there be no third-party dissemination) is still more sensitive; and certain personal information (such as financial or health records) is the most sensitive.

One particularly contentious issue is under what circumstances the government should have access to information that is widely available to the public. As discussed above, the explosion of information technology has meant that vast quantities of information are now generally available to the public, including personally identifiable information about relatively sensitive matters. A whole industry has sprung up consisting of firms that collect, aggregate, and mine that data for a variety of tasks, including employment screening, marketing, and risk assessment. In most cases these firms neither seek nor require the approval of the subject of the information; and the legal constraints are few except with regard to a small number of sensitive areas, such as health records under the Health Insurance Portability and Accountability Act (HIPAA).

Under current law, there are few restrictions on the government's ability to gain access to this kind of information. And many argue that this is appropriate, that it should be no more difficult for the government to gather information than it is for a commercial company or private citizen. We believe, however, that different considerations apply to government acquisition and use of personally identifiable data, even when it is widely available to the public. Although there are consequences associated with the data's being available in the private sector (such as loss of job opportunities, credit worthiness, or public embarrassment), the consequences of government access to and use of the data can be more far-reaching, and can include loss of liberty and encroachment on the constitutionally rooted right of privacy (both in the Fourth Amendment and more generally), which is designed to protect citizens from intrusions by government, not neighbors or credit bureaus. Therefore, we believe that the government should not have routine access to personally identifiable information even if that information is widely available to the public.<sup>42</sup>

---

<sup>41</sup> The Task Force has prepared two matrices that set out the diverse array of laws and regulations covering governmental and commercial access to privately held data. See [www.markletaskforce.org](http://www.markletaskforce.org).

---

<sup>42</sup> Another example of government forbearance regarding information that it might be legally entitled to collect involves "cookies." The OMB has issued a rule prohibiting federal agencies from using persistent cookies (for example, cookies that lasted longer than a single session) to track visits to their websites absent demonstration of a compelling need and clear notice to

At a minimum, there should be a requirement that the information be relevant to the counterterrorism mission, and that this showing be documented and subject to periodic audit.

**We believe that the government should not have routine access to personally identifiable information even if that information is widely available to the public.**

Technology can assist in enforcing such access and use guidelines. For instance, anonymizing technologies could be employed to allow analysts to perform link analysis among data sets without disclosing personally identifiable information. By employing techniques such as one-way hashing,<sup>43</sup> masking, and blind matching, analysts can perform their jobs and search for suspicious patterns without the need to gain access to personal data until they make the requisite showing for disclosure.

### **Government retention of private sector data**

In our first report, we expressed our strong preference for keeping data in the private sector whenever possible, rather than having the government retain it. This would be a prophylactic measure to help ensure that data gathered for one purpose was not impermissibly used for another purpose and to promote public confidence that the government is not inquiring into the activities of innocent people. Leaving data in private sector

---

the public. See Joshua B. Bolton, U.S. OMB, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (26 Sept. 2003), available at <http://www.whitehouse.gov/omb/memoranda/m03-22.html> (last visited 12 Nov. 2003).

<sup>43</sup> A one-way hash is “[a]n algorithm that turns messages or text into a fixed string of digits, usually for security or data-management purposes. The ‘one way’ means that it is nearly impossible to derive the original text from the string. A one-way-hash function is used to create digital signatures, which in turn identify and authenticate the sender and message of a digitally distributed message.” Webopedia, “One-way-hash function,” at [http://www.webopedia.com/TERM/O/one-way\\_hash\\_function.html](http://www.webopedia.com/TERM/O/one-way_hash_function.html) (last visited 4 Nov. 2003).

hands has another advantage: the data can be searched as part of a broad inquiry without creating any stigma that would be associated with the government’s holding that data itself. When the government conducts a search of privately held data, it is easier to maintain the sense that the searched data is simply part of an overall information landscape, and that the fact that particular data was searched does not connote anything about the individual who is the subject of the data. The government should strive for an approach to data mining that allows it to find correlations but without suggesting anything about the meaning of the data until after the data is analyzed.

In addition to the policy objections, there are technical and security reasons not to create large government databases. Quality management of such centralized government databases would be very difficult; when obsolete or inaccurate data is updated or corrected by the private sector source, the data would not necessarily—or easily—be updated or corrected in the central government repository. In addition, a centralized repository would become a target for cyber attack and espionage, a problem that can be mitigated by leaving the data in decentralized private databases.

There is some concern that this approach could result in costly delays in government access when urgency is vital. However, we believe that such delays can be ameliorated if directories and pointers to the private holders of information are used, and if information is accessible electronically and in a useable format once permission is obtained. Virtual aggregation and networking can also be part of the solution to this problem. Similarly, anonymizing technologies can be used to permit enterprises that screen for specific patterns and watch list matches to report to the appropriate agency only the information necessary to indicate when there are specific matches. The agency could then obtain the underlying information only after it made the requisite showing under the applicable guidelines. This would help prevent the government from amassing large databases of private transactional information and provide a more robust real-time solution than classical data mining approaches.

In areas where the government has a compelling need to retain information, a solution might be to create trusted data banks within the government with strict limitations on who has access to the underlying data and for what specific purpose. Another way to help limit the retention of data to

that which is essential to the mission would be to require formal, written justifications for the creation and retention of data sets that contain personally identifiable information. These justifications would be subject to review at the time the data set was created and also periodically thereafter to ensure that there was an ongoing need to retain the data. Justifications should be subject to fairly rigorous standards, such as “inability of the government to retain the data would significantly impede the counterterrorism mission.”

### **Sharing private sector data with agencies not involved in counterterrorism**

A key reason for leaving information in the hands of the private sector originator or aggregator is to avoid the risk that, once acquired by the government for a legitimate counterterrorism purpose, the data will be used for a different purpose without authorization by policymakers. This poses problems not only when the subsequent purpose is illegitimate, but also when the purpose is legitimate but unrelated to counterterrorism (such as the use of counterterrorism data to enforce child-support obligations). That said, an absolute ban on using counterterrorism information for any other purpose achieves the prophylactic goal at a potentially high cost—why should the government be barred from sharing information between agencies if the second agency could acquire the information directly from the private sector on its own? There will be considerable resistance to requiring agencies to acquire costly duplicate data sets simply to guard against the theoretical possibility that the data might be misused.

To avoid this problem, clear guidelines and procedures are necessary to permit legitimate sharing, and also to establish accountability for improper use. An agency wishing to acquire data that was first obtained for counterterrorism purposes should have to demonstrate that it was entitled to get the information directly under equally or less stringent substantive standards than those applicable to counterterrorism. Technology can assist in enforcing these guidelines. For instance, role-based access-control technology could restrict access to certain information to only those who had the appropriate permissions. Permission levels would be determined according to policy determinations but could be enforced through the use of technological markers assigned to specific users. Thus, if a police investigator

working on a white-collar crime case attempted to access a database or record that was restricted to counterterrorism uses, for which he did not have the requisite permission, he would automatically be denied access. Encryption and key management could also be used to control access by making data available for only a specified period of time and to a specified set of users. If someone without the appropriate decryption key attempted to access the data, he would not be able to access it (or view it in plaintext). And when the decryption key expired, users who had been authorized would no longer be able to view the data either.

### **Accountability and oversight**

Guidelines must also address the question of how we assure compliance with the required policies and procedures and foster accountability. In the highly decentralized system that we envision, there will be no single agency or entity with overall responsibility for the day-to-day decisions to acquire, retain, or disseminate private sector information. At the same time, relatively uniform standards and compliance are difficult to achieve if each agency is separately interpreting, applying and auditing compliance with the guidelines.

We believe a blended system is necessary. Government-wide rules will be necessary, and some agency must have overall supervisory responsibility to oversee the application of the guidelines, including the training of personnel, the implementation of auditing procedures, and the imposition of consequences for failure to comply. We think the DHS should play this central role, particularly in light of Congress’ decision to create strong privacy oversight as an element of the DHS structure. At the same time, each agency has a responsibility to develop its own procedures to assure compliance. This will be the most effective day-to-day guarantee that the guidelines are, in fact, respected.

Technology can play a key role in assuring accountability and transparency. For example, personally identifiable data can be anonymized so that personal data is not seen unless and until the requisite showing (specified in guidelines) is made. Selective revelation, another technique that permits a user to see only that data for which he or she has the appropriate permissions, can also be used. Auditing technology, too, can provide built-in recording and documentation capabilities to track how information is used, retained, and shared. Strong auditing capabilities could also allow

individuals to make Privacy Act or Freedom of Information Act requests to see what was done with the data about them.<sup>44</sup> These technologies would also permit independent, third-party auditing of the data mining and scoring algorithms used in pattern analysis systems such as those that might be used in CAPPs II. This would help ensure adherence to guidelines regarding permissible data sources and profiling. Information rights management technologies could also be employed by commercial enterprises to restrict the use of supplied data to a particular purpose and for a particular period of time. The potential utility of such technologies underscores the need to develop technology architecture in parallel with the development of the substantive policies embedded in the guidelines.

Another aspect of oversight is ensuring the accuracy of the data that is brought into the network. Accuracy is vital not only to protect the privacy and civil liberties of individuals who can be harmed by the use of inaccurate data, but also to assure that information has real value to the counterterrorism effort. Data anomalies or false positives that mistakenly suggest that an innocent person is somehow tied to terrorist activity can, if uncorrected, have significant adverse effects on the individual. They can also waste scarce investigative resources. Fortunately, technologies exist that can help assure that information is up-to-date. For instance, agencies could use directories, pointers, and Web services so that there is only one data source (preferably in the private sector, as discussed above), which is always kept current. Version control and update software can also ensure that information is updated according to a regular schedule. Expiration-enforcement software can ensure that data is unusable after a certain date. And data pedigree technology can permit users to track the information that has been used in an analytical product and visualize information dependencies. Technology can also enable systems to alert the holders of derivative documents if the original underlying data has been changed, or even to change the derivative document if the underlying data is replaced in full rather than merely modified.

Technology, of course, is only one part of the solution. We also need, as part of the guidelines,

policies that make it possible for individuals to have an opportunity to correct errors in information about themselves.

It is also important to make forms of identification in the physical world more reliable, since the reliability of the identities of people who are the subject of government scrutiny—via an investigation, analysis, or a security checkpoint—is a crucial precondition to the successful implementation of the Task Force’s main recommendations. We have identified some problems that currently render the most common forms of identification distinctly unreliable, and recommend both near-term measures and a longer-term research agenda to increase the reliability of identification while protecting privacy (see Appendix A).

Finally, indiscriminate requests for information not only pose risks to civil liberties but also potentially place a serious burden on private sector holders of the information. To the extent that data from the private sector is a “free good” for government, there will be an inherent tendency to overconsume it on the grounds that any information might eventually prove useful. Equally important, a vacuum cleaner approach could actually impede homeland security efforts by inundating the government with information of little or no value, thus complicating analysts’ ability to distinguish signal from noise and wasting valuable investigative resources.

Market mechanisms can help ensure that government officials take into account the costs and benefits of data requests—for example, by requiring the government to compensate private holders for the costs of furnishing data. This requirement should apply in particular where the requests are ongoing, costs are high, and where the cost of complying might put the holder at a competitive disadvantage. The government should enter into an ongoing dialogue with companies that are likely to be the subject of repeated requests and formulate procedures that would minimize the impact on the private sector while assuring that the government is able to access and use the information it needs. The market already prices much of the data that the government is likely to request. For that which is not priced, cost equations can be developed by a consortium of members of the private and public sectors on the basis of the scope of the information being requested and the timing and complexity of the request.

---

<sup>44</sup> See Freedom of Information Act, 5 U.S.C. § 552 (2003), and Privacy Act, 5 U.S.C. § 552a (2003).

At the same time, private sector holders of information also have some responsibility as citizens to assist in carrying out this vital national mission. Thus, in cases where the requests are infrequent and the costs are low, we believe that requiring compensation would be inappropriate. In such cases, employee training—supplemented by periodic, post hoc agency reviews—should be conducted to assure that government officials are sensitive to cost-benefit considerations in formulating data requests.

Congress plays a critical role in this system of oversight and accountability, and we encourage the development of informal and formal means of congressional oversight of the government's access to, use, retention, and dissemination of private sector data. In addition, we recommend that both the Executive Branch and Congress review agencies' performance in this area, from the perspective of both efficacy and protection of civil liberties. Some proposed metrics to evaluate the government's performance are set forth below in Exhibit G. The government could also measure

agencies' performance by assessing how well those agencies would do in meeting the challenges set forth in our technology challenge scenarios (see Appendix F) and in our information vignette concerning access to and use of privately held data (see Appendix D).

#### **Exhibit G**

##### **Evaluating improvements in the government's use of private sector data while protecting civil liberties**

As with the issue of information sharing among government agencies, we believe the Executive Branch and Congress should evaluate the progress of federal agencies in improving the way they collect, use, and disseminate private sector data while protecting core national values such as privacy and civil liberties. We set forth here some questions that Congress or others may ask after December 31, 2004, to determine whether adequate progress has been made toward the report's objectives.

##### **Question set 1**

Has the President issued guidelines for the collection and use of private sector information on U.S. persons? Were these guidelines put out in draft form for public notice and comment?

##### **Question set 2**

Has the Executive Branch created a directory that includes all relevant information from both governmental and appropriate private sector databases, and has it made this directory available to all appropriate homeland security players? Has the government made these databases accessible for appropriate rapid, federated searches?

##### **Question set 3**

Has the intelligence community implemented an ongoing process for determining intelligence requirements for private sector data? Are the results of the process subject to adequately high-level review and approval? Are intelligence collection priorities adjusted periodically so that they remain in line with these requirements?

**Exhibit G****Evaluating improvements in the government's use of private sector data while protecting civil liberties (Contd)****Question set 4**

Have the DHS and law enforcement agencies developed policies and provided guidance to investigators on when to conduct searches of private sector databases? Do these policies and guidelines address the use of commercial data aggregation services? Do they promote consistency in the use of these searches but remain flexible enough to allow investigators to adjust to the unique circumstances of individual investigations? Do the policies reflect a balancing of investigatory benefits of these searches against the potential negative impact on the privacy of U.S. persons and the private sector's conduct of business? Do the policies include a requirement that the government compensate private sector data holders for the conduct of these searches under some circumstances and provide guidance on those circumstances?

**Question set 5**

Do government employees who have access to private sector data on U.S. persons for counterterrorism purposes have clear guidelines—that are broadly consistent throughout the government—on the reasons for which they may access this data? Do the guidelines make clear when approval is necessary before accessing data and at what level, and when post hoc reporting and review are sufficient? Do the standards and procedures in the guidelines reflect a balancing of the value of the information sought and the sensitivity of the information? Do the guidelines preclude completely unfettered access by government employees to personally identifiable information on U.S. persons—even if that information is available to the public?

**Question set 6**

Do government agencies that access private sector data on U.S. persons for counterterrorism purposes have clear guidelines—that are broadly consistent throughout the government—on when and for how long to retain that data? Do the guidelines reflect a preference for keeping data in private sector hands? Do the guidelines contain standards and procedures for when this preference is not followed?

**Question set 7**

Do government agencies that access private sector data on U.S. persons have clear guidelines—that are broadly consistent throughout the government—on when data collected for counterterrorism purposes may be used to carry out other missions? Do the guidelines disfavor dissemination for non-counterterrorism purposes, except when the agency or unit requesting such data would have been entitled to access the data directly with the same or fewer constraints?

**Question set 8**

Are there effective mechanisms in place to ensure compliance with the guidelines? Do these mechanisms include rigorous and consistent training on the guidelines, regular auditing and periodic review of compliance, and accountability for failure to comply? Is the approach to oversight consistent—although not necessarily uniform—throughout the government? Is a single agency or entity within the government responsible for ensuring this consistency?

**Question set 9**

Is the government deploying technology (such as anonymization, access control, and audit technologies) to further the goals of the guidelines? Is the government identifying gaps in existing technologies and those in development? And is it investing in research and development of needed new technologies to protect private sector data from misuse?

**Question set 10**

Is one government entity (such as the DHS or the OMB) auditing the use of private sector data across all agencies and providing an annual report to the appropriate committee(s) of Congress?

## Future work of the Task Force

---

The Task Force plans to continue its work on the challenges addressed in this report. The current term of the Task Force extends to the summer of 2004, but, given the urgency of the questions we are addressing, we chose to publish an interim report. We will continue to focus on areas that supplement the good work being done by many in the government and the private sector.

We plan to deepen our research on best practices in the government and on how existing technologies and those in development can be deployed to greatest effect. To that end, we hope to develop collaborations in which we pilot the use of technologies (such as information rights management technology, publish and subscribe software, and anonymization tools) to achieve distribution of information with strong civil liberties protections. We also plan to pursue additional work on guidelines regarding the use of private sector data and on new rules for collection and use of information on U.S. persons to replace the old “line at the border” between domestic and foreign intelligence. New rules and new dynamics between our nation’s security and our civil liberties need a great deal of additional work.

## Conclusion

---

Since September 11, many people in the government and the private sector have given considerable thought and effort to solving the problem of how our nation can use information and information technology more effectively to protect our nation while preserving civil liberties. As sources of relevant information continue to proliferate and technology continues to advance, this challenge will only grow more complicated. Our Task Force has sought to contribute to the solution by providing the framework for a national strategy and an architecture for a decentralized system of robust information sharing and analysis that makes the most effective possible use of information while instituting guidelines and technologies to minimize abuses and protect privacy.

## Additional papers

### Part Two: Working Group Analyses

Working Group I: Networking of Federal Government Agencies with State and Local Government and Private Sector Entities

Working Group II: Building an Effective, Sustainable Partnership Between the Government and the Private Sector

### Part Three: Appendices

#### Appendix A

Reliable Identification for Homeland Protection and Collateral Gains

This paper sets forth near-term recommendations for improving existing forms of identification and an agenda for longer-term research on creating more reliable means of identification while protecting civil liberties.

#### Appendix B

A Primer on Homeland Security Players and Information

Our primer offers a description of the roles, responsibilities, and authorities of the many different players who are part of the community we seek to bring together in the network, and of the reasons that information often is not shared as fully as it should be.

#### Appendix C

The Immune-System Model

In considering the issue of information flow among government agencies and, in particular, the problem of potentially flooding the system with too much information, we thought it would be useful to explore different models for how a system might work. One potential model is the human immune system, which is discussed in this paper.

#### Appendix D

Information Vignettes

Our vignettes describe different types of information that might come into the possession of various entities in the network of governmental and private sector actors. The scenarios allowed the Task Force to consider how such information would be handled today and how it should be analyzed and shared to maximize its utility and to

optimize the capabilities of all the players in the network.

#### Appendix E

The Four Key Questions of Detection and Prevention: Who? How? Where? and When?

This paper describes the four key questions the government must typically answer when trying to thwart an attack on the homeland: Who? How? Where? and When? The model offered in this paper, derived from the board game *Clue*, helped us to develop information strategies and identify some information technologies needed to meet the government's security challenge.

#### Appendix F

Technology Challenges for the Near Future

To understand better the kinds of privately held data that are needed to meet real security challenges, we developed a number of plausible scenarios that government officials might face. These scenarios helped the Task Force to consider what types of information are truly necessary; what technological capabilities the government needs to acquire in order to gain access to the information in a timely, useful way; and what potential civil liberties and other concerns must be addressed by policies governing the circumstances under which the information is acquired and used.

#### Appendix G

Technologies Required to Meet the Challenges

In "Technology Challenges for the Near Future" we describe 12 scenarios that we used to contemplate the technology and infrastructure issues that need to be addressed to improve national security. In this paper, we reduce the technology requirements to a finite number of specific capabilities. In Section 1, these capabilities are presented alphabetically to enable the reader to quickly look up the description, availability, and best-case time frame for implementation of each capability. In Section 2, we highlight the most critical capabilities.

#### Appendix H

The Landscape of Available Data

In this table, we present an overview of the data landscape that exists in the private sector. The overview includes data sources, the types of documents that are generated from those sources, the availability of the data, whether the data is personally identifiable, and what entities, if any, currently aggregate or have access to that data. The purpose of this table is to present insight into the types of data that often exist as a byproduct of our digital society.

## **Appendix I**

### **Government Requests for Private Sector Data: An Informal Survey**

The purpose of this survey was to get a sense of the kinds of private sector data the government currently seeks for national security purposes, how it seeks that data, and some of the issues the private sector has with government use of its data.

## **Appendix J**

### **Data Analytics Practices of the Private Sector**

In considering how the government could make better use of information technology for counterterrorism purposes, we looked into how the private sector uses data for identity verification, risk assessment, and related purposes. This paper is the result of consultations with representatives of various companies on the use of data analytics in the private sector.

## **Internet-only information**

### **Matrices of Laws Governing Access to Privately Held Data**

A broad array of laws covers how and in what circumstances the government or commercial companies can acquire and use various types of private sector data. We have developed two matrices in which we set forth those laws in an accessible fashion. These matrices can be seen on the Task Force's website at: [www.markletaskforce.org](http://www.markletaskforce.org)