Mobilizing Information to Prevent Terrorism

Accelerating Development of a Trusted Information Sharing Environment

Third Report of the Markle Foundation Task Force

ZOË BAIRD, JAMES BARKSDALE
CHAIRMEN

MARKLE FOUNDATION

MARKLE FOUNDATION

TASK FORCE ON NATIONAL SECURITY IN THE INFORMATION AGE

MEMBERS AND ASSOCIATES, 2006

Chairmen

Zoë Baird
Markle Foundation

Jim Barksdale
Barksdale Management Corporation

Members

Robert D. Atkinson
Information Technology and Innovation Foundation

Rand Beers
Coalition for American Leadership and Security

Eric Benhamou
3Com Corporation, Palm, Inc., Benhamou Global Ventures, LLC

Jerry Berman
Center for Democracy & Technology

Robert M. Bryant
National Insurance Crime Bureau

Ashton B. Carter
Kennedy School of Government, Harvard University

Wesley Clark
Wesley K. Clark & Associates

William P. Crowell
Security and Intelligence Consultant

Bryan Cunningham
Morgan & Cunningham LLC

Jim Dempsey
Center for Democracy & Technology

Mary DeRosa
Center for Strategic and International Studies

Sidney D. Drell
Stanford Linear Accelerator Center, Stanford University

Esther Dyson
CNET Networks

Amitai Etzioni
The George Washington University

Richard Falkenrath
The Brookings Institution

David J. Farber
Carnegie Mellon University

John Gage
Sun Microsystems, Inc.

John Gordon
United States Air Force, Retired

Slade Gorton
Preston Gates & Ellis LLP

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

Jeff Jonas
IBM

Arnold Kanter
The Scowcroft Group

Tara Lemmey
LENS Ventures

Gilman Louie
Alsop Louie Partners

John O. Marsh, Jr.
Marsh Institute for Government and Public Policy, Shenandoah University

Judith A. Miller
Bechtel Group, Inc.

James H. Morris
Carnegie Mellon University

Craig Mundie
Microsoft Corporation

Jeffrey H. Smith
Arnold & Porter LLP

Abraham D. Sofaer
Hoover Institution, Stanford University

James B. Steinberg
Lyndon Johnson School of Public Affairs, University of Texas at Austin

Kim Taipale
Center for Advanced Studies in Science and Technology Policy

Rick White
former Member of Congress

Richard Wilhelm
Booz Allen Hamilton

Associates

Bruce Berkowitz
Hoover Institution, Stanford University

Fred Cate
Indiana University School of Law Bloomington

Scott Charney
Microsoft Corporation

Bob Clerman
Mitretek Systems

David Gunter
Microsoft Corporation

Drew Ladner
JBoss, Inc.

Bill Neugent
MITRE

Daniel B. Prieto
Reform Institute

Clay Shirky
Writer and Consultant

Peter Swire
Moritz College of Law, The Ohio State University

Mel Taub
Independent Consultant

Markle Foundation Staff

Karen Byers
Managing Director and Chief Financial Officer

Kimberly Hogg
Assistant to the President

Danna Lindsay
Administrative Assistant

Michelle Maran
Manager, Public Affairs

Linda Millis
Director, National Security Program

Stefaan Verhulst
Chief of Research

Mobilizing Information to Prevent Terrorism

Accelerating Development of a Trusted Information Sharing Environment

THIRD REPORT OF THE MARKLE FOUNDATION TASK FORCE

July 2006

A Project of

The Markle Foundation
New York City

Copyright © 2006 Markle Foundation
All rights reserved.

Table of Contents

Overview

For four years, we have been privileged to chair the Markle Task Force on National Security in the Information Age. In its two previous reports, the Task Force has advocated the mobilization of information to prevent terrorism through the creation of a trusted information sharing environment. That environment enhances collaboration, and facilitates the flow of information across the federal government, state and local agencies, and the private sector to enhance understanding of the threats to our nation's security. It does so in a trusted manner, using information effectively and appropriately, and protecting civil liberties. This vision of a trusted network, along with the key attributes of our proposed Systemwide Homeland Analysis and Resource Exchange (SHARE) Network, outlined in our previous report, were enacted into law in the Intelligence Reform and Terrorism Prevention Act of 2004.

The Task Force has not been alone in issuing such recommendations. Concepts such as ours have been proposed by the Report of the Joint Inquiry into the Terrorist Attacks of September 11, 2001, the National Commission on Terrorist Attacks Upon the United States, the Commission on the Intelligence Capabilities Regarding Weapons of Mass Destruction, and many others. Yet despite general agreement on the need for enhanced information sharing to combat terrorism, the nation remains far from achieving this goal. Indeed, we are struck by the wide gap that persists between ambition and vision on the one hand, and actual achievement and concrete steps towards implementation on the other.

To be sure, the President and Congress have adopted the vision of information sharing, and have acted in a bipartisan way to remove barriers to achieve that vision. We have witnessed some genuine improvements in information sharing. But two years since the publication of our last report, and almost five years since the terrorist attacks of September 11, systematic, trusted information sharing remains more of an aspiration than a reality. The government has yet to articulate a credible implementation plan for a broad and trusted information sharing environment, and the sense of commitment and determination that characterized the government's response in the immediate aftermath of those attacks has significantly diminished. Furthermore, the crucial policy framework that would establish the legal and regulatory context for trusted information sharing is yet to be defined, much less implemented.

Our previous reports, like this one, have benefited tremendously from the combined cross-sectoral expertise of Task Force members and those we interviewed within the government. In bringing together individuals from government, the private sector, and civil society, we have been able to outline a framework for a virtual reengineering of how government manages information. This allows new procedures, methods and structures for collaboration without requiring the whole scale reinvention of government. Nevertheless, efforts to enhance information sharing have been bogged down by gaps in leadership, policy articulation, turf wars, and struggles over competing—and frequently incompatible—technologies. Indeed, our government seems to have lost its sense of the broader mission—of the need to establish the general policy framework that would facilitate information sharing in a trusted manner.

This report therefore reemphasizes that broad vision, and provides guidance to address the challenges of implementation: it discusses the policies, technologies, and government processes that are required. Throughout this third report, we call upon our political leaders to renew a sense of commitment and determination to foster greater collaboration and information sharing across government. We discuss some of the specific steps that can be taken by the legislative and executive branches. We emphasize the need for interagency and departmental trust and collaboration. Ultimately, the goal of enhanced information sharing to protect our nation will only be achievable if all major players—across federal, state, and local jurisdictions—work together.

This third report thus articulates the need for persistent action and, recognizing the magnitude of the task, provides a practical suite of tools to help the government move forward with the vital objective of thwarting terrorist attacks through the creation of a trusted information sharing environment.

As a nation, we must sustain our determination to reform our government to prevent another attack. The terrorist threat has not abated; better information sharing remains essential to our defense and national security. We recognize that there are significant cultural, technological, and institutional obstacles, but we must continue to do what is necessary to support trusted information sharing if we are to protect our nation's security and the values for which we stand.

Zoë Baird Jim Barksdale

Acknowledgements

The Markle Foundation Task Force on National Security in the Information Age was founded in the aftermath of the September 11 terrorist attacks. This distinguished, bipartisan group brings together some of the nation's foremost national security experts from the Administrations of Presidents Carter, Reagan, George H.W. Bush, Clinton, and George W. Bush, as well as leaders in the fields of technology and civil liberties.

For four years, through two published reports and numerous background papers, briefings, and meetings, the Task Force has focused on one essential goal: to help the nation use information wisely and effectively to ensure its security while fully respecting traditional civil liberties.

Some of the original members of the Task Force have been asked by President Bush to serve in his administration. These members include Health and Human Services Secretary Michael Leavitt; Philip Zelikow, who was the Executive Director of the National Commission on Terrorist Attacks Upon the United States (also known as the 9-11 Commission), and is currently Counselor of the State Department; and Stewart Baker, who was General Counsel of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (also known as the WMD Commission), and is now Assistant Secretary for Policy in the Department of Homeland Security. In addition, a number of experts have joined the Task Force after leaving government service, and others from the private sector have been added over the past four years.

We are grateful to all of the members of, and expert advisors to, the Task Force. Their sustained and selfless contributions reflect the finest traditions of public service, and have contributed to making our nation and our civil liberties more secure.

To facilitate the work by the Task Force, a Steering Committee and multiple working groups were formed. The members of the Task Force Steering Committee are: Zoë Baird, Jim Barksdale, Eric Benhamou, Bill Crowell, Bryan Cunningham, Jim Dempsey, Mary DeRosa, John Gage, John Gordon, Slade Gorton, Jeff Jonas, Tara Lemmey, Gilman Louie, Judy Miller, Jeff Smith, Abe Sofaer, Jim Steinberg, and Rick White. We express special thanks to our colleagues on the Steering Committee.

The working groups were:

- New Borders for Use of Information, with Jim Dempsey, Mary DeRosa and Gilman Louie, as reporters;

- Government Procurement, with Judy Miller, Abe Sofaer and Tara Lemmey as reporters;

- Government Programs, with Jim Dempsey, Mary DeRosa, Jim Steinberg, and Stefaan Verhulst as reporters;

- Visualizing the SHARE Network with Mary DeRosa and Tara Lemmey as reporters;
- Rethinking the Rules, with Slade Gorton as Chair and Bryan Cunningham as reporter; and
- Designing for Users, with Jim Steinberg as Chair, and Rand Beers and Rich Falkenrath as reporters.

These working groups provided a blueprint for this report, and introduced new solutions to the implementation challenges of establishing a trusted information sharing environment. Further, they led to the drafting of six monographs that collectively form the basis for many of this report's new recommendations:

- Governance and Oversight for Information Sharing Success (Mary DeRosa)
- Rethinking Classified Information: A Risk Management Approach (Mary DeRosa)
- Redrawing the Line at the Border: The U.S. Persons Barrier to Information Sharing (Jim Dempsey, Mary DeRosa, and Bryan Cunningham)
- Developing Human Capital for Sharing: Education, Training, and Tools (Rand Beers)
- Adoption of the SHARE Network by Senior Officials (Jim Steinberg and Richard Falkenrath)
- Using Audit Logs to Secure the Information Sharing Environment (Jeff Jonas and Peter Swire)

We owe a debt of gratitude to everyone who participated in the working groups and assisted in the drafting and review of the monographs, including Dan Prieto, who was the lead editor of the monographs, and especially to the individuals listed above who not only provided leadership but also participated in editing this third Task Force report.

The preparation of this report has been aided by many people. Fred H. Cate, Distinguished Professor and Director of the Center for Applied Cybersecurity Research at Indiana University, was the reporter. In particular, the report would not have been possible without the relentless efforts, commitment, and cooperation offered by a core team of reviewers and editors comprising Bryan Cunningham, Bill Crowell, Jim Dempsey, Mary DeRosa, Jeff Jonas, and Kim Taipale. Tara Lemmey and Lens Ventures, prepared visualizations of concepts described in the report. Akash Kapur proofread the final product.

Many members of the Markle Foundation leadership and staff lent their talents and energy to this most recent work of the Task Force. In particular, Stefaan Verhulst provided extensive research and drafting assistance. Karen Byers oversaw the financial management. And the project was managed and overseen by Linda Millis.

Finally, we would also like to thank all those government officials who took time from their busy schedules to meet with Task Force members and associate members. They informed this report by candidly sharing their views and explaining the challenges they face.

On behalf of the Task Force, we express our gratitude to all of these individuals for their commitment and hard work.

Zoë Baird Jim Barksdale

Executive Summary

The terrorist attacks of September 11 provided one unmistakable lesson: to protect the United States against today's threats, it is essential that the right people have the right information at the right time. That is why the focus of the Task Force is and always has been on how best to mobilize information and information technology to improve national security while protecting civil liberties.

The goal is not just better or more information sharing. In our earlier reports, we envisaged a trusted environment that fosters sharing and collaboration among those with information useful to understand potential terrorist threats; where policies and technologies are developed in tandem; and where security is enhanced and civil liberties are protected.

> "To succeed the system must have the confidence of the American people it serves, while the analysts and operatives involved must feel confident that they know what they are expected and allowed to do, and that their work is lawful and appropriate."
>
> *Protecting America's Freedom in the Information Age*, First Report of the Markle Foundation Task Force, October 2002

The President, Congress, various agencies, state and local officials, and others have begun to develop such an environment. Several of our earlier recommendations have been enacted through laws, Executive Orders, and other steps. Today, information flows more efficiently, and far more information is being shared than just a few years ago.

Yet despite this progress, many projects and initiatives have been delayed because key organizations have not yet internalized these changes, and because many still cling to previous ways of doing business. Clear government-wide guidelines for the careful handling of personally-identifiable information have not been promulgated. Information sharing efforts have been stalled by turf wars and unclear lines of authority and control. Funding has sometimes been insufficient. Too many efforts are still focused on classified information from within the intelligence community, and not enough on all relevant information, whatever its origin, that might help prevent the next attack. Better cooperation between federal, state, and local agencies needs renewed attention. For these and other reasons, we are concerned that relevant information is still not being mobilized as fully as required to protect our nation's security.

This situation is perhaps no surprise, given the scope and complexity of transformation required. Full implementation of a trusted information sharing environment requires sustained leadership, commitment, and determination; renewed cooperation between agencies; constant evaluation and assessment; and, when necessary, the introduction and adoption of new ideas and approaches.

This third Task Force report thus calls for a renewed commitment by our nation's leaders to the development of an information sharing environment. It builds on the principles set out in our

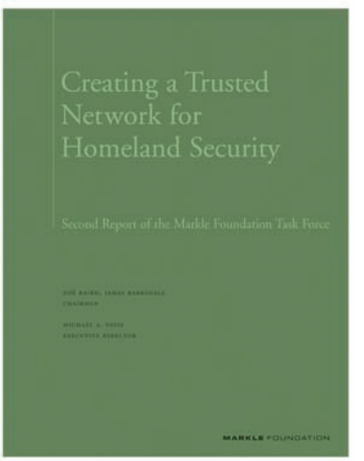
previous reports, and introduces new concepts and new solutions that can help address some of the lingering implementation challenges.

SUMMARY OF NEW CONCEPTS

To move forward effectively, the Task Force believes that the government must implement policies to overcome the significant cultural and bureaucratic hurdles that impede sharing. These recommendations include:

- adopting an authorized use standard to protect civil liberties in the sharing and accessing of information the government has lawfully collected; this standard would replace existing outdated standards based on nationality and place of collection;
- taking a "risk management" approach to classified information that better balances the risks of disclosure with the risks of failing to share information;
- creating a government-wide dispute resolution mechanism to facilitate responsible, consistent, and lawful information sharing;
- developing tools, training, and procedures to enhance senior officials' use of the information sharing environment and its technological capabilities;
- expanding community-wide training, modern analytic methods, and new tools to enhance the quality of information sharing and analysis;
- encouraging the use of new technologies such as anonymization, and the use of expert and data directories;
- employing immutable audit systems to facilitate both accountability and better coordination of analytical activities; and
- creating an Information Sharing Institute.

Our previous two reports outlined a vision of a trusted information sharing environment in which information could be used effectively and appropriately throughout government and the private sector to enhance national security while protecting civil liberties. The use of such information must be subject to



clear rules and guidelines which empower and constrain government officials and protect civil liberties. When we speak of trust, we mean three things:

- trust among users that the information sharing environment serves their mission, protects classified sources, and does not expose them to inappropriate legal risk;

- trust among policymakers that the laws and rules governing the information sharing environment are being implemented, followed, and enforced in good faith; and

- trust among the public that the information sharing environment and the information collection and sharing it facilitates are: necessary to protect national security, conducted according to clear laws and rules, subject to meaningful oversight and enforcement, and consistent with traditional civil liberties values.

This trusted information sharing environment would give participants, policymakers, and the public confidence that information will be shared fully and protected appropriately.

Furthermore, to broaden consensus and engender widespread support for mobilizing information to defeat terrorism, goals we recommended in our prior reports, we urge our government to engage in a public debate—to the extent possible while maintaining national security—about the guidelines and rules that govern information sharing. This debate should also seek to clarify agency missions, and address the requisite civil liberties and privacy protections.

> "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."
>
> *Creating a Trusted Information Network for Homeland Security*, Second Report of the Markle Foundation Task Force, December 2003

To continue making progress towards establishing a trusted information sharing environment, we propose an approach that includes:

- sustained leadership and strong oversight from all branches of government;

- clear policies, processes, and guidelines that facilitate collaboration and sharing of information while protecting civil liberties; and

- technologies that facilitate sharing while protecting security and privacy.

Leadership and the Integration of Policy and Technology to Guide Implementation and Use

Leadership from the President to Steer Cross-Agency Implementation, Facilitate Transformational Change, and Establish Public Confidence

Only presidential authority and sustained leadership can ensure implementation of a national framework for a trusted information sharing environment. In August 2004, the President issued a series of Executive Orders calling for improved sharing of terrorist-related information throughout the government. The Office of Management and Budget took the lead, and implementation was aggressive. Later that year, the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) created the Office of the Director of National Intelligence (ODNI) and called for the development of an information sharing environment under the direction of the Program Manager (PM) for Information Sharing, who would be accountable to the President. Many of the key elements and attributes described in earlier Markle reports were included in the IRTPA. The President subsequently assigned the PM to the ODNI (for an overview of developments, see Appendix 1). With the shift in responsibility to a new office, and confusion over whether the efforts were now to extend beyond the intelligence community, implementation efforts slowed. Presidential authority is needed to reinvigorate these efforts and instill a renewed sense of commitment to establishing the information sharing environment throughout government.

Thus, we recommend that the President develop and issue a specific implementation plan that outlines comprehensively the critical elements (people, authorities, processes, and resources) necessary for further development of an effective and trusted information sharing environment. This environment should foster sharing not just among existing members of the federal intelligence community, but more broadly among other federal, state, local, international, and private sector organizations**.** It should highlight the importance of establishing trust among participants, as well as with the public.

In particular, we recommend that the President:

- further define and articulate the need for a trusted information sharing environment, and take steps to prevent departments and agencies from using a purported lack of clarity in recent laws and Executive Orders to mask refusals to share information appropriately;

- issue guidelines and identify ways to overcome institutional resistance and barriers to information sharing among the disparate federal agencies with intelligence responsibilities, as well as among other federal, state, local, international, and private sector organizations;

- work with the Congress to ensure adequate funding for information sharing initiatives;

- hold the Director of National Intelligence (DNI) accountable for creating and implementing the plan and other tasks necessary to facilitate trusted information sharing. If the DNI is to be limited to addressing his efforts to the intelligence community, the National Security and

Homeland Security Councils could be called upon to extend the effort to other relevant participants;

- issue guidelines that rigorously protect privacy and civil liberties; and

- task the Privacy and Civil Liberties Oversight Board and the President's Foreign Intelligence Advisory Board's Intelligence Oversight Board to be actively engaged in the development and implementation of the information sharing environment in order to ensure greater confidence among the public that privacy and civil liberties concerns are being overseen.

Leadership from Congress to Oversee Effective Implementation

Leadership is also required by Congress. We recommend that Congress:

- exercise fully and appropriately its oversight responsibilities to ensure information sharing activities and include all necessary participants, not just the intelligence and federal communities;

- provide adequate funding; and

- develop appropriate methods of appraising progress on information sharing and consider greater use of investigative staff or the Government Accountability Office**.**

State and Local Leadership

Leadership is also required by state and local governments. We recommend that governors, mayors, regional authorities, and special district entities:

- develop appropriate methods of appraising progress on information sharing among regional, state, and local authorities;

- develop coordinated regional training and deployment exercises to coordinate sharing activities;

- develop standardized mechanisms for information sharing in coordination with Executive Branch agencies, in particular by implementing mechanisms for transactional access to emergency information; and

- develop unified, top-to-bottom mechanisms for authorized use of information, and unify dispute resolution mechanisms across jurisdictions.

Policies, Processes, and Guidelines that Facilitate Information Sharing and Provide Trust by Empowering and Constraining Users

> "An information network will not be sustainable if the government does not build public trust by embedding protection for well-established civil liberties. Only with guidelines and attendant public discussion can the government hope to engender and maintain the trust of the people in its efforts."
>
> "*Creating a Trusted Information Network for Homeland Security*," Second Report of the Markle Foundation Task Force, December 2003

In earlier reports, we called for appropriate government-wide information sharing guidelines and policies to be drafted and adopted in tandem with the introduction of new technologies and systems so that information sharing and the use of technology met policy objectives. Although some guidelines have been incorporated or called for in recent Executive Orders, no clear process exists for getting government-wide guidelines written, approved or enacted. At the same time, new technical applications continue to be introduced without appropriate polices and guidelines in place. We therefore reiterate our recommendation that the President (and, by extension, that of his appointed leadership and Congress) place a high priority on the establishment of a clear process for the development and adoption of government-wide guidelines for effective information sharing, dispute resolution, oversight, and protection of civil liberties.

A New Authorized Use Standard

The Task Force believes that the government should develop new mechanisms and rules to protect privacy and civil liberties in the sharing of private information. Current rules, based primarily on nationality and place of collection, have generated confusion and in some cases produced a rigidity that impedes desirable information sharing. The new regime must be coherent and consistent to ensure that relevant information is handled in a more efficient, appropriate, and secure manner.

In particular, we recommend the development of an authorized use standard for sharing and accessing information lawfully collected by, or available to, the United States government. Authorized uses are mission- or threat-based permissions to access or share information for a particular purpose that the government, through appropriate process, has determined beforehand to be lawfully permissible for a particular employee, component, or agency.

Our new approach has two requirements: clarity of authorized uses—which requires careful consideration of appropriate roles and missions of agencies and offices—and careful monitoring and oversight of the actual uses of information. In the past, the U.S. Persons rule, which largely determined conditions of access to or sharing of information, was viewed by many as a necessary proxy for rules on mission and use. In other words, many believed that denying some agencies – particularly in the intelligence community – access to or sharing of U.S. Persons information was the

most effective check on those agencies, preventing them from using such information to exceed their operational authorities. We believe that our approach safeguards these same interests, but does so more directly, efficiently, and effectively by permitting access for authorized uses while utilizing technological and other means to monitor usage and identify potential abuses.

The Task Force believes it is also important to reduce inappropriate risk aversion to information sharing, in part by providing confidence to participants in the information sharing environment that authorized uses will not subsequently result in unwarranted investigations or damage to careers if rules are later updated or reinterpreted. We therefore recommend the creation of a carefully considered safe-harbor mechanism to supplement the authorized use procedures.

Such a mechanism would provide confidence to career intelligence, law enforcement, military, and homeland security officials that, so long as authorized use principles were followed and there was no indication of bad faith, no punitive action would be taken against an individual government officer for having accessed or shared information.

We do not recommend that such a mechanism be extended to shield politically accountable government officials who make the rules and direct new policies from political or, if warranted, legal accountability. Rather, if a safe-harbor mechanism is adopted to supplement the authorized use standard, such a mechanism would benefit those career officers on the front lines of our national and homeland security who daily carry out the rules made by others.

A Process to Resolve Disputes over Information Sharing

No matter how clear and consistent the guidelines are for information sharing, disputes will inevitably occur. To resolve these disputes, we recommend the creation of a government-wide dispute resolution process that it is efficient, timely, and easy to use.

Managing the Risks of Sharing and Not Sharing

Current classification procedures and practices are frequently a barrier to effective information sharing because they overemphasize the risks of inadvertent disclosure over those from failing to share. These practices are designed almost exclusively to protect against inadvertent disclosure and do not address the risks to security from failing to share relevant information.

We recommend a new risk management approach to handling classified and other sensitive information that gives adequate weight to the risks of not sharing, and provides greater flexibility and more emphasis on mitigating the risks of disclosure. This requires an information architecture that emphasizes *pull* technology, which permits participants to locate and access information they need, over *push* technology, which distributes information broadly, whether recipients need it or not.

Improving the Decision-Making Processes of Senior Officials

To support senior officials in policymaking and decision-making, the information sharing environment should be designed to take into account the particular needs and practical constraints

of senior decision-makers. The Task Force recommends that the information sharing environment:

- facilitate a more robust two-way exchange between analysts and decision-makers, both for tasking and for analysis;
- provide decision-makers with a more nuanced understanding of the strengths and weaknesses of the information underlying finished analysis;
- include divergent perspectives; and
- reduce policymakers' dependence on stovepiped intelligence units within their own organizations.

Developing Adequate Training and Education to Improve Information Sharing Expertise

Ensuring compliance with guidelines through adequate training and education of participants is vital to engendering user and public trust. Therefore, we recommend that significant attention be paid to human capital in the information sharing environment by expanding community-wide training on a common set of skills, best practices, and the rules and guidelines applicable to information sharing.

Creating an Information Sharing Institute

Government and its contractors cannot provide all the expertise and capabilities required to address the various challenges associated with the information sharing environment. We therefore recommend the creation of an Information Sharing Institute that could make needed operational and professional expertise available when necessary beyond that which is available in the government in any particular agency, department or government contractor. This Institute would provide a mechanism to identify and distribute best practices, and to apply technologies available in other sectors. It should have the full and active participation of organizations from federal, state, and local governments as well as the private sector. In addition, it could help promote coordination of the necessary investment in research and development for new technologies needed to create a trusted information sharing environment.

Technologies that Support Policies and Processes to Connect People and Information

Developing a trusted information sharing environment requires designing and implementing a technical infrastructure, and employing technologies with features that support policy goals. Overall architecture, technical applications, and features must provide opportunities for rules-based operation of systems in which the technology itself serves an important function to both enable appropriate, and constrain inappropriate, information sharing. In this sense, technology is an important enabler of trust: it provides assurance to participants, policymakers, and the public that information sharing conforms to governing policy.

Technology can be employed:

- to improve the effectiveness of information sharing and analysis;
- to enhance the security of systems and shared information; and
- to enforce privacy protections and provide accountability.

This report is not intended to be an exhaustive discussion of specific technology developments, current research, or implementation activities. Rather, it provides a brief overview of certain available technologies that have particular applicability to implementing a trusted information sharing environment.

Conclusion

The need to mobilize information to prevent terrorism became apparent with the September 11 attacks. The terrorist threat and the need for knowledge about it have not abated. Significant progress has been made towards effective information sharing among federal agencies through the enactment of new legal authority and promulgation of Executive Orders, and the actions of some agencies. Implementation of these directives, however, has been slow and is not yet happening according to a government-wide plan. Agencies are creating programs to collect information without attention to how that information can be used appropriately in an information sharing environment. Sharing with state and local authorities and with the private sector is even further behind. This lack of sharing represents an ongoing threat to national security. It should therefore be considered an urgent national priority to make information sharing a reality—not just among intelligence agencies, but throughout the government, and with foreign governments and the private sector as well.

Trust among participants, policymakers and the public is crucial to the success of an effective information sharing environment. Each must have confidence that information will be collected and handled in a way that both enhances national security and protects civil liberties. Building that confidence requires strong leadership, clear laws and guidelines, and advanced technologies.

Mobilizing Information to Prevent Terrorism while Protecting Civil Liberties

This third report from the Markle Foundation Task Force on National Security in the Information Age reiterates many of our previous recommendations, and introduces new concepts facilitating the implementation of a trusted information sharing environment that mobilizes information to prevent terrorist attacks while protecting civil liberties.

Developing an extended information sharing environment among federal, state, local, and private sector entities that is both effective and accountable poses significant challenges for existing government structures, policies, technologies, cultures, and leaders.

This report addresses some of those challenges to further assist the government in overcoming some of the barriers to collaboration and information sharing. It calls on the President and Congress to exercise sustained leadership; to clarify the missions of agencies that collect, analyze, and share information; to develop guidelines that protect privacy and civil liberties; to foster public debate about these critical issues; and to hold accountable those charged with getting the job done.[1]

Ensuring that the right people have the right information at the right time is essential to protecting national security and preventing future terrorist attacks against the United States. This is the unmistakable lesson drawn from the terrorist attacks of September 11th, and it has been highlighted by all post-September 11 inquiries and commissions.[2] However, nearly five years after those attacks, and 18 months after the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), the effort to create a widely available, flexible, and accountable information sharing environment[3] that protects civil liberties is losing focus and momentum. Purported implementation barriers, many of which may actually be more indicative of a reluctance to change than legal or capacity limitations, have stalled progress, and in some cases chilled collaboration.

As we discussed in our previous reports, the challenge is broader than just collecting and sharing information. The challenge we face is one of using information effectively, linking collection with sound and imaginative analysis derived from multiple perspectives, and employing cutting-edge technology to support end-users, from emergency responders to the President, while protecting civil liberties and other important values.

---

[1] This report, unlike some sections of our prior reports, does not specifically address the standards for collection of intelligence. Rather, it focuses on how legally collected information already in the hands of the government can be used in an information sharing environment.

[2] These include the Joint Inquiry by the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence, the 9/11 Commission, and the WMD Commission.

[3] The IRTPA calls for the creation of a national Information Sharing Environment (ISE) with the attributes proposed in our earlier reports. Because we have gone into additional detail and in the interests of consistency and readability, this report will not capitalize the phrase "information sharing environment," whether referring to our recommendations or to those of the IRTPA.

During the past four years, the Markle Task Force on National Security in the Information Age has promoted the mobilization of information to protect national security and prevent terrorism through the creation of a trusted information sharing environment in which participants, policymakers, and the public can have confidence that information is used effectively and appropriately, and civil liberties are protected. In our two prior reports, we articulated the need for trusted information sharing, the key attributes of that sharing, and the essential tools for ensuring accountability and building trust. In the two and a half years since publication of our last report, we have witnessed many efforts intended to further this mission. However, we have become increasingly concerned that the initial focus and momentum have dissipated, and that not enough has yet been accomplished to truly mobilize information effectively while protecting civil liberties.

While the President has initiated a number of information sharing programs through Executive Orders and memoranda, and Congress has acted to remove the legal barriers to information sharing,[4] a comprehensive, trusted environment capable of marshalling information from across the federal government, state and local agencies, and private industry has still not emerged. (See Appendix 1 for an overview of developments towards establishing an information sharing environment).

The existing federal effort remains too focused on intelligence information, rather than on the full range of information necessary to detect and prevent terrorist activity. In addition, it remains too concerned with sources and users of information in the federal government, and not sufficiently with information available in state and local agencies, and the private sector. For example, the National Counterterrorism Center (NCTC) has been identified as the primary organization in the U.S. government responsible for analyzing and integrating all counterterrorism analysis. Yet the NCTC continues to focus primarily on classified intelligence information and has not fully incorporated other information sources or users. Earlier this year, the Government Accountability Office (GAO) opined that "[n]o government-wide policies or processes have been established by the Executive Branch to date to define how to integrate and manage the sharing of terrorism-related information across all levels of government and the private sector."[5] The Task Force is particularly concerned about this continuing gap.

In addition, the GAO found 56 different designations for Sensitive But Unclassified information alone, reflecting a variety of conflicting and inconsistent definitions that interfere with information sharing.[6] As a result, the GAO asserted, "information about terrorists, their plans, and their activities is fragmentary."[7]

---

[4] See, for example Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in various sections of U.S.C.); Homeland Security Act, Pub. L. No. 107-296, 116 Stat. 2135 (codified as amended in various sections of U.S.C.); and Intelligence Reform and Terrorism Prevention Act, Pub. L. No. 107-296, 116 Stat. 2135 (codified as amended in various sections of U.S.C.). These and other developments are described in greater detail in Appendix 1.

[5] U.S. Government Accountability Office, *Information Sharing*, GAO-06-385 (2006), at 14.

[6] Id. at 21. The GAO found that "there are at least 13 agencies that use the designation For Official Use Only, but there are at least five definitions of FOUO. At least seven agencies or agency components use the term Law Enforcement Sensitive . . . . [but] gave different definitions for the term." Id. at 24.

[7] Id. at 17.

At the same time, we are concerned that ad hoc, unfocused sharing is occurring, with attendant risks to civil liberties and less than optimal benefit to national security. Transfers of large databases or indiscriminate reporting of unverified information, without regard to the information quality, reliability or usefulness, or without considering the receiving agency's ability to analyze the information, is not the effective information sharing environment we envision.

State and local governments have not become full participants in the information sharing environment. Many feel they are still not getting the information they need, and that there is no effective process for sharing their information with the federal government. A 2006 National Governors Association survey of state Homeland Security Directors found that "[s]ixty percent of responding state Homeland Security Directors are dissatisfied or somewhat dissatisfied with the specificity of the intelligence they receive from the federal government. An additional 55 percent are dissatisfied or somewhat dissatisfied with the actionable quality of the intelligence they receive from the federal government."[8] These numbers represent a sharp increase from 2005, when 39 percent of respondents criticized the specific nature of federal intelligence and 20 percent faulted its actionable nature.[9]

Numbers like these make evident why a detailed and practical plan for building a broad and trusted information sharing environment is urgently needed. Despite universal agreement about the importance of trusted information sharing, almost five years after the September 11 attacks, and 18 months after the IRTPA, the government is still issuing "Preliminary" reports and "Interim" implementation plans.

In this third report, the Task Force therefore urges the government to move forward aggressively to implement a robust information sharing environment that encompasses all of the required participants and includes policies, architectures, and technical features for ensuring trust. Users must trust that the information sharing environment serves their mission, protects classified sources, and does not expose them to legal risk. Officials in all branches of government must trust that the laws and rules governing the information sharing environment are being implemented, followed, and enforced in good faith. And the public must trust that the information sharing environment protects national security; is conducted according to clear laws and rules; is subject to meaningful oversight and enforcement; and is consistent with core civil liberties values.

This report includes a number of specific and detailed recommendations that offer new approaches to the persistent implementation challenges we have witnessed since our first report. These recommendations, taken together, reflect a substantial departure from traditional federal government practices. To move forward effectively, the Task Force believes that the government must implement policies to overcome the significant cultural and bureaucratic hurdles that impede sharing. These recommendations include:

[8] NGA Center for Best Practices, *2006 State Homeland Security Directors Survey: New Challenges, Changing Relationships* 6 *(*April 3, 2006).

[9] Id.

- adopting a new, more workable authorized use mechanism to protect privacy and civil liberties when accessing and sharing personally-identifiable information that the government has collected lawfully; this mechanism would replace the existing U.S. persons and place of collection standards, which have become increasingly ineffective;

- taking a "risk management" approach to classified information that better balances the risks of disclosure with the risks of failing to share information;

- creating a government-wide dispute resolution mechanism to facilitate responsible, consistent, and lawful information sharing;

- developing tools, training, and procedures to enhance senior officials' use of the information sharing environment and its technological capabilities;

- expanding community-wide training, modern analytic methods, and new tools to enhance the quality of information sharing and analysis;

- encouraging the use of new technologies such as anonymization, and the use of expert and data directories;

- employing immutable audit systems to facilitate both accountability and better coordination of analytical activities; and

- creating an Information Sharing Institute.

These concepts respond to some of the significant policy barriers and other disincentives to robust, distributed information sharing. The fear of wrongful disclosure and the search for perfect security continue to drive decisions about the sharing and handling of classified information, posing some of the most significant hurdles to better information sharing. The government must rethink its approach to calculating and managing the risks involved with sharing sensitive security information, and it must adopt more flexibility in mitigating those risks.

Our recommendations are intended, to the greatest extent possible, to be implemented together. The new authorized use standard will allow for greater trust between agencies when accessing and sharing information, since the reasons for sharing will be known and disclosed to participants. Adoption of the authorized use standard must be accompanied by the deployment of robust audit log, monitoring technologies, and policies to ensure that actual use is consistent with authorized use. Likewise, an efficient and effective governance and dispute resolution mechanism, along with immutable audit capabilities, will ensure that the new standards are being used consistently and conform to governing laws, rules, and policies.

ATTRIBUTES OF AN INFORMATION SHARING ENVIRONMENT

In the second report, *Creating a Trusted Information Network for Homeland Security*, published in December 2003, the Task Force articulated its concept of a Systemwide Homeland Analysis and Resource Exchange (SHARE) Network. According to the report, the network would protect national security by "fostering a robust sharing of information and ideas."[10] It would focus on eliminating the gaps between government agencies, "get[ting] information into the hands of people who could analyze and act on it," and "leverage[ing] information from private holders within a system of rules and guidelines."[11]

The Task Force wrote that "[a]ll players in this network—including those at the edges—would be able to create and share actionable and relevant information."[12] The objective was an ambitious but critical one: "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."[13]

To achieve these objectives, we articulated a number of attributes of a successful information sharing environment. The network should:

- be developed incrementally and be scalable, so that it can operate nationwide;
- be implemented in a distributed, decentralized, peer-to-peer environment, so that information flows do not depend on a central information broker;
- not be Washington-centric;
- not be limited to intelligence data, but rather to recognize that most relevant information may come from other sources;
- keep data with the original data owners to the greatest extent possible, which also simplifies the task of keeping the data current across the network;
- feature rich directory-based services that allow rapid identification of all information relating to people, organizations, locations, time, and methods;
- meet the needs of users for real-time discovery, dissemination, collaboration, and communication;

[10] Markle Foundation Task Force on National Security in the Information Age, *Creating a Trusted Information Network for Homeland Security* 8 (2003).

[11] Id.

[12] Id.

[13] Id.

- be resilient and support redundant or complementary analyses and communication pathways in multiple locations;

- be secure and accountable to protect data, limit access to authorized users for authorized uses, and feature advanced technologies such as automated audit and policy enforcement to support civil liberties protection.

RECENT ELECTRONIC SURVEILLANCE ACTIVITY

The Task Force takes no position on the legality of any of the intelligence collection activities that have been the subject of recent public disclosures and debate. Instead, our work has focused on the sharing of lawfully-collected information and on rules for collection enabled by advances in information technology. However, the Task Force believes that intelligence activities and information sharing are most likely to be successful on a sustained basis when they operate within a consensus framework that has been developed, to the greatest extent consistent with the protection of our national security, through public debate. The details of operations, and the practical application of rules, will of course need to be secret. But intra-governmental and public confidence that articulated rules are being followed must be restored through a publicly-established framework agreed upon by the Executive Branch and Congress.

The Importance of Maintaining Trust and Sustaining Determination towards Transformation

> "To succeed the system must have the confidence of the American people it serves, while the analysts and operatives involved must feel confident that they know what they are expected and allowed to do, and that their work is lawful and appropriate."
>
> *Protecting America's Freedom in the Information Age*, First Report of the Markle Foundation Task Force, October 2002

The Task Force emphasized throughout both of our prior reports that effective information sharing was dependent on developing a trusted information sharing environment.

Trust in this context is a complex concept. It requires that policy and technology be developed and implemented in ways that ensure confidence among disparate communities that systems will function within guidelines, and according to known and agreed-upon rules. When such confidence is lacking, the consequences can be devastating, undermining both system effectiveness and the public support necessary to achieve success.

Thus, trust or confidence must be maintained at several levels. To begin with, providers and users of information must have confidence in the system. If providers do not believe that the information will be used and protected appropriately, they will not contribute to the network. If users do not believe that the information is reliable and comprehensive, or that they can gain access to deeper levels of information if circumstances warrant, they will implement their own collection systems and may keep the information to themselves. The concerns of the private sector, which faces legal liability and popular outcry when it shares personally-identifiable information in violation of consumer expectations, also inhibit the sharing of information with the government. As the Task Force wrote in our second report: "Without trust, no one will share."[14]

Trust is equally important among federal, state, and local governments. As the Task Force has emphasized, state and local governments are critical to homeland security. They have more resources, they interact more frequently with the public, and they are often in a better position than the federal government to provide and act on useful information. As the Task Force has written: "Seen from New York, or Texas, or Utah, or California, the homeland security picture is very different. Those officials think *they* are the ones who really manage homeland security. They have a point."[15] Ensuring the confidence of non-federal officials in the information sharing environment is therefore critical if they are to supply information to the envisaged network and act based on information from it. Conversely, federal officials must have confidence both in the quality and

[14] *Creating a Trusted Information Network for Homeland Security*, supra at 18.

[15] *Protecting America's Freedom in the Information Age*, supra at 11.

integrity of information shared by state and local governments, and that information provided to non-federal officials will be safeguarded and used appropriately.

This same need is reflected in the relationship between the U.S. government and other national governments. The information critical to preventing terrorism will come not only from the United States but from other nations as well. Mutual trust between national governments is therefore essential to fostering the necessary sharing of sensitive information. If other nations doubt that such information is shared or used appropriately in the United States, they will be understandably reluctant to provide it.

Trust is also essential between branches of government. Congress must believe that our Constitution and laws are being followed, and that it is being kept informed, or it will attempt to impose more restrictive provisions. The Executive must have confidence that other branches of government will respond appropriately to national needs and will not leak the classified information it shares with them, or act for partisan political purposes. The judiciary must be able to rely on the fact that the information provided to it is accurate, and that its decisions are being followed.

Finally, the public must trust that information sharing is effective, appropriate, and legal. Lack of public confidence that systems are functioning within clearly established guidelines can lead to the termination of essential government initiatives. For example, the Department of Defense's (DoD) Terrorist Information Awareness program,[16] the Transportation Security Administration's CAPPS II system,[17] and the Multistate Anti-Terrorism Information Exchange (MATRIX)[18] were all abandoned or significantly curtailed in the face of congressional opposition and public controversy about the impact on privacy.

As we pointed out in prior reports, whether or not the retreat from these specific programs was justified, they collectively demonstrate the power of public controversy to block the development or deployment of information systems designed to enhance security. In the absence of public confidence that personal information is being used effectively, appropriately, and consistently with both applicable laws and shared expectations of privacy, the necessary public support will not be forthcoming, and even the most promising intelligence systems will fail. As we emphasized in our second report: "The trust of the people…is vital to implementing the network we envision" and "an information network would not be sustainable if the government does not build public trust."[19]

---

[16] Department of Defense Appropriations Act, 2004, Pub. L. No. 108-84, § 8183 (Sept. 25, 2003).

[17] Privacy Act; System of Records, 68 Federal Register 45265 (2003) (DHS, TSA) (interim final notice); U.S. General Accounting Office, *Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges*, GAO-04-385 (2004).

[18] Thomas C. Greene, "A Back Door to Poindexter's Orwellian Dream," *The Register* (Sept. 24, 2003); Robert O'Harrow, Jr., "U.S. Backs Florida's New Counterterrorism Database," *Washington Post* (Aug. 6, 2003) at A1; Chris Maag, "The Matrix: An Expensive Government Program Was Doomed from the Start," *Cleveland Scene* (Ohio), (March 9, 2005); and "Too Much Information" (editorial), *St. Petersburg Times* (Florida) (May 10, 2005) at 8a.

[19] *Creating a Trusted Information Network for Homeland Security*, supra at 4.

Leadership and the Integration of Policy and Technology to Guide Implementation and Use

To continue making progress towards establishing a trusted information sharing environment, we make recommendations in three general – yet critically important – areas. We call for:

- persistent leadership and strong oversight from all branches of government;
- clear policies, processes, and guidelines that facilitate collaboration and sharing of information while protecting civil liberties; and
- technologies that facilitate sharing while providing security and privacy.

In our previous reports, we have suggested various principles and potential paths to achieve these goals. Some of these are reiterated below. At the same time, we provide a number of new and specific recommendations, building upon the foundations set out in earlier reports.

Persistent Leadership and Strong Oversight from all Branches of Government

Implementing a trusted information sharing environment requires leadership, collaboration, and commitment from the three branches of government (the President and his administration, Congress, and the courts) as well as state and local officials.

Leadership from the President to Steer Cross-Agency Implementation, Facilitate Transformational Change, and Establish Public Confidence

> "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 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."
>
> *Creating a Trusted Information Network for Homeland Security*, Second Report of the Markle Foundation Task Force, December 2003

Presidential authority and sustained leadership is critical to building an effective and reliable trusted information sharing environment, and in overcoming obstacles to effective information sharing. Much of this work has begun through Executive Orders mandating increased information sharing,

the implementation of the IRTPA, and the staffing of the Privacy and Civil Liberties Oversight Board.

Ensure security by accomplishing the mission and vision
The President should ensure that the vision and mission outlined in the IRPTA and the Executive Orders on the information sharing environment are executed in the manner and timelines described. He should restate and clarify his determination to create an information sharing environment that mobilizes all relevant information to prevent terrorism. To date, the Director of National Intelligence (DNI) appears to have taken a narrow view of the information sharing environment, focusing too much on information sharing within the intelligence community. We recognize this is a complex process, but it may be time to evaluate progress and introduce new ideas to move towards effective implementation.

Concerns persist about the effectiveness of the Office of the DNI (ODNI) structure; the perceived weakening of the Central Intelligence Agency (CIA); the continuing challenges faced by the Federal Bureau of Investigation (FBI) in structuring its intelligence functions and information technology systems; and the difficulties coordinating the diverse activities of the Department of Homeland Security (DHS), and the tension between its national security and other undertakings. In addition, and partly as a response to these concerns, there have been calls for the creation of a domestic intelligence agency. These concerns contribute to the need for renewed attention to the information sharing environment.

Ensure security with liberty
The President should ensure that we protect privacy and civil liberties as we achieve security. Security and liberty are dual core obligations and goals, not competing rivals.

Ensure responsive implementation through the Director of National Intelligence
The President should hold the DNI accountable for his government-wide responsibilities, not just information sharing within the intelligence community. Alternatively, if the DNI efforts are to be limited to the intelligence community, the National Security and Homeland Security Councils should be called upon to extend the effort to other critical agencies, state and local entities, and the private sector. The President should require the DNI to report regularly to him, to Congress, and, as appropriate, to the public about progress in implementing the information sharing environment and in enhancing responsible government-wide information sharing. The President should understand that his daily briefing by the DNI will only provide a strong insight into the threats to the nation if the information sharing environment is strong.

Eliminating resistance to change
The President should take responsibility for eliminating the resistance to change that may be keeping some departments and agencies from improving information sharing.

Lead the national debate
Our system of government works best when all three branches of government work together towards common goals. The President should therefore help foster the much-needed public

discussion about the proper protection for privacy and individual freedom in the context of national security.

Leadership from Congress to Oversee Effective Implementation

Leadership is also needed from Congress. Congress should exercise diligent and non-partisan oversight of the information sharing environment's creation. In the words of Chairman Kean and Vice Chairman Hamilton of the 9/11 Commission: "Our freedom and safety depend on robust oversight by the Congress."[20] Congress, therefore, should play an essential role in:

- promoting the creation of the information sharing environment with the right participants, necessary powers, and appropriate resources;
- assuring that privacy and other civil liberties are protected;
- reviewing and where appropriate approving in a timely manner the President's nominees for key intelligence, national security, and civil liberties posts;
- providing a forum and necessary information for a public discussion of the information sharing environment and the protection of privacy and other civil liberties; and
- requiring accountability and ensuring that the laws it enacts are implemented.

Like the President, Congress has already taken important steps. However, much more remains to be done. Concerns have been raised about the adequacy of laws governing the protection of privacy and other civil liberties, and the lack of appropriate oversight exercised by Congress. As deficiencies in current laws are identified, Congress should respond.

Leadership Throughout the Executive Branch to Promote Information Sharing while Preventing Misuse

Establishing and monitoring compliance of policies and guidelines

In an environment where information flows between so many users, ensuring consistent compliance with rules is essential. Doing this involves regular checks on system use through automated and manual reviews by officials responsible for compliance. Through these reviews, compliance officials can determine whether guidelines are understood and being applied correctly. This applies equally to guidelines requiring or permitting sharing and to guidelines limiting sharing. With robust monitoring, when deviations from guidelines are uncovered, compliance officials take immediate steps to correct them.

[20] *Remarks by Chairman Thomas H. Kean and Vice Chair Lee H. Hamilton*, supra at 5.

The Task Force has placed great emphasis on the ability to audit and record in real-time activity within the information sharing environment, and to maintain logs of that activity. These audit logs should track the origins of information, who is accessing that information, and for what reasons and how it is being used. The logs must be accessible, in near-real time, to compliance officials for monitoring. Compliance officials can use automated analysis of audit logs, periodic reviews, spot checks, or other mechanisms to monitor or review compliance.[21] Although it relies on technology, the process of compliance monitoring is not a technical function; it is a policy compliance function, and must be adequately institutionalized. Monitoring and custody of logs should not be the responsibility of the Chief Information Officer (CIO) or other technical officer in an agency.

Monitoring compliance of privacy and security guidelines is a way to control potential misuse of personally-identifiable information in the information sharing environment. Compliance officials must take special care to monitor compliance with privacy guidelines, and to ensure that employees are accessing, sharing, using, and retaining that information correctly. This should include reviewing that users are certifying an appropriate authorized use before accessing sensitive personally-identifiable and other information, and that their actual use conforms to such certification.

Monitoring adherence to policy guidelines will serve other important functions, such as assuring that information is being made available for sharing, that it is being protected from inadvertent disclosures, and governance mechanisms are functioning smoothly.

Institutionalized oversight and appropriate use

Traditional oversight reviews within the Executive Branch will remain a critical governance element of the information sharing environment. Oversight within agencies has typically been through agency leadership, inspectors general, and, for certain specific subjects, special purpose Executive Branch entities such as the recently established Privacy and Civil Liberties Board, the President's Foreign Intelligence Advisory Board's Intelligence Oversight Board, and ad-hoc advisory panels or presidential commissions. Additionally, a provision[22] in the 2005 appropriations act for the Transportation and Treasury departments mandated the establishment of Chief Privacy Officers in each agency funded by the act.[23] We recommend that these new officers be assigned the responsibility for monitoring the progress of policy and guideline developments for the information sharing environment.

[21] At the user level, differentiated access and permissioning technology can play a crucial role in ensuring policy compliance. They can build rules for use into the system and prevent access unless the user has—and records—an authorized use.

[22] Section 520 of the legislation (S. 2806) which came to be included in the Consolidated Appropriations Act, 2005 (Pub. L. 108-792).

[23] Section 119 of the Department of Justice Appropriations Authorization Act for fiscal years 2006 through 2009, Pub. L. No. 109-162, also required the Attorney General to designate a senior official in the Department of Justice to assume primary responsibility for privacy policy in the Department.

Further, technological tools, such as immutable audit logs, discussed further below, are an important resource for oversight. Non-technical tools for gathering information are also useful. Mechanisms such as 800-numbers for anonymous reporting of possible misuse can be a valuable source of information that would not otherwise be reported. In addition, periodic reviews by the privacy office, inspector general, or other designated agency or oversight personnel can provide indispensable system information.

Finally, a clear, calibrated, and predictable system of accountability for misuse of the system should be an important part of the information sharing environment. If there is no expectation that misuse of the system will result in a penalty, there is little disincentive for misuse. Penalties should be known, and they must be applied consistently. To be effective, penalties must be proportionate to the misuse. Overly-lenient penalties pose little disincentive for misuse, while overly-stringent penalties are unlikely to be assessed except for the most extreme abuse, and are therefore ineffective deterrents and, at least as importantly, lead to risk aversion.

Policies, Processes, and Guidelines that Facilitate Information Sharing and Provide Trust by Empowering and Constraining Users

Policies, Processes and Guidelines to Access, Protect, and Share Information[24]

While law is essential to the information sharing environment, it is not sufficient. Statutes are a powerful but often blunt instrument, and must be supplemented by guidelines and procedures to translate their strictures into practical terms. Information sharing and collaboration are still new concepts for many government employees. Information sharing environment users must understand the rules of the road. How is information to be made discoverable by others? When and how is information to be accessed? How are disputes about information access to be resolved? These and other questions must have clear answers if the information sharing environment is to function correctly.

A lack of clear guidance and instruction for personnel will likley result in either of two undesirable behaviors: users will fail to share information appropriately out of fear of making a mistake; or, because they do not want to be accused of having done less than they could, they will take actions that are risky, that intrude unacceptably on privacy and civil liberties, or that have questionable counterterrorism value. We cannot afford either behavior; clear guidelines can help prevent both.

It is most important for guidelines to be clear, understandable, and consistent for all users of the information sharing environment. Some distinctions based on differences in mission obviously will be necessary, but overall consistency is critical. Guidelines should be developed and issued incrementally. We have elaborated on these points in greater detail in each of our last two reports.

In an area this complex and dynamic, and so affected by evolving threats and rapidly changing technologies, the guidelines should be revisited at regular intervals to determine what is working,

[24] This section is based on a background paper the development of which was led by Mary DeRosa and Bryan Cunningham.

what is not, and what needs to be changed or improved. There inevitably will be ambiguities or unanswered questions; these should be addressed explicitly, not ignored or exploited to avoid the law's requirements. We recommend an annual or biannual review of guidelines by the DNI or another senior Executive Branch official charged with overseeing implementation.

Training and education are essential to ensure that agency employees know the requirements of the law and the guidelines, and that those requirements become part of the culture of the agency. When laws and guidelines are updated, they must be translated into changes in the way an employee conducts his or her job.

The Task Force therefore again recommends that the President issue detailed guidelines within existing laws to facilitate both effective information sharing and trust in the information sharing environment. While certain details of the guidelines may, as they have in the past, remain secret, by and large the guidelines should be public.

GUIDELINES FOR HANDLING OF PERSONALLY-IDENTIFIABLE INFORMATION

Since our first report, the Task Force has urged the Executive Branch to develop clear guidelines for access to and use of sensitive information, particularly information that involves personally-identifiable information about individuals. Increased information flow is a necessary response to the distributed terrorist threat, but it challenges our traditional notions of how to protect privacy and security of information. Previous protections, to the extent they existed at all, relied largely on limiting information flow. The government must replace these protections with a new approach that sets clear guidelines for use and ensures compliance.

What the Guidelines Should Address
We have offered the following principles for developing guidelines:

Retention and Dissemination of Information. Guidelines must set forth clearly the mechanisms for, and limitations on, retention and dissemination of personally-identifiable information. Administrative rules, training procedures, and technology should be implemented to prevent the unauthorized disclosure of this information. As a general rule, the collecting agency should not retain or disseminate personally-identifiable information about Americans unless it is demonstrably relevant to the prevention of, or response to, terrorism. The guidelines must articulate exceptions to this rule clearly.

Reliability of Information. Guidelines should require agencies to use the most accurate and reliable data available. They should also promote mechanisms to make any limitations on the reliability or accuracy of data known to those using the information. In the event that an agency determines that information is materially inaccurate and that an individual is likely to be harmed by future use of that inaccurate information, the guidelines should require reasonable efforts, and a clear process, to correct the inaccuracy or unreliability of the information.

Relevance of Information. A critical component of guidelines is a requirement that access to personally-identifiable information about Americans be permitted only for purposes relevant to preventing, remedying, or punishing acts of terrorism. Elsewhere in this report, we present a more specific proposal for access subject to an articulation of authorized uses. Articulation of relevance must be recorded in a way that permits auditing and compliance monitoring and other types of oversight.

Preference for Leaving Information with Stewards. Much of the information relevant to the fight against terrorism will be in private hands. The guidelines should adopt a general principle that this information remains with its original owner or steward. Any other approach would result in the development, over time, of a massive government database, which is unnecessary and inconsistent with the concept of a distributed information network. The guidelines should articulate clearly any exceptions to this rule.

Treat Different Classes of Information Differently. Different types of information involve different privacy issues. Therefore, the guidelines should separate information into a few categories and provide tailored guidance on how to access and use that information. The different classes of records should include:

- Information collected for law enforcement and intelligence purposes
- Other governmental information (e.g., Department of Motor Vehicle or Post Office Change of Address records)
- Non-governmental public information (e.g., White Pages and Google searches)
- Commercially-aggregated public record information
- Commercial non-public information (e.g., financial, credit, and travel data)

For each type of information, the guidelines should address the showing or predicate necessary to access the information.

How to Develop and Enforce the Guidelines

Implement Immediately, Develop Incrementally. Issuing clear guidelines for the handling of personally-identifiable information should be among the government's very highest priorities when implementing an information sharing network. Government officials who are accessing personally-identifiable information need immediate guidance on how to do it fairly and properly. To be certain that these guidelines are issued promptly, they should be developed incrementally, addressing first the issues that are clear. With time and experience, they can be modified and made more specific to address additional permitted uses and more complex issues.

Transparency and Public Debate. To increase public acceptance and understanding of the government's actions, and to assure a better product, the guidelines for use of personally-identifiable

information should be made available, in a manner consistent with national security, to the public for comment before being finalized or revised. In addition, any final guidelines should, on the whole, be publicly available to the maximum extent feasible.

Achieving Compliance. Compliance with these guidelines should be assured through training and monitoring, the use of audit logs and other mechanisms, to promote quick correction of problems, rather than principally through after-the-fact punitive measures. Rules can be changed, but after-the-fact punitive action directed at lower- and mid-level employees who complied with rules later deemed inadequate may lead to undesirable risk-averse behavior. In addition, investigations of suspected violations, when they occur, should focus principally on systemic measures to avoid future violations.

Ease of use. Guidelines for collection, use, and dissemination of data should be clear and easy to follow. Differences in standards and procedures should be minimized to ease confusion among employees required to follow the guidelines.

Promote use of Technology Tools. Information technology tools should be developed and deployed to allow fast, easy, and effective implementation of the guidelines for protection of privacy. These tools should create audit trails of parties that carry out searches; anonymize and minimize information when possible; and prevent both the intentional and unintentional dissemination of irrelevant information to unauthorized persons or entities.

Guidelines that comply with these principles are critical not only to protect privacy and civil liberties, but also to provide clarity about what is permitted and, in the process, to reduce risk-averse behavior.

A New Authorized Use Standard[25]

Outdated distinctions for intelligence information

At least since the late 1970s, access to,[26] and sharing of, lawfully-collected intelligence information between U.S. Government agencies has been controlled in significant measure by two factors: 1.) whether such information was collected within the territory of the United States or overseas; and, 2.) whether such information pertained to identified U.S. Persons (defined by law as U.S. citizens or permanent resident aliens). These distinctions are reflected in statute, Executive Orders, and agency guidelines. U.S. government agencies have adopted rules placing greater restrictions on sharing of information collected within the U.S. and on U.S. Persons than on other types of information.

These rules were developed to protect U.S. Persons' civil liberties as guaranteed by the Constitution. The values they reflect must continue to be respected as the information sharing environment is implemented. U.S. Persons should continue to be protected from unreasonable intrusion and

[25] This section is based on a background paper the development of which was led by Jim Dempsey, Mary DeRosa and Bryan Cunningham.

[26] In this context, "access" does not mean collection. Instead, we use the word "access" to refer to one government agency's accessing information already legally collected or obtained by another agency.

unjustified actions by their government, whether intentional or unintentional, even as information is being shared more broadly for legitimate purposes.

The impact of technology

Over time, as these rules were increasingly applied not just to collection but to access and sharing, the original interests that they sought to protect have become overshadowed by complexity, uncertainty, bureaucratic rigidity, resistance to change, risk aversion, and technological change. The rules on information sharing and access were over-interpreted and misinterpreted well beyond their original scope and purpose, with little or no public scrutiny, in ways that served neither national security nor civil liberties.

At the same time, the revolution in global communications increasingly makes it difficult to apply place-of-collection and U.S. Persons distinctions in a timely fashion. As much of the world's Internet traffic flows through the United States, and with new technical developments, it has become more difficult to determine whether information that has been lawfully collected relates to U.S. Persons, and sometimes even difficult to say where it is being collected. These technical developments include the proliferation of Internet Service Providers (ISPs) located in one country serving customers of various nationalities physically located in other countries; cellular telephones and personal digital assistants that operate across international borders; the ability of sophisticated users to mask their true identity and their physical location; the emergence of Internet-based voice communications; and the commingling of U.S. Persons and non-U.S. Persons information in various commercial and government datasets.

Too much or too little information sharing?

Task Force discussions with current and former government officials, as well as conclusions reached by other recent bipartisan investigations, indicate that the government lacks clear, understandable, and consistently interpreted rules for accessing and sharing information that formerly was governed by the line at the border provided by where the information was collected or whether it was U.S. Persons information. Lacking definitive guidance, government officials too often may fail to share information at all; may engage in ad hoc sharing practices without adequate regard for civil liberties; or may undertake uncoordinated collection activities outside their defined missions. All three results are unacceptable. For example, the NCTC, which was supposed to enhance fusion of information across the foreign-domestic divide that was so detrimental to our intelligence efforts before September 11, is still confronted with numerous limitations on accessing U.S. Persons information.

The Task Force believes that the only viable way to break through the dilemma of sharing too much or too little is to implement consistent government-wide guidelines that both better serve the original intent of the old rules (i.e., protecting civil liberties) and are workable in the post-September 11, Internet-dominated world.

The government should replace the outdated rules governing information sharing and access for legally collected information with a new, coherent, and consistent regime based on an authorized use standard. An authorized use standard would improve the access, sharing, use, and protection of relevant information legally in the government's possession while protecting privacy and civil liberties.

To achieve the widest consensus for implementation, we believe there should be an open debate involving the Executive Branch, Congress, and the general public resulting in clear guidelines. In what follows, we articulate several components of the new consensus required.

Authorized use standard to streamline and legitimize information sharing

Rules for information access and sharing should be based on the purpose for which the government party seeking access intends to use the information. An authorized use system, with such purposes clearly identified and approved in government-wide guidelines[27] promulgated in advance and approved at the highest levels of government, should replace outdated rules based on the place of collection, U.S. Persons status, or other "line at the border" distinctions.

To both enhance the ability to thwart terrorist attacks and improve protection for civil liberties, the authorized use system will have to calibrate two potentially competing goals: Ensuring that the system is 1) sufficiently granular, nuanced, and detailed to account for different levels of sensitivity of information, particularly in the case of personally-identifiable information concerning U.S. Persons; and, 2) sufficiently efficient (i.e., low in transaction costs[28]) so that information sharing environment members will use it in a timely enough way to prevent attacks.

As envisioned, an authorized use would be a mission- or threat-based justification to demonstrate that information was accessed or shared for a reason that the government, with public scrutiny, has determined beforehand to be appropriate and allowable. This concept is also intended, in part, to help define and enforce missions—the "lanes on the highway." Examples of an authorized use might include "Tracing of Terrorism-Related Financial Transactions"; "Responding to Threat to Civil Aviation in the United States"; or "Locating Known or Suspected Terrorist." An authorized use can extend to an entire program, and can be made more or less specific by program or activity, depending on the sensitivity of the information. Accountability as well as authorization is thus created for individuals' access to information.

Develop and issue specific guidelines

The guidelines for authorized use access and sharing should be based on the legal authorities and specific mission of each agency, and reflect the sensitivity of the information and how the receiving official will use it. An authorized use must be consistent with constitutional principles, statutes, Executive Orders, regulations, potential users' authorized mission, and that of their agency. This set of rules, like the other new procedures necessary to implement the information sharing environment, should be implemented only within the context of the strengthened system of auditing, monitoring of compliance, and oversight that we have recommended. Maintaining public

[27] The Task Force recognizes that authorized use must be articulated in ways that do not tip off our enemies as to how we are attempting to thwart them. Accordingly, there will be circumstances in which certain details of authorized use may not be public and may be subject only to classified oversight by appropriate Congressional committees. Such secret details, however, should not be inconsistent with public statements about missions and the application of authorized use.

[28] We frequently refer to lowering the "transaction costs" of various tasks in the information sharing environment. What we mean by this is that, as the government puts into place technical mechanisms, policies, and procedures to simultaneously enhance operational and analytic success through greater information sharing, as well as civil liberties protections for this new sharing, it must do so, to the maximum degree possible, in a manner that makes it easier for operators, analysts, and policymakers to comply.

confidence that U.S. Persons information is being used appropriately within the scope of existing legal authorities will require robust oversight and monitoring mechanisms and procedures.

To be most effective, an authorized use must be approved in advance, and embodied in guidelines of government-wide applicability. Such an approach will facilitate appropriate information sharing between agencies and replace the previous need-to-know threshold for sharing with a reason-to-share threshold while providing greater control and oversight because it requires individual officers to articulate an authorized use. In addition, articulations of authorized uses will be recorded, logged, and subject to auditing and compliance monitoring.

The authorized use standard would apply in particular, though not exclusively, to personally-identifiable information regarding U.S. Persons. This kind of information will require especially careful handling. However, a significant proportion of intelligence information that needs to be shared is either about non-U.S. Persons or is not personally-identifiable. For such information, an authorized use would be automatically generated by the system, based on the system's knowledge of the authorities relating to a particular user. If, among the results returned to the requestor are some containing personally-identifiable information that may include U.S. Persons information, then the requestor must articulate a more specific authorized use to access that information; these more specific articulations will need to meet a higher standard of care and need.

The authorized use articulation would not substitute for separate legal authority, where required, such as a National Security Letter or court order. If this additional authority is necessary under current law and regulation, then it should continue to be so. Even for personally-identifiable information, we expect that the process of certifying an authorized use would be built into the system for requesting and disseminating information. A somewhat primitive example of the type of automated authorized use certification we envision is the current process of automatically assigning the classification level to a document as it is created.

The government should adapt its technology, policies, and procedures to require users to select, articulate, and electronically certify one of a set of predetermined authorized uses as the basis for access to, or sharing of, information. The procedures and technologies for articulating authorized uses should be straightforward and easy to use.

Efficiency enhances sharing

To be effective, information sharing systems cannot impose unduly high transaction costs—that is, they cannot burden users with procedures so cumbersome that the system is unlikely to be used. Thus, procedures to protect information security and quality, as well as privacy and civil liberties, should be designed to put the least burden possible on systems usage.

For example, under existing rules, if an officer seeks personally-identifiable information in a piece of intelligence, that officer generally must initiate a dialog with the originating agency (either by letter, cable, or, at least, by phone), wait for a response and, if denied, escalate the dialog through two chains-of-command. Thus, in practice, much potentially relevant information is never even requested. Under our proposal, if an officer is able to articulate a sufficient authorized use to access that category of information, the officer would electronically certify the authorized use, which would

be recorded for system awareness and compliance through the audit log. Following this electronic articulation, the personally-identifiable information would be requested from the original information holder; if an adequate showing of authorized use is presented, the information would be provided. For many categories of information, this process can be built into the business rules of the electronic system, and not require any human intervention. For other, particularly sensitive types of information (e.g., income tax records of U.S. Persons), human intervention, albeit quick and efficient via electronic means, may be required. This can increase the timeliness and the consistency of gaining access to the information, while simultaneously enhancing civil liberties protection by compelling the officer to articulate an authorized use. It also creates a record of the transaction for subsequent compliance review.

As implied above, then, while significant amounts of information will be sufficiently non-sensitive to require a low threshold for articulating an authorized use (see below), our proposal assumes the necessity of a sliding scale in the degree to which anonymized information can be immediately deanonymized. That is, the more sensitive the information, the higher the required authorized use, the stricter the audit, and, potentially, the greater the need for an official to consider approval for deanonymization. For example, the spectrum of authorized uses might well include a limitation that, if an officer wishes to deanonymize information about a known U.S. Person that is of particular sensitivity (e.g., income tax records), then that officer might need not only to articulate a high authorized use, but electronically petition a supervisor or other officer for deanonymization.

It also is important to note that although the authorized uses will have to be fairly complex—taking into account not only the sensitivity of the information, but also roles and responsibilities of individual components and, most importantly, the use to be made of the information—these rules, once determined, would be embedded in the operating software and hardware of the system. Thus, for example, an authorized use of "to detain a criminal suspect" would never even show up in the CIA or the DoD menu of options for articulation of authorized uses, whereas it would in menus for the FBI and the DHS (for a sufficiently high authorized use showing).

In many cases, authorized use determinations would be made not on the basis of individual items of information but, in addition, by category or type of information. For example, an entire office in an agency might have an authorization, based on its mission, to obtain certain less-sensitive information. In some cases, however, specific electronic records of authorized uses would be necessary even for individual units or officers in these offices. One example when this might be required is when an officer who has received anonymized information (i.e., with personally-identifiable information concerning U.S. Persons electronically removed) seeks the personally-identifiable details. Another example would be when an officer seeks to use information accessed previously for one authorized use for another, new and more intrusive, purpose—e.g., to take some potentially adverse action against U.S. Persons.

THE U.S. PERSONS PROBLEM

For decades, U.S. intelligence agencies have treated information regarding U.S. Persons (defined as U.S. citizens and permanent resident aliens) more carefully than information concerning non-U.S. Persons. Also, the U.S. government has applied much higher standards to the sharing of information collected inside the United States through means such as electronic surveillance than to information collected outside the United States. These practices are in part constitutionally mandated and are reflected in statute, Executive Order, and agency guidelines. They serve important principles that should continue to be respected: U.S. Persons must be protected from unwarranted intrusion; and intelligence investigations inside the United States should be carefully controlled to fulfill the individual's rights vis-à-vis the state. The Task Force takes no position on the continuing appropriateness of the current collection rules.

However, applying these collection rules to the access and sharing of information based on the nationality of the subject or the geographic place where it was collected has generated confusion, and in some cases produced a rigidity that impedes necessary and appropriate information sharing. This outcome is often more the result of misinterpretations rather than a consequence of the rules themselves.

Current and former government officials with whom the Task Force spoke provided several scenarios by way of example to illustrate the issue and its impact:

Scenario No. 1: The National Security Agency (NSA), conducting lawful electronic surveillance of a suspected Al Qaeda cell in Pakistan, intercepts calls to and from telephone numbers in San Diego. The San Diego numbers may pertain to U.S. Persons and, in the absence of further information, the NSA likely will presume that they do. In these circumstances, under rules in place prior to September 11, the NSA would have disseminated a summary of this intelligence to the FBI, but, based on the NSA's internal interpretations of the U.S. Persons rule, it would not have disseminated the full 10 digits of these San Diego numbers to the FBI. Instead, the NSA would have reported the fact of the call but redacted all or part of the phone number, rendering it impossible for the FBI to follow-up. The FBI would need all 10 digits to compare them against lawfully-collected information in FBI files, and to conduct follow-up FBI fieldwork in San Diego—work that the FBI is legally authorized to conduct. Under traditional practice, the NSA would have shared the complete numbers with the FBI only if the FBI requested them in writing, and even then, the requests would have to be made on a *number-by-number basis.*

Under the Task Force's proposed approach, since the information is clearly of foreign intelligence value and merits follow-up in the United States, it would be permissible for the NSA to disseminate the full phone numbers to the FBI without awaiting a specific request from the FBI. Under our approach, absent appropriate legal authorization, the NSA would not target the San Diego phone numbers—the FBI would do that under its lawful process for wiretaps. An authorized use system would allow this sharing to happen quickly, while real-time auditing and oversight would ensure that the information was used and maintained properly.

Scenario No. 2: Assume that the FBI does acquire the complete U.S. telephone numbers from the NSA. It analyzes the information and does some investigation, determining that the subscribers to the U.S.-based numbers may indeed be

Al Qaeda associates. The subscribers, however, are U.S. Persons. The FBI has full legal authority to investigate U.S. Persons within the United States who are suspected members of a terrorist group. But varying interpretations of the U.S. Persons rule have affected whether the FBI shares with the NSA a number of additional details——including the names of the U.S. Persons, and information about other phones they have used or to which they have placed calls— so that the NSA could help determine whether it had other relevant information, and whether it should initiate the collection of overseas intelligence.

In the view of the Task Force, the guidelines should make it clear that the FBI can share with the NSA the names of the U.S. Persons and information about other phones they have used, or to which they have placed calls. This would permit the NSA, within its authority, to determine whether it has other information regarding those persons or telephone numbers, and to initiate the collection of foreign intelligence overseas. An authorized use system would facilitate such follow-up, which would be fully consistent with the NSA's mission and authorities, and would also allow real-time auditing to help generate new knowledge and intelligence by analyzing the ongoing access, sharing, and querying of the system.

Scenario No. 3: The FBI, in pursuing the trail of the San Diego-based individuals who may be Al Qaeda associates, finds indication that U.S. Persons may be engaged in money laundering in support of international terrorism. The FBI agent seeks the tax records of those individuals.

Tax records are under particularly strong legal protections. Thus, while the FBI has an authorized use for getting the records, it would need special legal authority. The authorized use concept proposed by us does not supply that legal authority. The authorized use system would notify the FBI agent that she needs to obtain additional legal authority before being able to access tax records, even though those records are lawfully in the possession of another branch of the U.S. government.

Scenario No. 4: The CIA, conducting overseas operations, discovers that overseas bank accounts of known terrorists are receiving transfers from certain U.S. bank accounts. The CIA wants to discover the names of the holders of the U.S. accounts (any or all of whom may—or may not—be U.S. Persons). It also wants to obtain the addresses, phone numbers and other identifying information about those individuals in order to determine if such information corresponds to any of the overseas bank accounts the CIA is monitoring, or if it is otherwise linked to other foreign intelligence information collected by the CIA overseas. The CIA also seeks further information on financial transactions within the United States to identify possible supporters of terrorism within the country.

The CIA has the statutory and Executive Order authority to pursue terror financing overseas, even if it involves U.S. Persons. Therefore, under the authorized use system, the CIA would be able to obtain information identifying individuals who may be U.S. Persons for the purpose of determining whether those persons are engaged in terrorist financing activities overseas. However, the CIA would not be authorized to collect presumed U.S. Persons information for the purpose of tracking money flows within the United States. To the extent that there is a need to investigate activity in the United States, the CIA should rely on the FBI or the Treasury Department. The CIA would receive U.S. Persons information only to the extent that such information constitutes foreign intelligence. Under an authorized use system, the appropriate limited access could occur with little transaction cost, while any potential misuse would be identified by the real-time auditing and oversight built into the system, as well as by traditional oversight mechanisms.

In each of the scenarios, the collection of intelligence was properly authorized under statute, Executive Orders, and agency guidelines. The scenarios highlight the importance of creating smooth processes for collaboration between agencies, and for access to and sharing of information within established rules. Under the authorized use system, the information would be shared for the purpose of the receiving agency using it to further its own authorized mission. Without rules like those we propose, the government is inhibited in its ability to protect our national security. The absence of such rules also fails to protect civil liberties, because it leads some state, local and federal entities not traditionally involved in the collection of intelligence information to develop their own sources of information inside the United States.

GENERAL PRINCIPLES FOR DEVELOPING THE AUTHORIZED USE STANDARD

Ensure Applicability Across the Government. Generally speaking, categories of authorized use should apply to all information sharing environment components, although, as discussed elsewhere in this report, the guidelines will also have to be tailored to the specific missions and authorities of individual departments and agencies.

Tailor to Anticipated Uses. The authorized use standard for access to, or sharing of, information generally should be lower when the information is to be used for terrorism-related analysis, policymaking, or alerting functions; and higher when the anticipated authorized use is reasonably expected to include some action (such as detention, travel restrictions, or denial of a benefit) within the territory of the United States or against U.S. Persons.

Treat Anonymized Information Differently. The Task Force has recommended the use of anonymization technology to enable information analysis without disclosure of personally-identifiable information. When combined with anonymization techniques, the implementation of a properly-defined and implemented authorized use system could facilitate use of information in ways that enhance both national security and the protection of civil liberties. For example, if an agency has an authorized use to obtain only a few records in a large dataset, the overall information could be correlated anonymously to determine the finite number of matching records. The receiving agency could use the matches discovered in the anonymized information to request specific records for sharing only when it meets a higher threshold of justification. This not only has obvious civil liberties benefits, but also would contribute to operational efficiency (i.e., less information transferred means less information to keep current).

Articulate Authorized Use Guidelines. Authorized use guidelines should be developed through an appropriate public process. Legislation would set out the framework for an authorized use regime and the Executive Branch would develop specific implementations through a formal high-level process with as much transparency as possible. This process should include the participating agency's information sharing environment privacy and civil liberties officer, and should be reviewed by the Privacy and Civil Liberties Oversight Board prior to final approval by the President.

Expansions to an authorized use should receive a thorough review and specific approval that is made public.

Electronic Record of Authorized Uses and Compliance Monitoring Through Audits. Transmitting agencies would be required to keep an auditable record of each dissemination for which an articulation of an authorized use was made. The sharing and subsequent use of the information would be subjected to auditing and monitoring of compliance to ensure that information is utilized consistently with authorized uses. This auditing will be helpful to protecting civil liberties, as well as the security of information against insider compromise. Auditing monitoring sharing logs would have the added benefit of creating new intelligence and knowledge for analysts, policymakers, and others, as well as facilitating dispute resolution, by creating real-time, electronically-accessible records that automated software could use to identify common questions by different analysts. Such real-time logs will also play a role in helping identify unauthorized access, both for counter-intelligence purposes and to protect civil liberties.

Minimize Transaction Costs. The system must be designed from the outset to record authorized uses electronically in the simplest possible way consistent with the sensitivity of the information requested. Sometimes it will be automatic, such as when an entire agency or component is authorized to receive information based on its mission. Other times it will require a single mouse click or a short explanation where an officer receiving, forwarding or authorizing access to information must affirmatively articulate an authorized use. To the extent that this process can be electronic—which we strongly recommend as the preferred solution wherever possible—it will minimize transaction costs to users. It will be critical, however, that, as the government seeks to minimize transaction costs for articulating authorized uses, it also creates mechanisms to ensure that authorized use determinations do not become either arbitrary or automatic. Officers must be required to think through, albeit quickly, their selections, and be able to articulate why they selected the authorized use they did.

Clarify Roles and Responsibilities. It is important to clarify the roles and responsibilities of all participants in the information sharing environment. Implementation of authorized uses will help ensure that departments and agencies stay in their lanes, as authorized by our nation's leadership and understood by the public.

Mitigating risk aversion

Any rule-based system must ensure that those who live by the rules will not be punished if the rules change, so long as they followed the rules applicable at the time of conduct. Appropriate consequences for violating rules should be coupled with a safe harbor for compliance. Based on previous Task Force work, we believe that an important element of the information sharing environment is that it must empower government officials with clear rules about actions they can take. Otherwise, confusion regarding their authority will cause them to refrain from taking appropriate action that might uncover a terrorist plot or thwart an attack.

One of the most significant barriers to effective pre-September 11 information sharing, identified by numerous investigations, is risk aversion. Risk aversion arises in part from fear among government

officers that information sharing that is clearly authorized at the time of sharing will subsequently be judged to be improper, resulting in personal criticism, career damage, and even criminal prosecution. Discussions with current and former officials indicate that the perception of this risk has been and, to some extent remains, a significant deterrent to effective information sharing.

To reduce such risk aversion, and thereby increase the effectiveness of our national and homeland security efforts, we recommend that our proposed guidelines include a carefully considered safe-harbor mechanism. A safe-harbor provision would ensure that, so long as there is a record of a proper authorized use having been articulated simultaneously with information access or sharing, and so long as there is no indication of bad faith, no punitive action could be taken against an individual government officer for having shared information with another agency. Departments and agencies would be ordered to revise their internal regulations to adopt safe-harbor provisions.

The guidelines should make clear that officials responsible for oversight of the information sharing environment could investigate systemic failures or misuses of the system (e.g., to improve the system, improve training, or ameliorate other systemic problems), so long as such investigations were not aimed at individual officers acting in good faith compliance with authorized use procedures. Investigations of individual officers could include random spot checks of authorized use certification, and regular training and testing; proper use of the system could also be included as an element in officer personnel evaluations. What should be avoided, however, are the kinds of perceived investigations that too often in the past have resulted in risk aversion among officers who felt they were trying to follow the rules in good faith, but were unfairly investigated either without evidence to suggest bad faith, or when rules were later changed.

It is not our intent that wrongdoing should be immunized. Rather, with this recommendation we seek to overcome the dynamic in which lower level employees find their judgment questioned, and their careers jeopardized, when it becomes clear that the rules they were following were inadequate. If the rules for sharing are inadequate, policymakers should focus on changing them, not on punishing career employees who thought they were following the right rules. This recommendation should be implemented only in conjunction with our call for clearer guidelines, an efficient dispute resolution process, and robust auditing of compliance. In the past, disruptive investigation of employee behavior often arose when the rules for the specific activity were non-existent or ambiguous. Our call for clear guidelines and a dispute resolution process will minimize the situations in which employees are acting in a vacuum. If our recommendations are implemented, it is more likely that employees will be held accountable to an objective standard, and that there will be an unambiguous audit trail.

A Process to Resolve Disputes in Information Sharing

Even with clear and consistent guidelines for information sharing, disputes will inevitably arise. Information sharing environment participants, particularly in the early stages, will confront unforeseen circumstances for which there exists no clear guidance. There will also be differences of opinion about interpretations of even the clearest guidelines, particularly when classified or otherwise sensitive information is involved and agencies have conflicting perceptions of the risks of sharing. The information sharing environment must include a systematic, workable, efficient process

to resolve these disputes. Through the resolution of disputes, that process can provide practical support to advancing the overarching goal of responsible information sharing.

In fact, a dispute resolution mechanism of sorts already exists. If someone's desire to access disputed information is strong enough, they will begin the process of having my boss call your boss. Sometimes this process will escalate to very senior levels before a decision is made. However, this type of ad hoc process is too cumbersome and inefficient for the demands of national security. It takes too long and, because it often will involve senior officials, it is invoked infrequently. Often, the requestor will simply give up, and no sharing, collaboration, or accommodation occurs. Further, there is no way to derive lessons from earlier decisions in an ad hoc process such as this one, and there is little prospect of the process becoming more efficient over time. It is clear that a better process is needed.

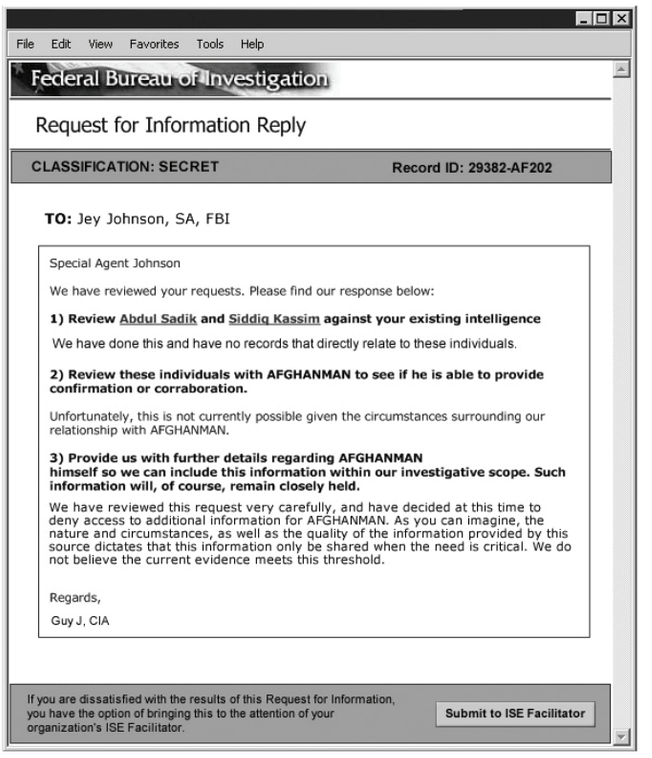
In its initial stages, a dispute resolution process will likely need to be fairly formal. Over time, however, it could become less formal as situations repeat themselves and a common law of sharing decisions develops. Once there is a systematic process for recording and referring back to previous decisions and the principles that guided them, the dispute resolution process will become more efficient, and will need to be invoked less frequently. With a body of common law offering precedents, information sharing environment participants will have an increasingly clear sense of how dispute decisions are likely to be resolved, so that they will be able to anticipate decisions and act accordingly.

This process would address a range of information sharing disputes. At the individual user level, the process would resolve disputes over one user's decision not to share information. It would also address disputes about dissemination and retention of information, the accuracy and correction of information, as well as broader disagreements about access to and use of databases and categories of information by information sharing environment users.

The transaction costs of invoking the dispute resolution mechanism must be as low as possible, but not so low as to encourage arbitrary appeals. In many cases, it will be more important to have an incomplete answer immediately, while the information can still be useful, than it will be to have the perfect answer later. The dispute resolution process should be dynamic, or it will be irrelevant.

The dispute resolution process in action

The first step should always be an attempt to resolve the issue at the lowest level, between the person requesting access to information and the steward of the information. However, because it is far too easy to have a stand-off between requestor and steward, there should be facilitators at the agency level who are responsible for coordinating with their counterparts in other agencies, collaborating, and, if possible, resolving these matters (See figure).



Illustrative dispute resolution screen

If that does not work, the person seeking access to information should be able to escalate the issue quickly to a dispute-resolution official outside of either agency who answers to the central coordinator. There should be a cadre of such officials with broad authority to employ mechanisms to mitigate risks of improper disclosure, and to obtain more details about the requestor's need for the information. There must be a short time limit for resolving disputes, and the dispute-resolution official's decision should be binding on the parties, absent unusual circumstances that require appeal.

There should be a process for elevating matters of significant importance rapidly—as high as the White House, if necessary—but its use should be rare, and strict time limits should apply. If senior officials become involved routinely, the process will bog down. Therefore, if escalation becomes common, the system will be too cumbersome.

No step in this process should require face-to-face meetings or exchange of paper, except when absolutely necessary. To the greatest extent possible, matters should be resolved electronically. Electronic resolution will also facilitate the creation and maintenance of up-to-date information about resolution of these disputes so that a common law can develop. This common law will enhance the prospects that disputes will be resolved consistently and predictably, and, over time, will result in fewer disputes because there will be general knowledge about how recurring disputes will be handled. In any event, the guidance must be consistent across all agencies, and coordinated centrally. Every effort must be made to assure that all officials are using the same guidance.

Managing the Risks of Sharing and Not Sharing[29]

Much of what must be shared in the information sharing environment is sensitive national security information that must be protected from improper or unintended disclosure.[30] Fear of wrongful disclosure has historically driven decisions about classification and dissemination; the result has been a search for almost perfect security. The rules, processes and culture of the current classification system concern themselves almost exclusively with the risk of information falling into the wrong hands, making it nearly impossible to tolerate any disclosure risk. To be sure, there are justifiable concerns that increased sharing will compromise security; greater sharing of sensitive information increases the risk of damaging security breaches. On the other hand, risks of disclosure must also be balanced against the risks associated with failing to share information. The current system fails, in any systematic way, to balance these competing risks. As some officials described it, the goal of the current system is to minimize regret by seeking almost perfect assurances that information will not be improperly disclosed.

Calculating the risks of sharing and not sharing information

Considering only a single risk variable poses a problem in the new threat environment because it fails to consider the very real risk to security of failing to share. Information sharing is so important because often, we will not know what information is relevant to the terrorist threat, where it will come from, or who will be able to make sense of it. In order to understand threats and prevent attacks, we must find ways of connecting relevant pieces of information when their holders might not fully understand their significance. This requires sharing information in a robust, distributed way. Therefore, a risk calculation for sharing classified information must weigh two competing risks. Seeking perfect protection from the risk of unintended disclosure by restricting information sharing will result in an unacceptable increase in a different risk -- the risk of failing to connect information.

The fact that significant security risks exist on both sides of the calculation makes a balancing or risk management approach to sharing decisions far more critical than in the past. Therefore, new policies and processes are necessary to ensure that both risks are considered appropriately. Most importantly, there must be clear direction to those making risk decisions that those decisions should take into account the importance of sharing information. Although there have been a number of clear statements of the Executive Branch policy to encourage robust information sharing,[31] the President must repeat this principle explicitly in the context of decisions about handling classified information.

It is also critical that the people making decisions about access have a broad perspective on both sides of the risk calculation. Currently, decisions about when to share classified information are made primarily by the producers of that information. Those producers may have a very good understanding of the potential dangers of disclosure, but they do not necessarily bring to the

---

[29] This section is based on a background paper the development of which was led by Mary DeRosa.

[30] The information sharing environment would be unlikely to include all types of classified information. Some of the most sensitive information—capabilities or numbers of technological assets, for example, or continuity of government information—is not the kind of information that would be useful to users seeking to collaborate with others or to detect terrorist plans or activities.

[31] Strengthening the Sharing of Terrorism Information to Protect Americans, Executive Order No. 13356, § 5(b), 69 Federal Register 53599 (Sept. 1, 2004), and Further Strengthening the Sharing of Terrorism Information to Protect Americans, Executive Order No. 13388, § 1(a), 70 Federal Register 62023 (Oct. 25, 2005),which superseded it, set forth the policy that "interchange of terrorism information" among agencies and between agencies and state, local, and international governments and appropriate private sector entities be given the highest priority.

decision-making process a rich understanding of the value of the information to users. Decision-makers in this process must have a more balanced perspective.

Obtaining a balanced perspective on risk is complicated by two factors. The first is the power that originators or producers of the information still hold over how it is handled. Classified information historically has been considered to be owned by its originator. This ownership, which the President sought to reform through Executive Order 13292, amending Executive Order 12958, permits the originator to control decisions not only about original classification, but also about subsequent handling and dissemination. This ownership power is a significant impediment to any process that would encourage officials with a broader perspective to make decisions about risk.

The second complication is the fact that the risk of failing to share is difficult to assess at the time a sharing decision is made. It is relatively easy to measure the potential harm of improper disclosure. It is far more difficult to identify and quantify the harm of failing to share and connect information. Decision-makers do not know how useful a piece of information will be if shared, or who needs to know that information in order to connect it with other information and make sense of it. The answer to this dilemma cannot be simply to assume there is broad need for all information and to push extremely sensitive information out to all parties who *might* need it. Nor can the answer be to insist on a complete accounting of this risk—a full explanation of the need to know—before factoring it into the calculation.

Several mechanisms are available to improve the calculation of risk. While there has been a significant effort to reduce the use of ORCON (or originator-controlled information) in government, particularly through Executive Order 13292, relevant terrorism-related information is still treated as if it is owned by the agency that retains exclusive control over its classification, use, and dissemination. First, there should therefore be an explicit statement of policy that originators or producers do not own or control the information they produce. If it is deemed too difficult to be rid entirely of the concept of ownership for classified information, then only two or three very senior officials, such as Cabinet Secretaries and the DNI, should be permitted to assert ownership to impose distribution limitations for classified information, and there should be explicit direction that this authority cannot be delegated.[32]

Second, since various stakeholders may disagree on how to classify information and whether and how to share that information, there should be a quick, efficient dispute resolution process, of the kind we described earlier. An effective dispute resolution process will force action; producers will not be able to avoid sharing simply by sitting on a request. A process with quick escalation of disputes to decision-makers whose perspective is broader than that of the information's producer or requestor can ensure that appropriate sharing decisions are made.

[32] This does *not* mean that these senior officials should be responsible for maintaining or making access decisions generally for all of this information. This shift only involves the ability to assert "ownership" to block access to classified information. It is a basic Task Force principle that information should reside with its originator, who will act as a steward for that information and be responsible for updating the information and maintaining its accuracy as well as assuring that it is accessed and used appropriately. This recommendation would do nothing to change that stewardship role for the classified information's originating agency.

Third, because not enough is always known initially about the risks of failing to share, one mechanism that can improve risk decision-making is to develop a process for learning more about those risks. One such process is *dynamic permissioning*. If a user seeking classified information cannot initially make a strong case that the information is needed for investigation, analysis, or some other important purpose, a process should begin of developing more information from less sensitive sources. As more is known about need—the risk of failing to share—the potential user can return to the dispute resolution process with more information and receive a new review quickly.

Finally, an important mechanism for coping with the risks of failing to share is to emphasize *pulling* rather than *pushing* to share information. Being aware that certain information exists can be more important than being able to access the information. If a user can locate information, he or she can begin discussion and collaboration or, failing that, dispute resolution. Although the information sharing environment PM and others in the government have recognized the importance of mechanisms for *pulling* information, to date not much progress has been made in that direction. The government has not yet developed a mindset and technology approach that encourages and empowers users to locate and seek access to (i.e., *pull*) relevant information that resides elsewhere in the bureaucracy.

The importance to risk management of *pulling* underscores the critical importance of creating an index or directory service for all information in the environment. Again, the information sharing environment PM has taken initial steps to create directories, but more progress must come quickly. These indices or directories would be used to register available information and create pointers to that information. No effective system for *pulling* will exist until potential users have a way to locate information, even if they might not get access. In seeking access, the user can provide the information's holder with a better explanation of his or her need for the information. If the holder is not convinced access is appropriate, the dispute resolution process described above can help determine whether there is sufficient information about the need for this information, begin a process of dynamic permissioning, and—as is discussed in more detail below—find mechanisms to mitigate the risks of disclosure.

Mitigating the risks of sharing and not sharing information

Even with an approach to calculating risks that recognizes the need to share, there will be a need to find creative ways to reduce disclosure risks. Currently, decisions about classification, declassification, and clearance for access are, for the most part, all-or-nothing. There is little room—officially at least—to adjust protections to particular situations or needs.

Because of the rigidity of the current system, people find ways to build in flexibility outside of the rules. When the need is great and sharing is necessary, well-intentioned employees will bend or break rules in order to get something done. Sometimes information that should be designated as classified is not because it would then become too difficult to transport or communicate. In crisis situations, the response to a lack of flexibility will sometimes be to adopt ad-hoc solutions outside of the system. These practices result in increased risk of unintended disclosures and, because they are ad hoc, do not help address the need for greater sharing on a regular basis.

Currently, the system for access to classified information has few points at which decisions are made, and allows for little flexibility or nuance in decision-making. These decisions include whether and at what level to classify information, whether to declassify that information, whether to clear a person for access to general categories of classified information, and whether a person has a need to know certain information. Except for the need-to-know inquiry, none of these decisions looks at a particular use or transaction; they attempt to make one determination for all time. In fact, the decision to classify is often made at the lowest level of the originating organization, and not reviewed again by either superiors or users.

A decision-making process that fosters information sharing should accommodate a greater focus on individual transactions and greater flexibility about decisions to allow access to information. Dispute resolution officials should be encouraged to mitigate risks as warranted under particular circumstances. This mitigation could include, under some circumstances, declassifying information or providing access—full, partial, or qualified—to people who have not been fully cleared for that information. If, for example, there is a crisis that requires state or local officials, or others with no security clearance, to be informed quickly about a piece of information, the current system has few workable mechanisms for relaxing standards of access, or for truncating the process of clearing a person. What often happens in situations like these is that the person is granted access, but the decision is ad hoc, made outside of the system, and guided by no consistent rules or processes across the intelligence and law enforcement communities.

A balanced approach to risk calculation requires some flexibility to, on rare occasions when the situation may warrant it, allow uncleared or inadequately cleared people access to classified information. But mechanisms can and must be developed to allow this access in a way that minimizes risk. This can be done primarily by using abbreviated measures to assess trustworthiness. For example, a state health official might not be cleared to see classified intelligence, but there could be a standard process within the system to assess her trustworthiness and allow access to critical information. This type of transactional decision-making should be available not only for emergencies, but also in the normal course of sharing and analyzing information, such as when an ad hoc collaborative team requires the expertise of an uncleared expert, or when an analyst is working on a particular subject to which the information is uniquely relevant.

Mechanisms for minimizing risk under these circumstances should include the ability to allow temporary clearances based on a truncated background check. Similarly, the government could adopt a program of determining places—in the private sector or among state and local officials—where this type of emergency clearance is likely to occur. It can then identify select people to whom it either provides clearances in advance, or on whom it conducts background checks, so they can be cleared immediately if necessary.

In the current system, there exists virtually no ability to calibrate the manner of access to information, or to adjust to different situations. Because the current system seeks perfect security, and no risk of unintended disclosure, it views all access as equally suspect. In fact, some types of access to classified information pose greater risks than others. There are many ways, particularly with the use of technology, to decrease the risk of access to classified information, but the current system

does not systematically allow this type of consideration to affect decisions about access to information.

One way to mitigate risks is to find creative ways to convey the useful information in a document while still protecting the most sensitive information. This concept of writing to share is something the Task Force has discussed in its earlier reports. Many elements of the intelligence community already use tearlines and other write-to-share techniques, but the practice should be expanded. Writing to share simply means that documents are produced in a way that permits the greatest number of users to access them. An electronic tearline is an example of writing to share. An official creating a document with an electronic tearline will record information that is subject to a low classification separately from highly classified information, so someone without the high-level clearance will be able to view portions of the information.

Another technique we recommended in an earlier report is the use of reputation meters to indicate the credibility of a classified source through the use of a ranking system, so that useful information can be conveyed without revealing the source. Similar tactics can be employed with other types of classified information. For example, certain kinds of quantitative information, such as patterns of contacts or characteristics of weapons, can be expressed with approximations ("at least 10," for example, instead of a specific number). Imagery information might be less sensitive if disseminated at lower resolution, but still provide useful information. In addition to using these write-to-share techniques at the time information is recorded, dispute resolution officials should be allowed and encouraged to adjust content at the time of disclosure decisions in a way that will reduce risks.

In addition to adjusting content, there are ways to allow access to information that are less risky than providing a hard copy of a document. For example, allowing access only in a shared but restricted technology environment, in which the users' identity and activities are recorded, logged, and subject to subsequent audit and compliance review will mitigate disclosure risks.

Finally, the rigidity of the current classification system makes it very difficult to adopt technology and policy that can mitigate, but not eliminate, risks of disclosure. The current standard for implementing technology for disseminating classified information is that it must be virtually free of risk from technical attack or compromise—obviously a difficult standard to satisfy. But often technology that has little, but some, risk of technical attack will be able to provide significant protection against human compromise. The current system lacks a mechanism for accepting some risk of technical attack if a technology might decrease the risk of human compromise.

Improving the Decision-Making Processes of Senior Officials[33]

The real value of an effective information sharing environment comes not from sharing for its own sake, but rather from the environment's ability to improve collaboration, decision-making and policy implementation. To achieve these goals, an information sharing environment must be designed in a way that takes into account the needs and practical constraints of senior decision-makers. An

[33] This section is based on a background paper the development of which was led by James Steinberg and Richard Falkenrath.

information sharing environment has the potential to improve the timeliness and quality of information available to senior officials. Beyond that, an information sharing environment should facilitate a more robust two-way exchange between analysts and decision-makers, both for tasking and for analysis; provide decision-makers with a more nuanced understanding of the strengths and weaknesses of the information underlying finished analysis; include divergent perspectives; and reduce policymakers' dependence on stovepiped intelligence units within their own organizations.

The potential of an environment where information is more discoverable and appropriately shared may be particularly beneficial for state and local officials, who currently have little or no direct interaction with the analytic community, and who therefore rely almost exclusively on products (both raw and finished intelligence) that are pushed to them by federal officials. Federal officials, particularly at the most senior levels, already have considerable ability to probe the analytic community and to stimulate additional tasking. Even for them, though, access to a properly designed information sharing environment could improve the ease and timeliness with which the interactions take place, for example by including real-time exchanges during senior interagency policy deliberations.

However, there are some complications associated with increasing policymakers' interactions with the intelligence community through an information sharing network. Some federal officials may be reluctant to engage with the system, either due to a lack of familiarity with the tools; or out of fear that too much interaction will expose internal policy deliberations or preferences, or even subject them to charges of interference with the analytic process. Properly designed safeguards can mitigate these problems while still maintaining accountability.

Extensive information sharing with state and local officials may complicate coordination between federal, state, and local officials when it comes to notifying the public about potential threats. Federal officials periodically acquire information on possible terrorist threats inside the United States. Threat information has both offensive and defensive value. On offense, it can be used as information to better understand, penetrate, and attack a terrorist conspiracy. On defense, it can be used to harden particular targets and to enhance readiness.

However, offense and defense can be significantly at odds. So even if threat information is almost always imperfect and incomplete, state and local officials may face significant pressure to advise the public of threats even when there is no clear operational benefit of issuing a threat warning. Unfortunately, defensive actions taken by state and local officials might tip off conspirators and undermine offensive operations by federal authorities.

Precisely because of these complexities, there should be a concerted effort to promote the use of information sharing capabilities among senior officials. Promoting the use of information sharing tools among senior officials is likely to be an uphill struggle. It is, however, critically important, so the information sharing environment PM should start with a very strong, orchestrated effort to push relevant information from the envisaged distributed network to senior officials. Training in the use of the new capabilities should be combined with the security briefings provided to incoming officials at all levels. Organizationally, the focal point for promoting usage of new information channels among senior officials should be the DNI. The DNI should combine or collocate the management

of the systems with the management of the intelligence community briefing teams for senior officials. The DNI should also issue a directive or guidelines regarding the use of the architecture for senior officials by departmental intelligence offices (e.g., the Defense Intelligence Agency, the DHS' Office of Intelligence, the FBI's Directorate of Intelligence, and the State Department's Bureau of Intelligence and Research).

WAYS TO PROMOTE THE USE OF INFORMATION SHARING CAPABILITIES BY SENIOR OFFICIALS

The information sharing environment Program Manager should develop technology designed to encourage senior official usage. Technical innovations in the information sharing environment can improve usability by senior officials. Develop a portable wireless device (e.g., a broadband wireless laptop with encryption and biometric security measures) for use by senior officials on travel or at home. Integrate electronic dashboards into a secure video teleconferencing system used routinely by senior officials in the national and homeland security area. Integrate senior official alerting systems (currently highly fragmented, but often non-secure commercial off-the-shelf applications) with the system. In particular, allow senior officials to customize the alerts they receive on their portable communications devices with respect to content and code words.

There should be special procedures to build capacity among senior officials to manage the risks associated with information sharing. The DNI should establish a technical training program for personal and special assistants to senior officials. It should also develop special guidelines, including greater control over the release of usage information, for senior officials at departments and agencies, and for White House staff. For White House and NSC staff, locate all usage information in the White House Counsel's office. For all presidential appointees confirmed by the Senate in departments and agencies, locate all usage information in the General Counsels' offices.

Conduct a comprehensive review of procedures and authorities for compartmentalizing information in light of expanding U.S. information collection and enhanced, innovative information sharing. From time to time, there will be legitimate reasons for compartmentalizing information (i.e., for not sharing it); senior federal officials are usually the individuals with the authority to make these determinations. But not all reasons for which senior officials may wish to compartmentalize information are legitimate. For example, compartmentalization for the purpose of protecting a particular sensitive operation, source or method is usually legitimate, but compartmentalization for the purpose of excluding properly cleared, responsible senior officials with differing policy views from decision-making—or for the purpose of avoiding lawful forms of review and oversight—is inappropriate, and should not be allowed. Another consideration to more fully leverage compartmentalized information could involve placing the existence of the information (e.g., using metadata and pointers only) into the catalog (possibly in an anonymized form if necessary) and then alerting users when a match is found.

There should be special training and awareness programs for senior state and local officials who are incorporated into the system. Participation in the information sharing environment should be treated as a privilege, not a right, and clear, reasonable rules of the road need to be established for all participants. In this respect, non-federal officials—whose lines of accountability do not trace to the President or any federal official—have a special responsibility to learn about and respect the interests of the many other stakeholders in the new information sharing environment, especially the federal agencies that conduct operations abroad to both acquire information about, and preempt, terrorist conspiracies. Federal officials, equally, have a responsibility to respect the needs of local officials for access to information to allow them to do their jobs.

Developing Adequate Training and Education to Improve Information Sharing Expertise[34]

The human dimension is critically important for information sharing. The intelligence, law enforcement, and homeland security communities need to give top priority to substantially expanding community-wide training based on a common set of skills, updating analytic methods, and using best practices.

Lack of common training contributes to cultural gaps between intelligence, law enforcement, homeland security, and military personnel; these gaps remain a root cause of poor information sharing. The situation has become even more difficult as the community of counterterrorism analysts and collectors expands beyond the federal level to include state, local, and private sector participants, and as the volume of available information grows.

While we and others have stressed the importance of education and training in the past, we believe they are so important as to warrant more detailed recommendations for how they can be significantly strengthened in order to build common skills, foster collaboration, instill a community-wide respect for civil liberties, and bridge cultural divides between the intelligence, law enforcement, homeland security, and military communities.

As a first and essential step, the DNI should develop a core curriculum on information access, sharing, analysis, and use, and basic standards of training and career development for the U.S. intelligence community. This should also be shared with, and used by, federal law enforcement and homeland security officials not already included in the intelligence community. The DHS also should develop similar guidelines for state and local officials, and for the private sector.

Establishing a foundation for entry-level skills and training

Taking an entry-level course and passing some form of proficiency evaluation should be a minimum requirement for initial certification into the information sharing environment community. There are several basic skills that should be required at entry into the environment. These include elements of critical thinking, an ability to communicate verbally and in writing, a standard set of analytic

[34] This section is based on a background paper the development of which was led by Rand Beers.

methods, and a basic understanding of information technology and tools. Real-world examples and lessons learned from both positive and negative experiences should also be incorporated into training.

Beyond these core competencies, individual agencies could still provide additional entry-level training that is relevant to their own entrants. It is essential that entry-level training include familiarization with the information sharing policies, procedures, and technologies with which entrants will be working, and that individuals master working collaboratively in a shared network environment. New entrants must view an ethic of teamwork as part and parcel of the business processes, guidelines, and tools of the information sharing environment.

The entry-level training course should be updated regularly to keep pace with new tools, methods, and other vital information. Graduates of entry-level training courses should be expected to update their skill sets through periodic recertification.

Generating and maintaining information sharing expertise across roles and functions
Analysts and collectors will need to build upon the common training they receive at job entry. Updated and higher-level training will be needed to maintain and improve proficiency for working within an information sharing environment. Intermediate- and senior-level joint education should be required at schools with interagency participation. As part of the curriculum, individuals, particularly those in supervisory positions, would be required to complete courses and demonstrate proficiency in advanced methods and tools; they would also be expected to communicate and interact effectively with policymakers and other consumers of information sharing environment products. The higher-level education curriculum would also be regularly updated. Moreover, students, teachers, managers, and graduates should systematically provide feedback on the efficacy of the training so that the overall educational system can remain relevant and effective.

In those predominantly law enforcement institutions in which non-specialists supervise collection and analysis staff—for example, the FBI special agents supervising intelligence analysts—special training for supervisors will be required. Additionally, selected members of congressional staff, the Congressional Research Service, and the GAO would benefit from familiarization with the common training that the information sharing environment community receives.

In addition to standard classroom instruction, national exercises, tabletop and field exercises, service rotations in other agencies, and other forms of cross-pollination are necessary for both training and team building. In fact, breaking down cultural barriers through common training and periodic cross-agency work assignments may be among the most important elements of making sure that the information sharing environment succeeds. The DNI would be responsible for a national-level exercise program, while the DHS would be responsible for a regular exercise program for regional and local players.

An education regime like this would be similar to the military education system. Military education, for officers in particular, combines specialty skills training with more general entry, mid-level, and senior schools—the latter two levels taking six to twelve months each, and required for advancement. Additionally, regular field and headquarters exercises supplement the schooling. The

medical profession, commercial pilots, and public school systems similarly require regular recertification. In the world of information technology, tools and methods of analysis change rapidly, and analysts and collectors need to stay up-to-date; the same is true in the study of terrorism.

Training should also cover privacy and fair information practices in the context of information collection and sharing. The concept of information privacy is easily misunderstood. Especially within the relatively closed environment of intelligence agencies, the most balanced and carefully written guidelines can be misinterpreted and misapplied in perverse ways, leading to a lack of respect for the values they are supposed to protect, and defeating the very goals they are intended to serve. Training, and dialogue with outside experts, can help avoid these negative dynamics.

Generating and maintaining information sharing expertise beyond the federal community
Most non-federal law enforcement entities do not require large counterterrorism elements, nor do they have the resources to fully support such efforts. The financial, personnel, and infrastructure requirements to develop a training program for state, local, and law enforcement agencies would be cumbersome for many jurisdictions if undertaken by individual agencies, or even if aggregated at the state level. The federal government, on the other hand, already possesses much of the infrastructure, training materials, and personnel to achieve the needed economies of scale. Consequently, Washington should bear some or all of the cost of setting up a program at training sites, at such places as the FBI training center at Quantico, the various Federal Law Enforcement Training Centers, or private-sector contract schools around the country. In addition, centrally-located training will build or enhance trusted networks among non-federal law enforcement officers.

Open source intelligence
Users of the information sharing environment must be trained to more readily use unclassified open source information. They must begin to view open source material as equivalent to the various types of intelligence or law enforcement sensitive information. Unclassified information should increasingly be the preferred form of information sharing, in particular for material which must be widely shared, including beyond the federal government.

Given the ever-present requirement for time-critical dissemination of information to a wide range of users, the objectives of low classification levels and ease of discovery and dissemination will be real and urgent. While guidance and standards may be disseminated from the center, analysis, like collection, will occur anywhere in the information sharing environment, and will be generally shared throughout the system. Network relationships expand knowledge and build trust, and the sharing of relevant information allows discovery, collaboration, and analysis to be carried out more efficiently and effectively.

Improving knowledge about threats by improving analytic capabilities
As the magnitude of the terrorist threat to the United States has grown in recent years, so has the requirement for the discoverability, sharing and analysis of terrorist-related information. In parallel, the intelligence and law enforcement communities have expanded and improved upon their analytic methods and techniques, drawing heavily on the approaches of other professions and disciplines. Unfortunately, the rich variety of analytic methods is seldom taught formally, and it is certainly not

taught across the entire and expanding range of users. As a result, on-the-job training remains the norm.

A commonly understood set of information sharing environment-wide analytic methods and techniques is essential to remedy this situation, and such a set of methods and techniques must be provided as part of the initial core training for analysts (see box.). In addition to training on common analytic methods, analysts should also be trained to methodically generate new ideas, conduct self-reviews, stress-test underlying assumptions, question judgments, and explore alternative outcomes.

TRAINING IN ANALYTIC METHODS

The methods and techniques—most of which are already in use in at least parts of the information sharing environment—that should be included in any baseline training in analytic methods:

Capabilities analysis seeks to examine the skills and capabilities of groups and individuals, as well as efforts to acquire those skills and capabilities.

Intelligence-target modeling provides a comprehensive and up-to-date description of intelligence targets. A target can be any object of interest, from an attack weapon to an attack target. Target models comprehensively describe what is known and not known about a target of interest, and outline alternative scenarios on how terrorists might use the target (e.g., acquire a weapon or attack a facility).

Pattern or trend analysis can be used to identify outliers and anomalies in information which can help in the triage of particularly large information sets of predicates (e.g., expired visas), and can help guard against an overemphasis on expected behavior.

Link analysis can be used to find obvious and non-obvious relationships between people that may warrant further scrutiny. Sometimes these relationships are represented visually with a network graph. In the representation, individuals and groups are depicted as nodes in a network, and relationships are represented as links between nodes. When using this technique in conjunction with a starting point (e.g., a known bad guy), and specific kinds of relationships (e.g., roommates), highly useful intelligence can be developed.

Temporal analysis looks at time-based relationships where events and activities are arranged in order of occurrence. Temporal analysis, combined with information on subjects of interest and their immediate network, may provide critical insight into detecting and preventing terrorist attacks.

Financial analysis has long been used as a tool against organized crime and drug trafficking, and it is now used to identify sources of terrorist financing. Financial analytic methods use link-analysis techniques to connect individuals and organizations through financial transactions.

Poll-based analysis can help in understanding the national and ethnic environment of terrorism. Poll information from around the world can help analysts better understand the attitudes and values of the societies in which various terrorist organizations exist.

Tools to identify the signal in the noise

The number of disciplines and substantive areas of investigation are too great for a single individual to master; the wealth of information too great for any individual or group to analyze quickly; and the short-fuse dissemination requirements too pressing to continue relying on antiquated information transfer systems. Better tools are essential.

Analysts are unlikely to adopt tools that require lengthy training, and they are likewise unlikely to use tools that do not clearly save time. Moreover, for some in the classified community, tools and software are regarded as a threat. While younger analysts, in general, may be more comfortable with exploring the use of new tools and applications, the information sharing environment cannot wait a generation for acceptance by the intelligence community; a risk exists that the skills of the younger generation will atrophy as its members become socialized within the existing system.

As with analysis, there has been a continuing effort in the intelligence community to develop and deploy ever-more diverse and powerful tools to aid in the discoverability, sharing and analysis of information and databases.[35] The intelligence community, as well as federal law enforcement and homeland security officials not already included in that community, should provide analysts with a baseline set of desktop productivity tools, including improved workspace organizers, instantaneous two-way translation, automated link analysis, automated entity extraction, report templates, directory integration (e.g., data directories, expert directories), and interactive training and simulation modules (see box.). This is especially important as a younger generation of intelligence professionals is more comfortable and adept with technology. Mechanisms should be established to solicit greater user input when developing and designing tools, and training and help-desk support for using the tools should be made widely available.

TOOLS TO IDENTIFY THE SIGNAL IN THE NOISE AND IMPROVE ANALYSIS AND COLLABORATION

Basic tools can improve the efficiency of the individual analyst, and also benefit joint analysis and collaboration. These tools include:

Workspace organizers that allow analysts to file copied material or notes from classified and unclassified sources, including from the Internet, in a single location. In addition, a workspace organizer would allow users to automatically incorporate links back to the source material. The

[35] The CIA has an Advanced Technology Programs office. The broader intelligence community has the Advanced Research and Development Activity office; the DoD has a Defense Advanced Research Projects Agency; and the DHS has its Homeland Security Advanced Research Projects Agency. These offices, among others, undertake projects that support the technology needs of their agencies, with much of the research and development contracted out to the private sector, where much of the innovation currently resides.

analyst could also annotate the information, assign categories for sorting or retrieval, and easily group the needed information for report writing. With the links back to the source material, footnotes and other forms of attribution could be easily added to the analysis. Such footnoting would give others the ability to probe the analysis for source credibility and overreliance on weak information. The workspace organizer could also automatically include a log of reports read, websites visited, and other activities which could be annotated by the analyst regarding usefulness of the information.

Machine bidirectional text translation capability for the non-linguist to search for and read documents in a foreign language. An automated translating capability would allow analysts to more quickly survey and read greater amounts of foreign-language information, even if the translations provided were far from perfect.

Multi-source and real-time link analysis that allows new information to be analyzed for relevance with little or no human intervention. Such a tool could recognize the importance of new information as it appears in various databases and notify the appropriate analyst when, where, and what new information exists.

Entity extraction from unstructured data allows systems and analysts to draw meaningful data points from various media or documents with little or no direct human intervention. This could produce the necessary data points to drive automated link analysis. Such a capability could also allow identification of themes in the media (or elsewhere) that are gaining prominence in countries or regions, as well as charting the intensity of such themes at points in time or over time. For example, the system could help detect growing or lessening animosity towards American troops deployed in a specific region.

Field report templates for use with laptop computers and personal digital assistants to organize field reports into data fields to expedite early reporting, enhance discovery and usability, and improve the timeliness and value of the data to the community at large.

Information directories that facilitate the discovery of available information. These directories will contain limited metadata (as needed to locate information) and pointers to the data holders. Anonymization may play a role here in the form of anonymized information directories to further enhance privacy as the risk of unintended disclosure is even further reduced.

Expertise location directories to allow analysts to find subject matter experts with minimal search requirements.

Training simulations can reinforce classroom training on analytic methods and tools by adding an interactive component that makes training seem more real. In particular, the simulations should include scenarios which require and reinforce collaborative efforts. This is a high-return area for development, as it would allow the propagation of common tools and techniques quickly and efficiently.

24-Hour help desk and regularly-updated online resources will be important features to support various aspects of human capital development for information sharing. Help-desk functions can be made available during training so that analysts can seek additional help and support as they undertake any form of training, either in-class or online, during entry-level or advanced training. A 24-hour help desk that provides assistance as analysts adjust to using new technology tools would also be useful. This help desk could assist with such questions as: "I have a fragment of a phone number found in pocket litter. What techniques might be available to make full use of it, or what resource is available to learn all of the possible name transliterations for this uncommon name?"

Community tools that allow collaboration within a virtual environment are becoming increasingly prevalent in consumer and business use. The intelligence community should seek to apply these emerging community tools—for example, blogs, wikis, social book marking—to promote innovative sharing and collaboration within the government.

Creating an Information Sharing Institute

Government and its contractors cannot provide all the expertise and capabilities required to address the various challenges associated with the information sharing environment. We therefore recommend the creation of an Information Sharing Institute that could make needed operational and professional expertise available when necessary beyond that which is available in the government in any particular agency, department or government contractor. This Institute would provide a mechanism to identify and distribute best practices, and to apply technologies available in other sectors. It should have the full and active participation of organizations from federal, state, and local governments as well as the private sector. In addition, it could help promote coordination of the necessary investment in research and development for new technologies needed to create a trusted information sharing environment.

Technologies that Support Policies and Processes to Connect People and Information

Developing a trusted information sharing environment requires designing and implementing a technical infrastructure and employing technologies that support policy goals. The architecture, technical applications, and features of the environment should provide opportunities for rules-based operation of systems in which the technology itself serves an important function to both enable appropriate, and constrain inappropriate, information sharing and usage. In this sense, technology is an important enabler of trust—providing assurance to participants, policymakers, and the public that information sharing conforms to governing policy.

Technology can be employed 1.) to improve the effectiveness of information sharing and analysis; 2.) to enhance the security of systems and shared information; and, 3.) to enforce privacy protections and provide accountability. This section describes certain technology developments

related to these functions. This section is not intended to be an exhaustive discussion of specific technology developments or current research or implementation activities; rather, it provides a brief overview of certain available technologies that have particular applicability to implementing a trusted information sharing environment. We recognize that many efforts are already underway in the government to adopt these tools for the counterterrorism mission. We urge that those efforts be expanded, be given coherence through the PM, and be sufficiently funded by the President and Congress.

Improving Information Sharing and Analysis with Technology

There are many technologies and tools currently available or under development through government initiatives, or in the private sector, that can improve information sharing and analysis. We focus here on technologies in five particular areas:

- data interoperability through metadata tagging;
- information discoverability through electronic directories;
- personalized collection and presentation tools;
- collaboration technologies; and
- anonymized information exchange and processing.

Data interoperability through metadata tagging

One of the principal goals of networked information sharing is to separate content from applications—i.e., to make information usable and interoperable across many applications and systems.[36] A major challenge in implementing trusted information sharing for national security and counterterrorism is how to integrate information from the myriad terrorism-related databases, each of which was constructed by a different agency for a different purpose in a different format using a different technology.[37] This problem is compounded when one considers the thousands of state, local law enforcement and private sector databases that may also contain relevant information, and may ultimately need to be integrated into a common environment.

Complete data interoperability—i.e., a system in which every data item could be exchanged and used in any application—would require that all information, including all legacy information, be presented in a common format. Since this is both impractical and technically impossible, other techniques are required to enhance sharing, and ensure that the right information gets to the right place.

---

[36] Network interoperability is another required feature of an effective information sharing environment. Network interoperability refers to making discrete networks able to exchange information. Network interoperability involves developing or translating between common transport protocols and making physical (whether wired or wireless) connections between networks. Recent migrations to TCP/IP-based networks have substantially enabled network interoperability. However, information interoperability still remains a challenge.

[37] See *Creating a Trusted Information Network for Homeland Security*, supra at 14: "Information 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 information sets."

One way to avoid having to use a common presentation or organization format for all information, applications, or information bases is to use data tags containing metadata—i.e., information about information—to separate content elements from presentation or structure. This allows different systems to recognize and process information appropriately in context. By using commonly agreed-upon information tags for categories of data elements,[38] systems can understand original context, and can then handle these exchanged information elements according to their own processing needs.

Commonly-available information exchange standards such as Extensible Markup Language (XML) allow categories of information to be tagged with agreed-upon names for each field. Many government initiatives have already been undertaken to develop common vocabularies in various domains. The DoD has developed the DoD XML model,[39] the intelligence community through the Intelligence Community Metadata Working Group has developed an intelligence domain model,[40] and the Department of Justice (DoJ) has successfully developed its Global XML Data model[41] for exchanging law enforcement information within the justice and law enforcement domains. In February 2005, the DoJ and the DHS executed a Memorandum of Agreement to create the National Information Data Exchange Model, which would extend the DoJ Global Justice XML Data Model to include the requirements for sharing information related to homeland security.[42]

The development of a comprehensive information sharing environment depends to a large degree on adoption—to the extent possible consistent with the protection of sources, methods, and activities—of a common XML standard for the retention, production, use, management, and sharing of terrorism information throughout the extended information sharing environment. To address these issues, the PM of the information sharing environment has established the Common Terrorism Information Sharing Standards Working Group for the Information Sharing Council[43] and has developed an interim plan "to develop and issue common standards for preparing terrorism information for maximum distribution, which provides common standards for all communities that affect easier user access, search and discovery, and knowledge extraction while maintaining security and privacy safeguards." The Task Force supports these efforts and urges that the President and the Congress to make funding and resources available to fully realize these goals.

Information discoverability through electronic directory services

As noted in earlier Task Force reports, employing directories of available resources, services, and information is a useful way to make information discoverable without having to actually exchange full data sets among every user. Searchable directories that allow information seekers to contact experts, call on resources, or find information relevant to their inquiries can improve effective information sharing, as well as contribute to security and protect civil liberties and privacy, by

---

[38] For simple example, the tags <NAME>Paris</NAME> or <CITY>Paris</CITY> could be used to distinguish the specific use of the information element "Paris".

[39] See DoD Metadata Registry at http://metadata.dod.mil/

[40] See Intelligence Community Metadata Working Group at https://www.icmwg.org/

[41] See Global Justice XML Information Model (Global JXDM) at http://it.ojp.gov/topic.jsp?topic_id=43

[42] See Press Release, http://www.niem.gov/pdf/20050307_press_release_dhs_doj_global_jxdm_exec_briefing.pdf

[43] See Information Sharing Environment Common Terrorism Information Sharing Standards Working Group, Task 2.1, Develop and Issue Common Standards for Preparing Terrorism Information, Existing Initiatives Report, April 13, 2006 , Draft Version 1.3. Available at http://colab.cim3.net/forum/sicop-forum/2006-04/doc00004.doc&e=42

minimizing the amount of actual information that needs to be shared. In many ways, knowing where relevant information is, or with whom it is, will be more important than having direct access to the information. Connecting information seekers with data stewards will result in increased collaboration and better analysis.

A fully developed information sharing environment, built on a distributed architecture, will have many directories covering different domains, each having different security and access requirements. However, for a fully integrated environment to function, such directories should be developed so that they are searchable or usable across domains by appropriately authorized users.[44]

The PM of the information sharing environment has begun implementation of the first phase of a fully integrated electronic directory service (EDS).[45] As contemplated by the PM, the EDS will eventually include searchable attributes of people, organizations, information, and services available throughout the network. The EDS will ultimately:

- be fully integrated into the information sharing environment;
- provide multiple EDS capabilities working together;
- support controlled access and sharing of information across security domains, consistent with applicable laws, regulations and policies;
- include technical framework and standards, business processes, and policies enabling integration and collaboration;
- include federated agreements for governance;
- include people, organizations, services, and information to support mission intelligence and information needs; and
- maintain security and privacy of information that may be useful to adversaries and competitors of the United States, the owners of the information (corporate, organizational, individual) and individual citizens.

The first phase of implementation contemplates development of a "people and organization" directory service (EDS-PO) described as:

> a set of registries that share a common, trusted and up-to-date view of people and organization information, which includes identification of necessary attributes, desired attributes and

[44] IRTPA specifically calls for the development of electronic directory services in the information sharing environment. IRTPA §1016(c)(2).

[45] In February 2006, the Program Manager released its Concept of Operations for Electronic Directory Services for the information sharing environment (available at http://www.ise.gov/docs/EDSPO-CONOPS.pdf) and in March 2006 released the Implementation Plan for the this phase (available at http://www.ise.gov/docs/EDSPOImpPlan.pdf).

> standardized metadata on people and organizations, to assist in locating in the Federal Government people with relevant knowledge about intelligence and terrorism information.[46]

The EDS-PO directory service will assist users of the information sharing environment to locate "people with relevant knowledge about intelligence and terrorism information."[47] Participants in the information sharing environment will be able to locate contact information in a manner analogous to the use of paper White, Yellow and Blue page telephone directories[48] (See Appendix 1 for more details).

In addition to these people and organization directories, the fully-developed information sharing environment will employ information and service directories to assist users in locating information or services directly. These directories may point users directly to relevant information or services. In some cases users will be able to directly access the information by following pointers from searchable indexes. In others, they will be directed to people or organizations that have custody over relevant information. They will then be able to initiate a process—electronically, it is hoped—to assert their authorized purpose for access, and eventually to get the information they seek.

Using directories will allow users to request specific information without a need to share the entire information base, thus cutting down on information overload and improving security and privacy protections by minimizing irrelevant information transfers.

In addition to facilitating access and enhanced sharing, directories, when coupled with user notification or alert functions, decision support tools, and collaboration tools can also greatly improve analysis and the production of analytic products.

Security of directories and controlling for inadvertent disclosure of classified or sensitive material through the directories themselves is required for assuring participant trust in the information sharing environment. Many technologies for developing and managing directories already exist, including technologies that can shield confidential information while still responding to queries. Other technologies allow directories to be queried but shield the query itself. In both cases, automated handling of queries can make appropriately authorized information owners, analysts, or monitors aware that information is required, and can allow for human or procedural intervention at that point.

The Task Force supports the efforts of the PM to develop electronic directory services, urges that the effort be expanded to fully include all potential participants, and calls on the President and the Congress to provide the funding and support for these efforts to go forward.

Personalized collection and presentation tools

Effective information sharing requires ensuring that the right information gets to the right person at the right time. However, a fully integrated information sharing environment will make vast

---

[46] Concept document, supra at 6.

[47] See IRTPA §1016 (c)(2).

[48] Concept document, supra at 7.

information volumes available, with the potential to overwhelm limited analytic resources. Information will expand geometrically as new participants come online, and individual information bases will continue to grow both in size (i.e., in number of records) and in dimensionality (i.e., in the number of fields or attributes relating to a particular subject). Under such circumstances, avoiding information overload will require using automated information management technologies to *personalize* information collection and presentation. Some of these technologies are described below.

Collection tools: subscription and automated search

Subscription tools allow users to subscribe to information or information sources that match their particular interests. A common example in the commercial context is the use of Real Simple Syndication (RSS) feeds. By making information available through RSS feeds, information providers enable information consumers to subscribe to those feeds that meet their specific needs. In the context of the information sharing environment, such feeds could be used, for example, to subscribe to directory services, updates, intelligence products, or individual analysts' blogs that would allow users to keep up with the latest expert knowledge.

In addition to subscription, other personalization tools include automated search technologies, allowing user-initiated search queries to be automatically updated; and system aware notifications, allowing information producers to automatically notify potentially interested persons. Many of these technologies already exist, or are being developed to manage information in commercial enterprise networks or in public networks like the Internet.

Presentation Tools: portals, dashboards and custom reporting

Personalization tools also allow for information to be presented contextually—i.e., in a manner relevant to the particular task or query. These kinds of personalization tools are widely used in commercial settings, for example, in customer relationship management (CRM) applications, for general content management, or for other applications and settings in which "just-in-time and relevant" information is key.

Portals, in which selected information sources or services are presented to the user through a single interface, or dashboards, in which users can select which sources or services they wish to access from their desktops, also have great potential for improving information access and analytic capabilities. For example, individual agencies can make proprietary information sources or services available, and users can pick and choose those that suit their particular needs. Likewise, portals can be used to deliver uniform sources and services to different classes of users (e.g., specialized information sources and services could be delivered to analysts working on weapons of mass destruction while others would be made available to analysts working on terrorist funding).

Portals are already widely used throughout government to make services available. Adapting these same technologies to provide custom sources and services to groups or individual users across department, agency, or unit boundaries will greatly enhance the effectiveness of the information sharing environment.

Collaboration technologies

It is beyond the scope of this report to discuss the many collaboration tools already in use or under development throughout government and the private sector. Many departments and agencies have developed specialized suites of collaboration tools to support their particular missions. For example, the Defense Information Systems Agency makes a Defense Collaboration Tool Suite available, which supports voice and video conferencing, document and application sharing, instant messaging, and whiteboard capability and that is certified for use on the Secret Internet Protocol Router Network (SIPRNet).[49] Also, we have already discussed how other technologies, for example directories, can lead to increased collaboration by making individuals and organizations aware of each others' interests. So too, we have mentioned systems awareness, through which monitoring of usage within the information sharing environment can actually create new knowledge by spotting aggregated interest or identifying emerging trends.

Notwithstanding the wealth of available options, we believe that there are other emerging technologies that are just beginning to gain the requisite attention in government information sharing initiatives, and that deserve greater support. In particular, we urge those charged with developing the information sharing environment to examine the utility of blogs, wikis, and social tagging technologies to enhance collaborative information sharing and analysis. Blogs are electronic journals in which experts in particular areas could publish their views for a wider community than traditional reporting lines or unit boundaries allow. Wikis are collaborative writing spaces in which many users can contribute so that the content reflects many points of view, thus allowing for the emergence of both consensus and dissent in potentially useful ways. Blogs and wikis have already been examined as potentially useful for intelligence analysis.[50] Social tagging (or social bookmarking) technologies allow individual users to tag information and make those tags available to others (or to the system) so that the aggregation of collective tags conveys collective intelligence. We urge making these kinds of technologies available within the information sharing environment be considered at the earliest stage possible.

Anonymized analysis and processing

The ability to analyze or process information in anonymized form is seen as a potentially useful way to allow greater information sharing and analysis while still protecting information security and confidentiality, thus protecting privacy and civil liberties as well. Anonymization has the potential to solve some of the privacy concerns that could become roadblocks to information sharing programs. Technologies are now available and being used commercially to reliably perform some forms of information matching and certain other analyses on anonymized information with little or no diminution in operational capability.[51] Anonymized information in this context is information that has been scrambled or encrypted so that it is not human readable, and so that the underlying information cannot be accessed without taking particular actions.

---

[49] See http://www.disa.mil/main/prodsol/dcts.html

[50] For a discussion of the use of these technologies for intelligence analysis, see Andrus, D. Calvin, "The Wiki and the Blog: Toward a Complex Adaptive Intelligence Community," *Studies in Intelligence*, (Sept. 2005), available at http://ssrn.com/abstract=755904

[51] For a general discussion of the use of anonymization technologies for counterterrorism, see James X. Dempsey and Paul Rosenzweig, "Technologies That Can Protect Privacy as Information is Shared to Combat Terrorism," *Legal Memorandum* (Heritage Foundation), (May 26, 2004), at 7-9.

Usually, information matching requires sharing entire information bases of clear-text information for one or the other party to run matches against. Even where information is encrypted for transport or storage, it is usually decrypted for processing. Alternatively, where unknown information relating to a specific subject is sought, it may require sharing confidential queries with the information base custodians. In many cases, these procedures are adequate, but, in others, they can raise significant operational or information security issues, or privacy and civil liberties concerns, particularly with large information sets that may include a great deal of sensitive or personally-identifiable information. Thus, for both security and privacy reasons, a method to accomplish anonymized information matching or querying, without revealing the underlying information, is required.

The emerging world of anonymized analytics provides a useful approach for particular applications. Using these technologies, it is now possible to anonymize certain confidential or sensitive (example.g., personally-identifiable) information using one-way hashing to scramble the information so that it is no longer human readable (and so that the process is not reversible) in a way that still allows the information to be compared and matched with other information scrambled in the same manner. Thus, matching can be accomplished without decrypting the underlying information. Should a match occur, a request to access the original unscrambled information relating only to that match can be made to the original information holder. Compliance with such a request would be subject to whatever policy governed disclosure of the underlying information—e.g., through certification of an authorized use, or compliance with legal processes, such as a National Security Letter, subpoena, or warrant—and would be recorded in a tamper-resistant log for monitoring or subsequent audit or review.

These anonymization techniques allow records to be compared in a manner that greatly reduces the risk that any party can learn anything other than what records have in common. Many government counterterrorism missions (e.g., airline safety measures) could use this kind of technology to determine which third party-information records (e.g., passenger records) match sensitive government-held information (e.g., terrorist watch lists) while protecting the security and confidentiality of the underlying information. Such techniques may also help address critical information sharing challenges, for example, the conflict between U.S. information needs and E.U. information-protection laws. The use of anonymized information may enable matching to be accomplished in a manner that the European Union would view as consistent with its laws.[52]

Anonymized information matching of non-standardized information can be accomplished by anonymizing standard information attributes (e.g., name, address, phone number, etc.) in both their original form (e.g., "Bob") and in their root or normalized form (e.g., both Bob and Bobby are also hashed and matched as "Robert").[53] Likewise, transposition errors (e.g., when the month and date are transposed), as well as common spelling errors, can be accounted for by creating and comparing plausible or common variants (e.g., 6/11/1972 will be matched as 11/6/1972). While this obviously expands the number of attributes for each subject, false positives can be reduced by requiring

[52] See Stewart Baker paper published at Steptoe & Johnson, *Anonymization, Information-Matching and Privacy: A Case Study,* http://www.steptoe.com/publications/279d.pdf.

[53] Thus, for example, such systems could match the 128 known spellings of Mohammed.

multiple attributes to be matched (depending on the application) in order to establish a definitive match.[54]

While these anonymized analysis techniques are not new, their application in commercially and operationally viable technologies is relatively recent. Several companies now offer technologies with such capabilities, and systems are being used in a variety of applications, for example, in monitoring network traffic for systems security purposes and in public health surveillance. It is expected that this market will continue to grow and that new applications will become available.

These techniques reduce the risk that the underlying information will be disclosed, misused, or repurposed while still allowing information to be matched and connected. This approach is consistent with the Task Force's recommendations that information be left with its original information stewards to the extent possible, and that the transfer of large information sets be minimized. Anonymized analytics enable users to seek (using legal mechanisms or other procedures where applicable) only those items from the original stewards of the information that are identified as matching the subject of interest.

By allowing for the selective revelation of underlying information only after some match has already been determined, these techniques provide an intervention point for authorization procedures to function. It is important to note that in many cases the process of the information steward's approval of transmission of clear-text versions of records identified through anonymized searching can be built into the business rules of the systems. In other cases, where particularly sensitive information (e.g., income tax records of U.S. Persons) is involved, there may be a need for human intervention before disclosure of these records. Even in these cases, however, we recommend that the decisions be facilitated, to the greatest degree possible, by real-time electronic communications.

These technologies are not useful for all applications and further research and development is required for expanded use. Nevertheless, these technologies are available, and offer significant advantages for privacy, security, and compliance with legal requirements for particular applications. The Task Force therefore recommends additional investment in the development and deployment of these technologies.

Enhancing System and Information Security with Technology

System and information security are important requirements of any system allowing access to sensitive or confidential information. In the complex distributed environment for information sharing contemplated here, such concerns are magnified.

In addition, systems and information security requirements are subject to specific laws, regulations, and directives. As a recent handbook on information security states:

---

[54] Particular architectures may be required to provide additional protections. For example, in some circumstances it may be necessary to separate the anonymizing technologies from the information center performing the analysis in order to avoid so-called "dictionary attacks." In other circumstances it may be appropriate for information matching or analysis to occur at a trusted third party. Particular architectures are circumstance- and threat-model dependent, and should be customized based on the sensitivity of the program, its scalability, and the security and accuracy required.

> The United States (U.S.) Congress and the Office of Management and Budget (OMB) have instituted a number of laws, regulations, and directives that govern establishment and implementation of federal information security practices. These laws, regulations, and directives establish federal- and agency-level responsibilities for information security, define key information security roles and responsibilities, identify minimum information security controls, specify compliance reporting rules and procedures, and provide other essential requirements and guidance. These laws and regulations place responsibility and accountability for information security at all levels within federal agencies, from the agency head to IT users. They also provide an infrastructure for developing and promulgating detailed standards and implementation guidance to the federal government agencies and overseeing implementation of required practices through the National Institute of Standards and Technology and the Government Accountability Office (GAO), respectively.[55]

We note also that systems and information security are no longer considered just technical issues with technology solutions; current security strategies in the private sector take an enterprise approach, and seek to align security practices with business processes and enterprise resilience planning to anticipate and respond to new emerging security threats. We urge the information sharing environment managers to take this same approach.

However, it is beyond the scope of this report to discuss systems and information security in any detail.[56] Nevertheless, we highlight here for policymakers a few particular issues relevant to developing a trusted information sharing environment.

Generally, ensuring systems and information security, including assurances that information is being used appropriately, by authorized users, and according to established policies, requires employing a layered security approach that includes at least:

- Authentication, authorization, and access control
- Systems-, application- and user-monitoring
- Data encryption (both for data in transit and at rest)
- Robust audit trails

We briefly discuss the first three of these features (access control, monitoring, and encryption) here, and the fourth (audit trails) in the section below.

---

[55] Information Security Handbook: A Guide for Managers, NIST Special Publication 800-100, Initial Public Draft (June 2006) available at http://csrc.nist.gov/publications/drafts/Draft-SP800-100_Handbook06-07-06.zip

[56] For additional information about systems and information security, see the Computer Security Resource Center of NIST at http://csrc.nist.gov/index.html; the Information and Computer Security Resource page at the SANS Institute at http://www.sans.org/resources/resources.php; and the resources available at the US-Computer Emergency Response Team web site at http://www.us-cert.gov/

Authentication, authorization, and access control

There are generally three distinct elements of the process for determining whether a particular user will be granted access to a system or resource: authentication, authorization, and access control.

1. *Authentication* means verifying that someone is who they claim they are. This may involve a username and a password, but can include any other method of demonstrating identity, such as the use of a smart card, security token, retina scan, voice recognition, or fingerprints. Authentication is generally determined by assessing something you have (e.g., a card or token), something you know (e.g., a password), or something you are (e.g., a biometric). Robust systems employ multi-factor authentication combining two or more of these methods. Authentication is the equivalent of checking your driver's license at the airport.

2. *Authorization* is determining if the user, once identified, is permitted to have access to the system, resource, or information. Authorization may be role-based, mandatory, or discretionary. In role-based systems, identities are assigned a role, and roles are granted privileges. In mandatory systems, certain privileges may always be denied or always granted to users. In discretionary systems, resource or information owners make discretionary decisions at the time of access request. Authorization is the equivalent of checking the guest list at an exclusive nightclub, or checking for your ticket when you reach the boarding gate.

3. Finally, *access control* is a more general way of describing the control of access to a system, resource, or information. Access may be granted or denied based on a wide variety of arbitrary criteria, which may or may not relate to the attributes of the particular user. For example, access may be granted (or denied) based on the network location of the user, the time of day, or the application being used for access. Access control is analogous to locking the door at closing time, or only allowing official vehicles or uniformed visitors access.

These three techniques are closely related in most applications, and an integrated system for identity management and access control will be required to ensure that information and system resources are adequately protected in an information sharing environment. To the extent possible, such a system will ensure that information is only accessed by authorized users, and only for limited purposes consistent with the "principle of least privilege" as discussed in earlier reports.[57]

One difficulty that should be noted is that authorization strategies are difficult to manage centrally in complex heterogeneous systems (like the contemplated information sharing environment), and thus require a federated approach to identity management -- one composed of trusted partners who reciprocally honor each others' grants and credentialing of authorization on the basis of some agreed minimum vetting standards. Federation, however, introduces a lowest-common-denominator risk: all partners are exposed to the least capable or least competent partner's security practices. Thus, systems monitoring, information encryption, and strong audit trails are required to supplement access controls.

[57] *Creating a Trusted Information Network for Homeland Security*, supra at 15.

Systems, application and user monitoring

Systems and information security cannot rely on access control alone because any perimeter breach provides access to all system resources or information. In addition, any authorized user with access to the network, applications or databases can engage in misuse or other unauthorized purposes. Thus, access control and user authentication strategies for information sharing environment security must be supplemented with automated intrusion detection systems, code scanners, and user monitoring to detect unauthorized uses, misuse or abuse.

Intrusion detection systems (IDS) can be host-based (i.e., they monitor system calls or logs on a particular host) or network-based (i.e., they monitor the flow of network packets). Robust IDS usually combine both of these approaches. Another important distinction is between systems that identify patterns of traffic or application data presumed or known to be malicious (misuse or pattern detection systems), and systems that compare activities against a normal baseline and detect deviations (statistical anomaly detection systems). Specialized detection systems can also monitor applications to detect whether they are functioning as expected. When an intrusion or anomaly is detected by an IDS, typical actions would be logging relevant information, generating a real-time alert to an administrator, or, in sophisticated systems, automatically revoking authorizations or isolating errant applications or users.

Likewise, user monitoring should be employed to monitor participants in the information sharing environment. User behavior should be measured against both objective (i.e., peer group norms and models) and subjective (i.e., previous or typical behavior for that user) behavior patterns. Monitoring should be dynamic and, to the extent possible, conducted in real-time. Furthermore, access authority itself should be limited (individuated to need according to the "principle of least privilege"), dynamic (subject to continuous updating based on new information), and technically easy to revoke or modify. System behavior can then be monitored for conformity to expectations, and authorizations adjusted accordingly.

Enterprise Security Management (ESM) systems provide the ability to perform correlation and analysis on internal and perimeter activities to monitor for inappropriate, incorrect, or anomalous activity within the system. ESM systems can correlate information from IDS, firewalls, authentication servers, routers and switches, and other network elements and applications to look for patterns that violate security policies.

Data encryption

Encryption is the process of obscuring meaning by encoding information (plain text) into unreadable cipher text (i.e., unreadable without special knowledge, for example, the decryption key). It is beyond the scope of this report to discuss cryptography in depth. [58] However, the Task Force recommends that, to the extent consistent with operational efficiency, all information in the information sharing environment should be stored and transmitted in encrypted form to protect against information loss, inadvertent disclosure, misuse, or abuse.

[58] For a detailed discussion of cryptography, see Bruce Schneier, *Applied Cryptography*, 2nd edition, Wiley 1996.

Facilitating Privacy and Accountability through Rules-Based Technologies

Technology can also play an important role in helping protect privacy and civil liberties by ensuring that information sharing systems conform to governing policy rules. In particular, information rights management (IRM) technologies can impose sharing and use limitations on information by invoking rules-based processing; and immutable logging, combined with monitoring and audit, can provide a mechanism for effective oversight, monitoring, and review of systems to make abuse difficult to accomplish and easy to discover.

Information rights management technologies

IRM technologies can enable policy rules to travel with information to enforce use rights wherever the information is used within the information sharing environment. IRM technologies involve information labeling that can occur either at the information record level through tagging, or through the use of a wrapper (i.e., software code that contains the information item or record). Labeling (whether direct or through use of a wrapper) then presents structure, metadata, and references to the processing application.

Labeling can be static (i.e., permanently assigned to the object) or synthetic (i.e., assigned by the server to the item when it is requested). The purpose of the label is to specify to some application the rules under which processing can occur. Encrypted wrappers can be used to maintain secrecy, except under specified conditions.

Thus, even if a data item is removed or copied to another information base, it retains relevant rules by which it must be processed within compliant systems. For example, a data item may be returned in encrypted form in which only subsequent processing under a warrant or pursuant to a security clearance is permitted. Alternatively, a particular data item may be labeled as belonging to a U.S. citizen or to a foreign national, or its original source labeled as from a particular government or commercial information base. In each case, different procedures developed to enforce particular policy decision and privacy concerns would apply in the data item's subsequent processing.

Challenges to labeling in a trusted information sharing environment include how to handle derived information (information that is itself the result of a query) and legacy information (preexisting information that has not been labeled). Possible solutions depend on research in program semantics technologies that interpret what the application requirements are at the time of access, and then label the information accordingly. For example, under the authorized uses standard discussed earlier, information might be labeled with its authorized use upon initial access. Any subsequent reuse of the information for another use or in another context (or even conceivably after the expiration of a set time period) would automatically invoke a call for certifying a new authorized use.

IRM technologies are becoming ubiquitous in commercial applications. A simple example is the rights management features available in Adobe or Microsoft document production environments in which copy, save, edit, and print privileges can be attached (or denied) to a document. IRM technologies are also related to digital rights management (DRM) technologies used to enforce intellectual property rights, and automated permissioning systems, like P3P, which are used to negotiate permissions between web browsers and web sites.

Robust audit trails through immutable logs[59]

To ensure compliance with rules-based processing and systems usage, audit and monitoring of logs is also required. Maintaining tamper-resistant logs of user activity in the information sharing environment will increase security, build trust among users, measure compliance with relevant policies and guidelines, and improve transparency and the ability to perform oversight by appropriate stakeholders outside of the system.

Immutable logs are tamper-resistant logs of user activity in the information sharing environment. Audit of immutable logs would allow authorized officials to trace the origin of a piece of information, who has accessed it, under what circumstances, pursuant to what authority, and how it actually has been used, thus providing a mechanism to oversee or measure compliance with privacy and security rules. As a mechanism for oversight and review of systems usage, immutable logs are a key component of accountability.

Another benefit of rich audit trails is the ability to track the related dependency of information, as we noted in the second Task Force report.[60] For example, if several analytic products used a common piece of information or source, and that information or source is later found to be inaccurate or unreliable, the logs could provide tracking information so that users of that information or source could be notified or updated. Additionally, log monitoring can provide real-time systems awareness by, for example, identifying common queries or emerging topics of interest, which can then foster collaboration or improve resource allocation by alerting users or system monitors that others are interested in the same information or topics.[61]

Immutable audit logs should be used to record activity that takes place on individual hosts or servers, as well as traffic over the network. Logged events could include, for example, authentication and log on procedures, queries made by users, tupples or database records returned to queries, authorized uses certified, information accessed, information flows between systems, and date and time markers for those activities.

Care, and appropriate security steps, must be taken so that audit logs do not themselves create new security vulnerabilities or points of attack. Use of encryption, ensuring that logs are never stored in a single location, strictly limiting access, and making monitor, review, or the audit of logs itself subject to logging should be required. If designed, used, and protected appropriately, the availability of robust audit logs will enhance accountability, demonstrate that information sharing complies with applicable laws and policies, help detect intrusions or policy violations, and contribute to building trust in system usage. Together with effective oversight, monitoring, and audit regimes, immutable logs can therefore play a vital role in enhancing participant, policymaker, and public trust in information sharing and analysis.

---

[59] This section is based on a background paper the development of which was led by Jeff Jonas and Peter Swire.

[60] *Creating a Trusted Information Network for Homeland Security*, supra at 16.

[61] Dempsey and Rosenzweig, supra at 11.

IMMUTABLE AUDIT SYSTEM DESIGN CONSIDERATIONS

Custodial solutions: distributed storage of logs. Various configurations for log custody can be devised to improve confidence that a log has not been altered, or to protect against the inadvertent disclosure of underlying information through the logs. A simple model to ensure against alterations would distribute copies of logs to multiple offsite storage facilities, thus assuring duplicate original files and requiring a multi-party conspiracy to alter logs. An alternative that would also protect against information disclosure would be to split transaction records into two or more parts, with each part sent to a different (or multiple) off-site location. In this scenario, multiple parties would have knowledge that a particular record exists but the collaboration of all such parties would be required to reveal the contents of any given record. Also, if one party deletes, alters, or loses its piece, the related pieces at the other locations would provide the necessary evidence that something was amiss.

Serialization and digital signatures. A primary goal of audit logs is to have a complete record of transactions, accompanied by an accurate date- and time-stamp for each. In the paper world, a standard tool for meeting this goal is to use a continuous roll of paper that logs each transaction sequentially at the time it occurs. The paper roll is tamper evident, because any missing transaction is physically apparent from a gap in the paper roll. In the shift to computerized recordkeeping, there are techniques for essentially reproducing the functionality of the continuous roll of paper. Electronic records can be digitally date- and time-stamped, to assure the integrity of the stamped record. In addition, records can be serialized by a system-generated counter and given a digital signature, which will show evidence of tampering if any information is subsequently altered.

Limited functionality hardware. Another way to mimic the paper roll is to use a write-once, read-many (WORM) storage drive that is designed so that information cannot be altered once it is written to disc. WORM drives are slower than other storage devices and thus may burden functionality in high transaction systems.

The Limits of Technology

Technology alone cannot ensure that the information sharing environment is effective, secure, or protective of privacy and civil liberties. However, by designing systems and employing technologies with features that support policy requirements, information sharing environment designers can help foster trust that technical systems and their users are conforming to governing laws, rules, and guidelines.

Because technology development is dynamic, however, it is incumbent on those charged with developing the information sharing environment to adopt, and adapt to, new technologies and techniques as they become available. The most difficult fact for government information initiatives to embrace is that technology development is iterative and indeterminate, requiring constant reevaluation of desired outcomes and available opportunities.

Conclusion

Effective information sharing is an important priority to improve national security and prevent terrorism. Yet, despite repeated efforts by the President, the Congress, and others, information sharing among federal agencies appears to be lagging, and sharing with state and local authorities and the private sector is even further behind. It is fair to say that without information sharing, we do not know what we know. The consequences for our national security are serious, and seriously harmful.

For information sharing to succeed, there must be trust—the trust of government providers and users of information, of policymakers, and most importantly, of the public. Each of these must trust that information is being shared appropriately, consistent with law, and in a manner protective of privacy and civil liberties. Building trust requires strong leadership, clear laws and guidelines, and advanced technologies to ensure that information sharing serves important purposes and operates consistently with American values.

Trust is essential for three fundamental reasons. First, a lack of trust will prevent the information sharing necessary to protect our national security. Second, a lack of trust will prevent the administration and Congress from giving information sharing the support and funding it requires. And third, a lack of trust will prevent the necessary public support that is required for success. Without trust, we will be less safe.

Respect for privacy and other civil liberties, and adherence to the law, are core obligations of a democratic government, even when the nation faces grave threats. This report has called for enhancing the ability of government to share information appropriately within a strong, but flexible framework of law, guidelines, and oversight, with both institutional and organizational checks and balances built around a broad consensus achieved, to the extent possible, through open debate and transparent procedures. Such an integrated information sharing environment and policy framework, properly designed and implemented, will empower officials to act swiftly and confidently, but within democratic accountability, to mobilize information to help prevent future terrorist attacks.

Appendix 1

Overview of Major Developments towards Establishing an Information Sharing Environment

Since the Markle Foundation Task Force issued its second report in December 2003, the federal government has moved forward in the process of developing the Task Force's concept of a decentralized and horizontal environment of information sharing to prevent terrorism. This appendix provides an overview of major developments since 2003.

The Markle Foundation Task Force's recommendation for a trusted information sharing network resonated with other organizations, government officials, academics, and experts in related fields. The 9/11 Commission lauded the Task Force's "outstanding conceptual framework," and recommended, integrating the Task Force's findings, that the President lead a "government-wide effort to bring the major national security institutions into the information revolution . . . [and] to create a 'trusted information network' based on a decentralized network model."[62] The Commission also shared the Task Force's principle of the importance of the President determining guidelines to "safeguard the privacy of individuals about whom information is shared."[63] Informed by the Task Force's concept of a decentralized, networked national security framework—with particular emphasis on promoting information sharing—the 9/11 Commission made a series of recommendations to reorganize intelligence in July 2004.

The President agreed with many of the Markle Foundation Task Force's and 9/11 Commission's recommendations, and on August 27, 2004, issued a series of Executive Orders restructuring management of the federal government's intelligence operations, and of the ways in which intelligence information is shared and used.[64] These Executive Orders and Homeland Security Presidential Directives (HSPDs) effectively mandated information sharing in the national security community. They responded to the Commission's recommendation for a "trusted information network" to be modeled upon the Markle Foundation Task Force's concept and assigned information sharing responsibilities to particular offices and set up an Information Systems Council to develop a concrete plan for information sharing.

In addition, in December 2004, Congress passed the Intelligence Reform and Terrorism Prevention Act (IRTPA), which made sweeping changes to the U.S. intelligence community, including by creating the new post of Director of National Intelligence (DNI) to oversee all intelligence

---

[62] National Commission on Terrorist Attacks on the United States, *9/11 Commission Report* (2004), at 418-419.

[63] Id. at 394.

[64] In addition to the Executive Orders discussed in the text, see Amendment of Executive Orders, and Other Actions, in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security, Executive Order No. 13286 Federal Register 10619 (Mar. 5, 2003) (directing the National Infrastructure Advisory Council to provide guidance to the Secretary of Homeland Security on how to foster information sharing); National Counterterrorism Center, Executive Order No. 13354, Federal Register 53589 (Sept. 1, 2004) (creating the National Counterterrorism Center to integrate information from multiple intelligence sources); Strengthened Management of the Intelligence Community, Executive Order No. 13355 Federal Register 53593 (Sept. 1, 2004) (calling for improved procedures for information sharing among the intelligence community); and Continuation of Certain Federal Advisory Committees and Amendments to and Revocation of Other Executive Orders, Executive Order No. 13385 Federal Register 57989 (Oct. 4, 2005) (updating authorities of the National Infrastructure Advisory Council). See, generally, Peter P. Swire, "Privacy and Information Sharing in the War on Terrorism," forthcoming in the *Villanova Law Review*.

operations in the federal government.[65] The Act also created the National Counterterrorism Center (NCTC) to serve as the primary federal agency for "analyzing and integrating all intelligence possessed or acquired by the United States Government pertaining to [foreign] terrorism and counterterrorism."[66] On the subject of information sharing, the IRTPA added more conceptual depth to the information sharing provisions from the White House, integrating the attributes of a decentralized and trusted information sharing environment the Markle Foundation Task Force had recommended. The IRTPA mandated creation of an "information sharing environment" and attempted to address the cluster of technical, political, cultural, and organizational issues that complicate information sharing in the national security community.

In studying these reforms, the WMD Commission concluded that the IRTPA's information sharing provisions set up confusing lines of authority, leaving it unclear who is primarily responsible for information sharing. The Commission proposed several adjustments to improve the legislation, such as requiring that the Program Manager (PM) for the information sharing environment (a position that the IRTPA established, but did not place in any particular office or agency) report to the DNI. The Commission also recommended expanding the information sharing environment to include all information related to national security rather than just terrorism information. On June 29, 2005, the White House endorsed 70 of the Commission's 74 recommendations.

Both the WMD and 9/11 Commission members have continued to push for the implementation of their recommendations. Nonetheless, implementation is proceeding too slowly in their view, hindered by missed deadlines and bureaucratic turf wars. They have argued that successful implementation will depend in large part on the strength and determination of the DNI as he struggles to overcome entrenched interests and manage a newly refashioned, decentralized intelligence community.

The 9/11 Commission's Recommendations

In its July 22, 2004 report, the 9/11 Commission highlighted specific gaps in information sharing that impeded the national security community before September 11, and endorsed the Task Force's concept of a trusted information network.[67] The Commission recommended that the President determine the guidelines for information sharing among government agencies, and between those agencies and the private sector. To engender the trust required for effective information sharing, it called on the President to protect the privacy and civil liberties of individuals about whom information is shared. It suggested the creation of a new position, a National Intelligence Director, to, among other things, set common information sharing and information technology policies that will maximize the flow of information among the disparate elements of the intelligence community. To bridge the foreign-domestic intelligence divide, the Commission recommended establishing a National Counterterrorism Center.

---

[65] Pub. L. No. 108-458, § 1011(a), 118 Stat. 3638, 3644 (codified at 50 U.S.C. § 403-1).

[66] Id. § 1021, 118 Stat. 3673 (codified at 50 U.S.C. § 404o).

[67] National Commission on Terrorist Attacks on the United States, *9/11 Commission Report* (2004), at 416-419, available at http://www.gpoaccess.gov/911/.

The Commission also reiterated the Task Force's emphasis on shifting from a *need-to-know* to a *need-to-share* culture of collaboration through incentives for horizontal communication networks within and across agencies. Recognizing the tension between information security and information sharing, it advocated the Task Force's strategy of simultaneously empowering and constraining officials through information rights management and practical policy guidelines. The President, it said, should lead a government-wide effort to establish a trusted information network among the major national security institutions. This effort should ensure that technological and organizational structures would be fully modernized, decentralized, and adapted to address national security threats in the information age.

The Executive Orders and Homeland Security Presidential Directives

The Bush Administration followed these recommendations with four Executive Orders and two HSPDs issued on August 27, 2004, which collectively mandated information sharing in the national security community. The policy set forth in Executive Order 13356, Strengthening the Sharing of Terrorism Information to Protect Americans, states:

> To the maximum extent consistent with applicable law, agencies shall, in the design and use of information systems and in the dissemination of information among agencies:
>
> (a) give the highest priority to (i) the detection, prevention, disruption, preemption, and mitigation of the effects of terrorist activities against the territory, people, and interests of the United States of America, (ii) the interchange of terrorism information among agencies, (iii) the interchange of terrorism information between agencies and appropriate authorities of States and local governments, and (iv) the protection of the ability of agencies to acquire additional such information; and
>
> (b) protect the freedom, information privacy, and other legal rights of Americans in the conduct of activities implementing subsection (a).[68]

To implement this policy, Executive Order 13356 requires the intelligence community, now headed by the DNI, to establish common standards for the sharing of terrorism information.[69] These standards will govern information sharing among agencies in the intelligence community itself, as well as with others involved in counterterrorism, including state and local governments. The Executive Order lists several methods that echo the Task Force's information sharing proposals, including widening access to information through classification on a tearline basis, using metadata to make information more manageable and shareable, relaxing strict originator controls, and creating specific incentives for sharing information. The order also requires the establishment of Executive Branch-wide collection and sharing requirements, procedures, and guidelines for terrorism information to be collected within the United States, including publicly available material. Finally,

---

[68] Strengthening the Sharing of Terrorism Information to Protect Americans, Executive Order No. 13356, Federal Register 53599 (Sept. 1, 2004), available at http://www.whitehouse.gov/news/releases/2004/08/20040827-4.html.

[69] "Terrorism information" is defined as that which "relates to" foreign, international or transnational terrorist groups or individuals, providing an important limit on the kinds of information that can be part of a shared information environment, and thereby enhancing public trust that information unrelated to terrorism will not be brought into the system.

the Executive Order sets up an Information Systems Council, chaired by a designee of the Director of the Office of Management and Budget. The Council's mission is to plan and oversee the development of an interoperable terrorism information sharing environment to facilitate automated sharing of terrorism information.

The other three Executive Orders of August 27, 2004 also flow from the 9/11 Commission's recommendations. Executive Order 13355 grants more power to the intelligence community head, including over funding, and tasks the position with establishing efficient information collection and sharing procedures, as well as standards and qualifications for persons engaged in the performance of United States intelligence activities.[70] Executive Order 13354 creates the NCTC, responsible for analyzing and integrating all intelligence pertaining to terrorism and counterterrorism, except purely domestic counterterrorism information.[71] As the successor of the Terrorist Threat Integration Center (TTIC), the NCTC is to serve as a central, shared knowledge bank on current terrorist threats. In addition, the NCTC is to be responsible for "strategic operational planning." Executive Order 13353 establishes the President's Board on Safeguarding Americans' Civil Liberties to ensure that civil liberties and information privacy rights are fully protected in the new national security framework.[72]

The HSPDs of August 27, 2004 provide for more narrowly-targeted information sharing, focusing on terrorist-related screening procedures and common identification standards for federal employees and contractors. HSPD-11 calls for an enhancement of terrorist-related screening through comprehensive, coordinated procedures to detect, track, and interdict threats to homeland security, including potential terrorists and suspicious cargo.[73] It builds on HSPD-6, Integration and use of Screening Information to Protect Against Terrorism, which established the Terrorist Screening Center to facilitate searching in a consolidated Terrorist Screening Center Database. HSPD-12 requires a mandatory, government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and contractor, which is expected to increase the flow of trusted information.[74]

The Intelligence Reform and Terrorism Prevention Act

The IRTPA, adopted in December 2004, further develops the information sharing provisions contained in the Executive Orders. In particular, Section 1016 on Information Sharing tasks the President with creating an information sharing environment for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy

---

[70] Strengthened Management of the Intelligence Community, Executive Order No. 13355, Federal Register 53593 (Sept. 1, 2004), available at http://www.whitehouse.gov/news/releases/2004/08/20040827-6.html.

[71] National Counterterrorism Center, Executive Order No. 13354, Federal Register 53589 (Sept. 1, 2004), available at http://www.whitehouse.gov/news/releases/2004/08/20040827-5.html.

[72] Establishing the President's Board on Safeguarding Americans' Civil Liberties, Executive Order No. 13353, Federal Register 53583 (Sept. 1, 2004), available at http://www.whitehouse.gov/news/releases/2004/08/20040827-3.html.

[73] Homeland Security Presidential Directive-11: Comprehensive Terrorist-Related Screening Procedures, available at http://www.whitehouse.gov/news/releases/2004/08/20040827-7.html.

[74] Homeland Security Presidential Directive-12: Policy for a Common Identification Standard for Federal Employees and Contractors, available at http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html.

and civil liberties.[75] The IRTPA empowers the President to determine the organizational management structure and policy framework to govern the new information sharing environment. Incorporating federal, state, local, and tribal authorities as well as the private sector where appropriate, the information sharing environment will be a decentralized, distributed, and coordinated environment that:

- connects existing systems, where appropriate, provides no single points of failure, and allows users to share information among agencies, between levels of government, and, as appropriate, with the private sector;
- ensures direct and continuous online electronic access to information;
- facilitates the availability of information in a form and manner that facilitates its use in analysis, investigations, and operations;
- builds upon existing systems capabilities currently in use across the government;
- employs an information access management approach that controls access to data rather than just systems and networks, without sacrificing security;
- provides directory services, or the functional equivalent, for locating people and information;
- incorporates protections for individual privacy and civil liberties; and
- incorporates strong mechanisms to enhance accountability and facilitate oversight, including through the use of audits, authentication, and access controls.[76]

The IRTPA designates the new position of PM outside of the intelligence community to plan and oversee the implementation of the information sharing environment. Responsible for terrorism information sharing across the federal government, the Program Manager will develop policies, rules, and procedures to govern the operation of the information sharing environment in consultation with the Information Sharing Council (ISC) (the new name for the Information Systems Council from Executive Order 13356). Section 1016 also sets up a schedule for implementation of its provisions and submission of performance management reports.

Perhaps the most significant IRTPA innovation—which affects information sharing, among other things—is the creation of the position of Director of National Intelligence, or DNI. The 9/11 Commission had recommended creating this position (although they called it National Intelligence Director). Responsible for managing the intelligence community, the DNI is appointed by the President with the advice and consent of the Senate. Among his primary duties is to ensure information sharing in the community. To that end, IRTPA empowers him to:

---

[75] Intelligence Reform and Terrorism Prevention Act, Pub. L. No. 107-296, § 1016 (b)(1)(A), 116 Stat. 2135.

[76] Id. § 1016 (b)(2).

- establish uniform security standards and procedures;
- establish common information technology standards, protocols, and interfaces;
- ensure development of information technology systems that include multi-level security and intelligence integration capabilities;
- establish policies and procedures to resolve conflicts between the need to share intelligence information and the need to protect intelligence sources and methods;
- develop an enterprise architecture for the intelligence community and ensure that elements of the intelligence community comply with such architecture; and
- have procurement approval authority over all enterprise architecture-related information technology items funded in the National Intelligence Program.[77]

With new budget and personnel authorities, the DNI is empowered to establish national intelligence centers to address intelligence priorities as they arise, with the requirement that each center share information with the rest of the community.[78] The IRTPA locates the NCTC, created by Executive Order 13354, in the DNI's office, where it is to serve as an information sharing center for counterterrorism efforts. The director of the NCTC is required to manage the effective integration of counterterrorism intelligence and operations across agency boundaries, both inside and outside the United States.[79] IRTPA enhances the information sharing role of the Federal Bureau of Investigation (FBI) as well, requiring its Director to submit annual reports on the progress of the Bureau in implementing information sharing principles.[80] IRTPA requires the Department of Homeland Security to develop an advanced passenger prescreening system that would enable comparisons with a consolidated and integrated terrorist watch-list maintained by the federal government.[81]

To encourage public trust in government intelligence and information sharing efforts, IRTPA establishes a Privacy and Civil Liberties Oversight Board, building on the board that Executive Order 13353 created. Among the Board's responsibilities is reviewing proposals for information sharing guidelines and monitoring their implementation.[82] Section 1062 also indicates the responsibility of Congress to establish privacy and civil liberties officers in all relevant departments; one such officer is explicitly required in the office of the DNI. In the development and use of the information sharing environment, Section 1016 requires the President to issue guidelines that protect privacy and civil liberties, which are to be made publicly available for review if possible.

---

[77] Intelligence Reform and Terrorism Prevention Act, Pub. L. No. 107-296, § 102 A(g).

[78] Id. § 1023.

[79] Id. § 1021.

[80] Id. § 2001(g)(4).

[81] Id. § 4012.

[82] Id. § 1061.

The WMD Commission's Recommendations

In its March 31, 2005 report, the WMD Commission reviewed the progress made toward information sharing and offered suggestions to improve upon the IRTPA. Based on its study of Iraq, it concluded that important intelligence was still not passed 1.) from the collectors to the analysts; 2.) from the analysts to the collectors; and, 3.) from foreign liaison services to the intelligence community.[83] Like the Task Force, the WMD Commission highlighted the bureaucratic turf wars and confusion that have resulted from the creation of the NCTC, focusing on competition with the CIA Counterterrorist Center and uncertainty over roles and responsibilities. Although the NCTC has pooled information about terrorism, it has not expanded into other intelligence areas, such as counter-proliferation. There is currently no single entity in the intelligence community, the Commission stated, with the responsibility and authority to impose a centralized approach to sharing information.[84] Still, the Commission noted that information sharing in general has improved since 9/11, especially through the use of consolidated terrorist watch-lists at the Terrorist Screening Center and the NCTC's integration of analytic perspectives from the entire intelligence community.[85]

The Commission believed the IRTPA's requirements for the information sharing environment were unworkable, and offered a number of suggestions for improvement.[86] While the DNI is responsible for all information sharing within the intelligence community, the Commission pointed out, the Program Manager is responsible for creating the information sharing environment itself—an integrated, government-wide framework for sharing only terrorism information. The Commission recommended that:

> The confused lines of authority over information sharing created by the intelligence reform act should be resolved. In particular:
>
> - The Information Sharing Environment should be expanded to encompass all intelligence information, not just terrorism intelligence;
>
> - The Director of the National Counterterrorism Center should report to the DNI on all matters relating to information sharing; and
>
> - The overlapping authorities of the DNI and the Program Manager should be reconciled and coordinated—a result most likely to be achieved by requiring the program manager to report to the DNI.[87]

Furthermore, recognizing the importance of protecting sources and methods, the Commission argued that one position should be responsible for information sharing, information technology, and

---

[83] WMD Commission, *Report to the President of the United States* 177 (March 31, 2005), available at http://www.wmd.gov/report/

[84] Id. at 288.

[85] For information about the bureaucratic battles resulting from the NCTC's creation, see id. at 288. The Commission's overview of improvements in information sharing begins on page 282.

[86] See id. at 432-445 for more detailed explanations of these recommendations.

[87] Id. at 432.

information security—a Chief Information Management Officer (CIMO) within the DNI's office. The Commission suggested that making one position responsible for balancing the competing priorities of information security and information sharing—as well as establishing performance metrics and self-enforcing milestones for the information sharing environment—would lead to a better system overall. The Commission also agreed with the Task Force about the importance of making communications among participants in the information sharing environment flexible and two-way by encouraging more inclusive directory services, such that where sensitive information is restricted to a limited group of users. The information sharing environment should ensure that others searching for such information are aware of its existence and provided with a point of contact who can decide quickly whether to grant access.[88]

Another major area for improvement in information sharing is the incorporation of non-federal actors into the information sharing environment. The Commission stated that there is still no comprehensive policy or program for achieving the appropriate balance regarding what terrorism information to provide state, local, and tribal authorities and how to provide it. .These authorities typically are deluged with information which they are neither equipped nor trained to process, prioritize, and disseminate.[89] The DNI and CIMO should be responsible for establishing information sharing standards to incorporate these important actors. The Commission did not devote much attention to the challenge of integrating private sector actors into the information sharing environment, however.

Overall, the Commission found that the most fundamental obstacle to effective information sharing has been the absence of empowered, coherent, and determined community leadership and management.[90] The Commission agreed with the Intelligence Community Inter-Agency Information Sharing Working Group that "[a] great deal of energy…is being expended across the [intelligence community] to improve information sharing. However, the majority of these initiatives *will not produce the enduring institutional change required to address our current threat environment*."[91] The Commission therefore advocated increasing the DNI's powers and responsibilities to bring about the enduring institutional changes that are most needed for effective information sharing.

On June 29, 2005, the White House endorsed 70 of the WMD Commission's 74 recommendations, including the creation of a National Counter Proliferation Center (NCPC) and a National Security Service within the FBI that will specialize in intelligence and other national security matters. Like the NCTC, the NCPC will be under the DNI's control, and the FBI's National Security Service will respond to priorities set by the DNI. The recommendations generally consolidate the DNI's power, giving the office expanded budget and management authorities with respect to the FBI and a staff of mission managers to develop strategies for specific intelligence areas. Other recommendations that the administration supported include *pushing* for more congressional oversight of the intelligence community and creating a new Assistant Attorney General position to centralize responsibility for

---

[88] For the Commission's rationale on the need for a Chief Information Management Officer, see id. at 436, and for information about the importance of two-way communications and directory services, see id. at 439.

[89] Id. at 287 (emphasis added).

[90] Id. at 320.

[91] The intelligence community Inter-Agency Information Sharing Working Group's conclusion is discussed and quoted in id. at 431.

intelligence and national security matters into a single office at the Justice Department. At the CIA, the reforms set up a center to focus on collecting open source intelligence and make the CIA Director in charge of all overseas human intelligence carried out by government operatives.[92]

In addition to implementing these recommendations, the President issued Executive Order 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans, in October 2005 to underscore the ongoing importance of terrorism-related information-sharing. That Executive Order implemented many of the information sharing requirements of the IRTPA and also revoked Executive Order 13356. It required federal agencies, when designing and implementing information systems, to give the highest priority to ". . . (ii) the interchange of terrorism information among agencies; (iii) the interchange of terrorism information between agencies and appropriate authorities of State, local, and governments, and between agencies and appropriate private sector entities; and (iv) the protection of the ability of agencies to acquire additional such information."[93] It also reiterated the requirement that agencies protect the freedom, information privacy, and other legal rights of Americans when doing so.[94]

In December 2005, the President reiterated these requirements in a memorandum to the heads of Executive departments and agencies on Guidelines and Requirements in Support of the information sharing environment[95] and established the information sharing environment requirement to implement common standards across all agencies regarding the acquisition, access, retention, production, use, management, and sharing of information.[96]

Implementation

Director of National Intelligence

The federal government has implemented a number of the information sharing provisions established in the year following the release of the 9/11 Commission's report. In February 2005, President Bush nominated the former Ambassador to Iraq and career Foreign Service Officer, John Negroponte, to become the nation's first DNI. Confirmed by the U.S. Senate on April 21, Negroponte was joined by Lt. Gen. Michael Hayden as his Principal Deputy Director of National Intelligence (Principal DDNI), until Hayden was confirmed as the Director of the CIA in May 2006.[97] The post of Principal DDNI is currently vacant. At the press conference announcing

---

[92] For information about the White House's endorsement of the WMD Commission's recommendations, see White House Fact Sheet: Bush Administration Implements WMD Commission Recommendations (June 29, 2005), available at http://www.whitehouse.gov/news/releases/2005/06/20050629-3.html; "White House Embraces Intelligence Changes," *CNN.com* (June 29, 2005), available at http://www.cnn.com/2005/POLITICS/06/29/intelligence.commission.ap/; and Douglas Jehl, "Bush to Create New Unit in FBI For Intelligence," *New York Times*, (June 30, 2005).

[93] Further Strengthening the Sharing of Terrorism Information to Protect Americans, Executive Order No. 13388, § 1(a), 70 Federal Register 62023 (Oct. 25, 2005).

[94] Id. § 1(b).

[95] Memorandum from the President to the Heads of Executive Departments and Agencies on "Guidelines and Requirements in Support of the Information Sharing Environment" (Dec. 16, 2005).

[96] Id.

[97] Katherine Shrader, "Senate confirms Hayden as CIA chief." *Associated Press (*May 26, 2006), available at http://www.baltimoresun.com/news/nationworld/bal-hayden0526,0,4996914.story?coll=bal-home-headlines.

Negroponte's nomination, the President reiterated the DNI's role as his principal advisor on intelligence matters. In addition to managing the overall intelligence budget, Negroponte will have the authority to order the collection of new intelligence, ensure the sharing of information among agencies, and establish common standards for the intelligence community's personnel.[98]

In addition to the Principal DDNI, there are four other DDNI's, each representing an important part of the intelligence process: customer outcomes, analysis, collection, and management.[99] More importantly for the purposes of information sharing, the ODNI's Chief Information Officer (CIO), Dale Meyerrose, has taken up a critical role in furthering information sharing within the intelligence community.

Program Manager and Information Sharing Council

In mid-April 2005, the President appointed John Russack, former Intelligence Director for the Department of Energy, to be the first information sharing environment's Program Manager tasked with terrorism information sharing across the federal government.[100] The White House aimed to clarify the relationship between Russack as Program Manager and the DNI in a memorandum issued June 2, 2005.[101] Following the WMD Commission's recommendation, the memorandum places the Program Manager within the ODNI, which shall exercise authority, direction, and control over the Program Manager and ensure that the Program Manager carries out the functions listed in Section 1016 of IRTPA. John Russack resigned on January 26, 2006, just 17 days after delivering his Interim Implementation Plan. Since then he has been succeeded by Ambassador Thomas McNamara, who heads an office that, as of May 2006, had 15 federal employees.

McNamara testified in May 2006 before Congress[102] where he stated that the information sharing environment must accomplish four key things:

- [It] must facilitate the establishment of a trusted partnership between all levels of government, the private sector and foreign partners to mitigate the effects of terrorism;
- [It] must promote an information sharing culture that eliminates information gaps between partners and facilitates the creation and sharing of validated actionable information;
- [It] must function in a decentralized, distributed, and coordinated manner;
- [It] must be developed and deployed incrementally by leveraging existing information sharing capabilities and deploying centralized core functions and services.

---

[98] White House Press Release. President Holds Press Conference announcing nomination of John Negroponte (Feb. 17 2005), available at http://www.whitehouse.gov/news/releases/2005/02/20050217-2.html.

[99] Office of the Director of National Intelligence (June 12, 2006), available at http://www.dni.gov/aboutODNI/organization.html

[100] White House Press Release. Personnel Announcement (April 15, 2005), available at http://www.whitehouse.gov/news/releases/2005/04/20050415-6.html.

[101] White House Memorandum for the Heads of Executive Departments and Agencies (June 2, 2005), available at http://www.whitehouse.gov/news/releases/2005/06/20050602-9.html.

[102] Thomas McNamara, testimony before the House Homeland Security Subcommittee on Intelligence, May 10, 2006.

In addition to the functions from the IRTPA, Executive Order13388 of October 25, 2005 also designates the PM as the head of the new Information Sharing Council (ISC).[103] The ISC was originally established as the Information Systems Council following the Executive Orders of August 27, 2004.

The original Information Systems Council was tasked to draft a plan for an interoperable terrorism information sharing environment; its objective remained the same after it was renamed. The WMD Commission later expressed concern that the ISC's initial plan lacked specific quantitative metrics by which to measure success or failure over time. In the Commission's view, the ISC had defaulted to consensus, leading it to settle on only a "plan to make a plan."[104]

The new ISC currently consists of members of 17 different government agencies, and facilitates coordination with state, local and tribal officials through a State, Local and Tribal Subcommittee. Its mission is to provide advice and information concerning the establishment of an interoperable terrorism information sharing environment to facilitate automated sharing of terrorism information.[105]

In June 2005, the information sharing environment PM issued his Preliminary Report on the Creation of the Information Sharing Environment, followed in January 2006 by his Information Sharing Environment Interim Implementation Plan. These documents recognized the failures in information sharing that contributed to the September 11, including instances in which potentially useful information was 1.) available but no one knew to ask for it; 2.) distributed only in compartmented channels; or, 3.) requested but withheld due to a determination that sharing was not permitted.[106] The 2006 report acknowledged that the current information sharing environment is not as integrated, interconnected, or robust as the nation requires, and that information about terrorists and their plans remains fragmentary.[107] The report promised a comprehensive implementation plan for the information sharing environment by July 2006.

On March 31, 2006, the PM and the ISC released their implementation plan for an initial capability for the information sharing environment electronic directory services (EDS) within a classified environment (following a February release of the Concept of Operations). The approach to EDS appears to be incremental, starting first at the federal level to provide directory services information within a classified environment; and then eventually creating the capability at the Sensitive But Unclassified (SBU) level. According to testimony of the Program Manager,[108] this first delivery of the EDS provides contact information for counterterrorism-related watch centers, and is similar to a telephone book's Blue Pages listing. These Blue Pages are available to anyone who has access to the Sensitive Compartmented Information (SCI) and SECRET security domains. The Blue Pages reflect

---

[103] White House Press Release. Executive Order: Further Strengthening the Sharing of Terrorism Information to Protect Americans (Oct. 25, 2005).

[104] WMD Commission, supra at 432.

[105] "DNI Program Manager Information Sharing Environment—About the Information Sharing Council," http://www.ise.gov/ISC.html

[106] Information Sharing Environment Program Manager, *Information Sharing Environment Interim Implementation Plan* 2 (2006)

[107] Id. at iii, 8.

[108] Thomas McNamara, testimony before the House Homeland Security Subcommittee on Intelligence (May 10, 2006)

agreements and cooperation among the Information Sharing Council members; in particular, the ODNI, who is hosting the Blue Pages in the SCI security domain, and the Department of Homeland Security (DHS), which is hosting the SECRET security domain Blue Pages. By the end of October 2006 the Program Manager plans to increase existing ODNI White Page capability (Name, personal attributes and at least one method of contact for named personnel) at the SCI and SECRET domains to include non-IC information. Also planned for October 2006 is the initial iteration of Yellow Pages (Organization and contact information, which may include description of roles and responsibilities and organization charts) in the SCI and SECRET domains.

National Counterterrorism Center

Executive Order 13354, issued in August 2004, established the NCTC to serve as the primary organization for integrating and analyzing all intelligence pertaining to terrorism and counterterrorism, and to conduct strategic operational planning by integrating all instruments of national power.[109] In December 2004, Congress codified the NCTC in IRTPA and placed the NCTC in the ODNI. On June 10, 2005, the President announced the nomination of Vice Admiral John Redd, the WMD Commission's Executive Director, to be Director of the NCTC, replacing its Acting Director John Brennan.[110] Redd was confirmed by the Senate on August 1, 2005. The NCTC imports information from over 28 different government networks on a daily basis, which it analyzes, sorts, and then disseminates to fellow agencies such as the Terrorist Screening Center.[111]

Most recently, Redd positioned NCTC at a Senate Foreign Relations Committee[112] Hearing on Counterterrorism as the government's model for classified information sharing. The NCTC does not, however, currently share information with state and local officials. John Brennan, former NCTC Acting Director, said in a November 2005 op-ed on intelligence reform that: "Clearly, state and local officials aren't going to get any tips from the National Counterterrorism Center, which is prohibited by law from directly disseminating any information outside the federal family."[113]

Privacy and Civil Liberties Oversight Board

The Privacy and Civil Liberties Oversight Board was established by the IRTPA at the recommendation of the 9/11 Commission. In February 2006, Carol Dinkins and Alan Raul were confirmed by the Senate as Chair and Vice Chair, respectively, and the Board had its first meeting on March 14, 2006.[114] The civilian board members are Lanny Davis, Theodore Olson, and Francis Taylor. Chairwoman Dinkins, in June 2006 testimony before Congress, reported that the Board was proud of how far it had come since it began meeting in March.[115] The Board has hired an Executive

[109] See http://www.nctc.gov/about_us/about_nctc.html.

[110] White House Press Release. President Visits National Counterterrorism Center (June 10, 2005), available at http://www.whitehouse.gov/news/releases/2005/06/20050610-4.html.

[111] Thomas McNamara, "Statement for the Record," before the House Homeland Security Subcommittee on Intelligence, (May 10, 2006), available at http://www.ise.gov/docs/sftrPMISE20060510.pdf.

[112] Senate Foreign Relations Committee Hearing on Counterterrorism (June 13, 2006)

[113] John Brennan, "Is This Intelligence? We Added Players, but Lost Control of the Ball," *Washington Post* (Nov. 20, 2005)

[114] "Privacy and Civil Liberties Oversight Board," available at http://www.whitehouse.gov/privacyboard/.

[115] Carol Dinkins, testimony before the House Committee on Government Reform Subcommittee on National Security, Emerging Threats, and International Relations (June 6, 2006), available at http://reform.house.gov/UploadedFiles/Dinkins%20HouseTestimony6606.pdf.

Director, and will address the issue of protecting privacy and civil liberties with information sharing as an early priority.[116]

Department of Homeland Security

Secretary of Homeland Security Michael Chertoff announced on July 13, 2005 that, based on its Second Stage Review—a comprehensive study examining programs, policies, operations, and organizational structure—the DHS will pursue six major objectives.[117] The DHS will:

- Increase overall preparedness, particularly for catastrophic events;
- Create better transportation security systems to move people and cargo more securely and efficiently;
- Strengthen border security and interior enforcement and reform immigration processes;
- Enhance information sharing with our partners;
- Improve DHS financial management, human resource development, procurement and information technology; and
- Realign the DHS organization to maximize mission performance.

Among these objectives is improving information sharing with state and local partners, the private sector, law enforcement, and first responders. Secretary Chertoff referred to state and local authorities as the front line of defense, and pledged to work with them, as well as with private sector infrastructure owners, to promote greater situational awareness through information sharing. The Department is currently working with state homeland security advisors and emergency management coordinators to establish information exchange protocols, evaluate the Homeland Security Advisory System, and develop state and regional data fusion centers.[118]

The DHS Office of Intelligence and Analysis (OIA), created along with the position of Chief Intelligence Officer (CINT) in January 2006, is the division of the DHS tasked to effectively integrate and manage the Department's intelligence programs.[119] According to Charles Allen, the current CINT, in May 2006 testimony before Congress, the primary goals of the OIA are:

- Improving the quality of intelligence analysis across the Department;

---

[116] Ibid.

[117] Homeland Security Press Release. Homeland Security Secretary Michael Chertoff Announces Six-Point Agenda for Department of Homeland Security (July 13, 2005), available at http://www.dhs.gov/dhspublic/display?theme=43&content=4598&print=true.

[118] Secretary Michael Chertoff, U.S. Department of Homeland Security, Second Stage Review Remarks as Prepared Washington, D.C., (July 13, 2005)

[119] Charles Allen, "Progress of the DHS Chief Intelligence Officer," before the House Committee on Homeland Security Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment (May 24, 2006), available at http://hsc.house.gov/files/TestimonyAllen2.pdf.

- Integrating the DHS intelligence enterprise;
- Strengthening our support to state, local, and tribal authorities, as well as the private sector;
- Ensuring that DHS intelligence takes its full place in the intelligence community; and,
- Solidifying our relationship with the Congress by improving our transparency and responsiveness.

According to Allen, the OIA has made great progress in all of these goals. It has encouraged a culture of write-to-release in order to improve the quality of analysis; used the Deputy CINT as a liaison with state, local, and tribal agencies; worked more closely with the NCTC and ODNI to better integrate the OAI into the intelligence community; and provided Congress with responsive access to relevant intelligence information to improve transparency.

Other Developments

When asked to assess the implementation of the information sharing environment, Program Manager Thomas McNamara acknowledged that there are many areas where the government needs to do better. In addition to initiatives already discussed, Mr. McNamara mentioned the following initiatives in May 2006 written testimony for Congress:

> The Terrorist Screening Center (TSC) used to receive terrorism information from NCTC via a computer disk. Today, the TSC receives this information directly from NCTC in controlled unclassified format and electronically. This has greatly enhanced the ability for TSC to efficiently produce the Terrorist Watch List and distribute it to local law enforcement partners.
>
> Fusion Centers have been established—or are in the process of being established in 42 states. Additionally, a growing number of localities—particularly major urban areas—are also establishing similar centers. State and local fusion centers are a critical component of the [Information Sharing Environment] because they can dramatically enhance efforts to gather, process and share locally generated information regarding potential terrorist threats and to integrate that information into the Federal efforts for counterterrorism. Federal law enforcement is working closely with these Fusion Centers.
>
> The Department of Homeland Security (DHS) offers a series of web-based portals and other tools that support information exchange, file sharing and chat services among state & local law enforcement, emergency operations centers, 53 major urban areas, local, state or regional intelligence fusion centers, and the private sector.
>
> Department of Justice's (DOJ) Law Enforcement Information Sharing Program (LEISP) implements a unified Department-wide technology architecture to enable DOJ partnerships with State, local, tribal & Federal law enforcement agencies, and identifies which IT investments to support. LEISP enhances DOJ's ability to share information across jurisdictional boundaries.

The Department of Defense (DoD) has recently designated a full time Information Sharing Executive; an initiative the Program Manager intends to encourage other large agencies to follow. DoD has also continued to invest in the development of Global Information Grid (GIG). The GIG is being developed in concert with ODNI IC Enterprise Architecture (ICEA) to support all DoD, National Security, and related IC mission and functions in war and peace.[120]

9/11 Public Discourse Project

To advance the unfinished agenda left by the recommendations that were not addressed in their July 2004 report, the members of the 9/11 Commission came together again in September 2004 to form the 9/11 Public Discourse Project. The unfinished agenda includes using maximum effort to prevent nuclear terrorism, allocating homeland security grants on the basis of risk rather than politics, providing reliable radio spectrum to first responders, and restructuring Congress to better oversee the intelligence community.[121] A report card issued by the project in December 2005 as its final act, demonstrated the mixed results in the implementation of the 9/11 Commission's recommendations, giving out twelve "Bs" and twelve "Ds."[122] Two major areas of concern that the Project highlighted were the dissemination of information to state and local authorities as well as adequate support of the Program Manager for the information sharing environment, specifically by clarifying exactly what authorities that position holds. Additionally, in testimony before Congress in June 2006, Thomas Kean and Lee Hamilton, chair and vice-chair, respectively, of the 9/11 Commission and co-founders of the 9/11 Public Discourse Project, voiced concerns about protecting civil liberties while still creating an effective information sharing environment, noting that there must be a strong voice within the Executive Branch on behalf of the individual, and on behalf of civil liberties.[123]

DNI's Current and Future Perspectives

On April 20, 2006, DNI John Negroponte gave a speech to commemorate the one-year anniversary of the inception of the ODNI. In addition, the ODNI released a report detailing the progress on implementing the IRPTA.

His speech, and the report[124], addressed the broad issue of intelligence reform, but also discussed the issue of information-sharing and the progress the intelligence community was making in that regard. Mr. Negroponte used the NCTC's integration of 28 different databases from the homeland security, defense, and intelligence communities as an example of the progress made in the sharing of

---

[120] Thomas McNamara, testimony before the House Homeland Security Subcommittee on Intelligence (May 10, 2006)

[121] The 9/11 Public Discourse web site can be viewed at http://www.9-11pdp.org/about/index.htm. For further information on the "unfinished agenda," see remarks by Chairman Thomas H. Kean and Vice Chair Lee H. Hamilton, Final Report of the 9/11 Public Discourse Project 5, (Dec. 5, 2005)

[122] Thomas Kean and Lee Hamilton, "Prepared Statement for the Record," before the House Committee on Government Reform Subcommittee on National Security, Emerging Threats, and International Relations (June 6, 2006), available at http://reform.house.gov/UploadedFiles/Kean%20Hamilton%20Testimony%20before%20SHAYS%20060606.pdf.

[123] Id.

[124] John D. Negroponte, "Intelligence Reform: Making it Happen," speech, National Press Club, Washington, DC (April 20, 2006), available at http://www.dni.gov/speeches/20060420_speech.html

information. He also cited the CIO of the ODNI, retired Major General Dale Meyerrose, whose duties consist of looking at the architecture of the entire intelligence community with respect to information sharing, as another example of successful implementation of information sharing policy.

Mr. Negroponte also stated that information sharing between the intelligence community and state, local, and tribal agencies was something that the ODNI was looking to improve next. In addition, he mentioned that the intelligence community had agreed in principle on the idea of joint tours of duty for intelligence officers as another method of integrating and sharing information between agencies.[125]

[125] Id.

Appendix 2

Letter to the President of September 7, 2005 and White House response of October 21, 2005

MARKLE FOUNDATION

Task Force on National Security in the Information Age

September 7, 2005

The President
The White House
1600 Pennsylvania Avenue, N.W.
Washington, D.C. 20500

Re: Building the Information Sharing Environment

Dear Mr. President:

We write on behalf of the Markle Foundation Task Force on National Security in the Information Age. At our August 2005 meeting, the Task Force asked that after Labor Day we convey to you some thoughts as you prepare the report due this month to Congress on the Guidelines and Requirements to Implement the Information Sharing Environment mandated by the Intelligence Reform and Terrorism Prevention Act of December 2004 (the Act). We reconsidered sending the letter in light of the terrible loss from Hurricane Katrina, but concluded that you would appreciate this input since so many of the issues may be similar to those Secretary Chertoff and others have suggested be examined in an after action report on the response to the hurricane.

As you know, the Markle Task Force has issued two reports that frame a decentralized network of information sharing, guided by policy principles that simultaneously empower and constrain government officials and provide meaningful privacy and civil liberties protections for our people. The information sharing environment requires, as we stated, clear and understandable rules and business practices on collection and sharing of data that is permissible, and that which is prohibited.

Your Executive Orders and the Act have generated genuine progress toward creating an Information Sharing Environment (ISE), and individual and agency initiatives show good promise. We remain concerned, however, that risk aversion and bureaucratic resistance to change continue to hamper the carrying out of announced new policies. The constitutional and statutory authorities to do what needs to be done exist. We urge you to reiterate to your Cabinet officers and all U.S. Government officers that they should interpret all applicable laws and regulations to enable information sharing rather than use ambiguities between the Act and prior law which Congress left unresolved as an excuse to protect prior approaches. They need to embrace rather than resist the change.

It is our view that we as a nation must move to create the ISE with great urgency, and that we should not be satisfied with the first steps – as major as they are – that have been taken in the four years since the 9/11 attacks. The same sense of urgency and focused attention exercised by our military men and women in the battlefield must be applied to reforming how government agencies work together to understand and prevent the threats to the nation.

10 Rockefeller Plaza, New York, NY 10020 Phone 212.489.6655 Fax 212.765.9690 www.markle.org

In your report to Congress, we believe it will be helpful if you address the following:

1. Make clear that the Director of National Intelligence (DNI) has responsibility for the creation of the ISE. Since the ISE Program Manager (PM) has been placed administratively in the DNI's office, the DNI must assume the responsibility to ensure that the PM creates an effective ISE with the full recognition that such a system extends beyond the Intelligence Community. Because successful implementation of the ISE is critical to achieving intelligence goals and meeting other responsibilities of the DNI such as providing the President with a well-informed briefing, nothing in his portfolio is more fundamental.

2. Emphasize the development of government-wide policies and guidelines immediately as the foundation for the adoption of information sharing capabilities and procedures. Sweeping change is needed to remove any pre-9/11 confusion about information sharing that, regrettably, still exists in some departments and agencies. A single set of policies across the government, while recognizing the need for some additional rules depending on agency-specific missions, should end confusion and interagency battles about whose rules apply in particular situations.

3. Consistent with our earlier recommendations, and as required by the Act, these policies should address four key issues.

    - Clear and enforceable rules and procedures are needed that ensure information is accessed, shared, handled, and retained in a manner that meets operational efficiency and security, while protecting our nation's privacy and civil liberties. Perhaps most urgently, the government needs to create new guidelines governing information sharing of "U.S. persons" data since that designation is an outdated boundary for what is permissible.

    - A clear and consistent government-wide process must be created that guides classification decisions to protect sources and methods while enabling access and sharing without undue or arbitrary dependence on originator control (ORCON).

    - Technical and organizational mechanisms for policy compliance, oversight, and dispute resolution are needed to minimize and adjudicate failures to share information. This will reduce risk aversion by government officials who might be concerned about the personal impact of wrong decisions in a new environment.

    - A comprehensive and independent assessment of the value being created by the ISE for different participants, including policymakers is needed.

    We believe that addressing these fundamental policy challenges will accelerate the implementation of the ISE consistent with privacy and civil liberties concerns and national security needs.

10 Rockefeller Plaza, New York, NY 10020 Phone 212.489.6655 Fax 212.765.9690 www.markle.org

4. The PM should immediately be given the resources needed to get the job done by both Congress and the Administration. The White House staff and the DNI should ensure obstacles are removed. Because his responsibilities extend beyond the Intelligence Community, the PM should have enhanced authority within the Executive Office of the President. Thus, we recommend the PM chair the Information Sharing Policy Coordinating Committee in addition to chairing the Information Sharing Council.

5. Creating the Privacy and Civil Liberties Oversight Board in the Executive Office of the President was a key step in ensuring that effective information sharing for national security conforms to our nation's traditions and values. We hope the board will engage quickly as the policies and guidelines are developed.

The nation has only begun to mobilize the tremendous resources provided by the capabilities of its people and its advanced technology. We cannot afford to lose the innovation race to the terrorists who are aggressively using technology like the Internet to connect and train recruits as well as plan and execute operations. We must train government employees to work in new ways, sponsor research on new technologies and methods, and create systems that manage information in smarter and more cost-effective ways, while providing real security improvements and accountability. It is our sense that people in government are already working hard and therefore instead of asking them to work harder, the leadership must create an environment that allows them to work smarter.

We remain concerned that if another terrorist attack were to take place in the U.S., the immediate reaction could cause the pendulum to swing toward measures that impinge on our privacy and civil liberties. Any potential future intelligence failures will not rightly be blamed on legal constraints that prevent sensible information collection and sharing. The authorities to collect and share information exist, but cannot be realized without clear government-wide guidelines on how this can be maximized while protecting the security of information and the civil liberties of our people.

The Markle Task Force stands ready to assist in any way you may find useful.

Respectfully yours,

Zoë Baird Jim Barksdale

Co-Chairs of the Markle Task Force on National Security in the Information Age

10 Rockefeller Plaza, New York, NY 10020 Phone 212.489.6655 Fax 212.765.9690 www.markle.org

THE WHITE HOUSE

WASHINGTON

October 21, 2005

Dear Ms. Baird:

Thank you for your thoughtful letter of September 7, 2005, in which you shared with the President insights and suggestions of the Markle Task Force as he prepares to issue guidelines and requirements pursuant to section 1016(d) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA).

As you likely have heard by now, the priority response to Hurricane Katrina by many of the key information-sharing stakeholders temporarily delayed our efforts to meet the IRTPA's September 13 deliverable. We are now back on track, and expect the President to issue a directive shortly.

On behalf of the President, we are deeply grateful to you and the entire Markle Task Force for your abiding commitment to improving the U.S. Government's capacity to facilitate access to and sharing of terrorism information. We also share your sense of urgency about establishing an Information Sharing Environment (ISE) that will facilitate the flow of terrorism-related information within and beyond the Federal Government without infringing on information privacy rights or civil liberties.

As for your specific suggestions, please rest assured the Director of National Intelligence (DNI) fully appreciates his responsibility with respect to creating the ISE, and will ensure the Program Manager -- who is subject to the DNI's authority, direction and control -- receives the support he needs. In addition, the President's guidelines will be designed to set Government-wide policies and procedures, and will address conflicting authorities between and among agencies in the information-sharing context.

We appreciate your concern about the need to address Originator Controls (ORCON) and U.S. person data, among others, in the ISE context. Guidance on these matters will be forthcoming. The Privacy and Civil Liberties Oversight Board -- once its chair and vice chair are confirmed and it becomes operational --

promises to provide a valuable resource for the Program Manager, the Information Sharing Council, and participating departments and agencies in both the development and use of the ISE.

We have no plan to designate the Program Manager as chair of the Information Sharing Policy Coordination Committee (ISPCC). The ISPCC, like other PCC's, is a White House-based forum that neutrally addresses policy issues and disputes which, in this case, relate to terrorism information sharing and building the ISE. The Program Manager, who himself is a member of that body separate and apart from the O/DNI representative, is expected to raise issues and advocate positions before the ISPCC.

Thank you, again, for your ongoing commitment to this critical initiative and for your generous offer of further assistance. An identical letter has been sent to Mr. Barksdale.

Sincerely,

Stephen J. Hadley
Assistant to the President
for National Security Affairs

Frances Fragos Townsend
Assistant to the President
for Homeland Security and
Counterterrorism

Zoe Baird
Co-Chairman
Markle Task Force on National
Security in the Information Age
10 Rockefeller Plaza
16th Floor
New York, NY 10020-1903

MARKLE FOUNDATION

Markle Foundation
10 Rockefeller Plaza
16th Floor
New York, NY 10020-1903
Phone 212.713.7600
Fax 212.765.9690
www.markle.org