Nation At Risk:

Policy Makers Need Better Information to Protect the Country

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

March 2009

THE MARKLE FOUNDATION
TASK FORCE ON NATIONAL SECURITY IN THE INFORMATION AGE

Zoë Baird, Co-Chair*
The Markle Foundation

Jim Barksdale, Co-Chair
Barksdale Management Corporation

MEMBERS:

Robert D. Atkinson
Information Technology and Innovation Foundation

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**
Senate Committee on the Judiciary

Sidney D. Drell
Stanford Linear Accelerator Center, Stanford University

Esther Dyson
CNET Networks

Amitai Etzioni
The George Washington University

Richard Falkenrath
New York Police Department

David J. Farber
Carnegie Mellon University

John Gage
Kleiner Perkins Caulfield & Byers

John Gordon*
United States Air Force, Retired

Slade Gorton*
K&L Gates

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

* Members of the Steering Committee who prepared the *Nation At Risk* report.

** These individuals were members of the Task Force and participated in the development of its first three previous reports. Although the fundamental recommendations in those past reports form the foundation for the *Nation At Risk* report, these individuals have taken positions in the government and were not part of the Steering Committee that prepared *Nation At Risk*.

ASSOCIATES:

Fred Cate
Indiana University School of Law Bloomington

Scott Charney
Microsoft Corporation

Bob Clerman
Noblis

David Gunter
Ernst & Young LLP

Drew Ladner
Pascal Metrics Inc.

Bill Neugent
MITRE

Daniel B. Prieto
IBM

Clay Shirky
Writer and Consultant

Peter Swire **
Moritz College of Law, The Ohio State University

Mel Taub
Independent Consultant

STAFF:

Taite Bergin
Associate, Quorum Strategies

Karen Byers
Managing Director and Chief Financial Officer
Markle Foundation

Christopher Kojm ***
Elliott School of International Affairs
George Washington University;
Associate, Quorum Strategies

Danna Lindsay
Administrative Assistant
Markle Foundation

Philippe Oudinot
Senior Attorney, Arnold & Porter

Mara Rudman***
Principal, Quorum Strategies

Douglas Sosnik
Independent Consultant

Nicholas Townsend
Associate, Arnold & Porter

Colette Walker
Associate, Quorum Strategies

Stefaan Verhulst
Chief of Research, Markle Foundation

*** Through January 2009
**** Through April 2009

Contents

Executive Summary

NATION AT RISK:
POLICY MAKERS NEED BETTER INFORMATION TO PROTECT THE COUNTRY

For all the nation has invested in national security in the last several years, we remain vulnerable to terrorist attack and emerging national security threats because we have not adequately improved our ability to know what we know about these threats.

The Obama administration confronts a stark set of national security challenges including terrorism, instability from the global economic crisis, energy security, climate change, cybersecurity, and weapons of mass destruction. President Obama and his administration cannot identify, understand, and respond to these threats without the collaboration and sharing of information among officials across the government so fragments of information can be brought together to create knowledge. To improve decision making, the new administration needs to take immediate steps to improve information sharing.

Today, we are still vulnerable to attack because—as on 9/11—we are still not able to connect the dots. At the same time, civil liberties are at risk because we don't have the government-wide policies in place to protect them as intelligence collection has expanded.

Since April 2002, the Markle Foundation Task Force on National Security in the Information Age, a diverse and bipartisan group of experienced former policymakers from the Carter, Reagan, Bush, Clinton and Bush administrations, senior executives from the information technology industry, and privacy advocates, have recommended ways to improve national security decision making by transforming business processes and the way information is shared.

Over the last few months, the Markle Task Force has interviewed multiple officials in the Executive Branch and the Congress on the state of information sharing in order to identify priorities for the new administration, which now includes several former Markle Task Force members.

The President and Congress must reaffirm information sharing as a top priority, ensuring that policymakers have the best information to inform their decisions. We are at a critical moment, where immediate action at the start of the Obama administration is required. There is unfinished business in implementing an information sharing framework across all agencies that have information important to national security (including state and local organizations). If there is another terrorist attack on the United States, the American people will neither understand nor forgive a failure to have taken this opportunity to get the right policies and structures in place. An

information sharing framework will allow government to collaborate effectively across diverse areas to inform policymakers better without undermining civil liberties.

The President and Congress must ensure that all government information relevant to national security is discoverable and accessible to authorized users while audited to ensure accountability. Otherwise we will remain vulnerable.

- When government officials have the capacity to locate relevant information and to make sense of it, they can find the right information in time to make better-informed decisions—including the prevention of terrorist attacks. Such a system of discoverability, rather than the creation of large centralized databases, improves our security and minimizes privacy risks because it avoids bulk transfers of data.

- When combined with an authorized use standard, discoverability ensures that users obtain what they need but only what they need. Such an authorized use standard permits analysts and others to obtain information based on their role, mission, and a predicated purpose.

- The necessary feature of auditing, which we recommend, allows for improved enforcement of the authorized use standard as well as contributing to enhanced information security.

The President and Congress must develop government-wide privacy policies for information sharing to match the increased technological capabilities to collect, store and analyze information. These policies must be detailed and address the hard questions not answered by current law—who gets what information for what purpose under what standard of justification. Without those privacy policies in place, the American people won't have confidence in their government, while the analysts and operatives using the information sharing framework won't have confidence that they know what they are expected and allowed to do, and that their work is lawful and appropriate.

The President and Congress must overcome bureaucratic resistance to change. Old habits die hard. The "need to know" principle and stovepiping of information within agencies persist. The adoption of the "need to share" principle and the responsibility to provide information, and actions to transform the culture through metrics and incentives, are necessary to the success of the information sharing framework. In addition, those who depend on information to make decisions and accomplish their mission must be empowered to drive information sharing, to ensure they get the best possible data.

These recommendations, which are detailed further in the report, are neither complicated nor technically difficult. They require strong, sustained leadership and attention to implementation.

Nation At Risk:

Policy Makers Need Better Information to Protect the Country

An effective information sharing framework will enhance knowledge creation to improve decision-making across the government.

Making information sharing a priority is necessary to safeguard our national security. The threats of the 21st century are too complex and difficult to discern with traditional intelligence practices. Whether the question is Iran's nuclear activities, biosecurity or a potential cyber attack on critical computer networks, government personnel across agencies must collaborate and share information to identify, understand, and respond to evolving security threats.

The 9/11 Commission identified ten lost "operational opportunities" to derail the 9/11 attacks—and most involved a failure to share information. Progress on information sharing is the single most important step required to improve the national security of the United States. If there is another terrorist attack on the United States, the American people will neither understand nor forgive a failure to have connected the dots. Lack of progress on information sharing is a clear and present danger to the country.

An information sharing framework is necessary. Information sharing is not only about technology. It is about establishing a collaborative environment with a clear purpose: ensuring that the right people have access to the right information at the right time under the right conditions to enable the most informed decisions. The terrorism threat is the impetus for the information sharing framework, yet its value is enhanced knowledge creation to improve decision-making and policy implementation across the government.

Unfortunately, the sense of urgency on information sharing has diminished in the seven years since the 9/11 attacks. Each new problem our country confronts pushes information sharing further down the priority list. *The clarion call of this report is a simple one: the President and Congress must provide sustained leadership on information sharing in order to protect the nation.* They must ensure accountability, sweep away bureaucratic resistance to information sharing, and foster an open debate about how best to achieve the twin goals of national security and protection of civil liberties. An information sharing framework will succeed only if the American people are confident that it will respect their privacy and protect against inappropriate disclosure.

The good news, to date, is that the required laws have been passed:

- President Bush and Congress have acted on many of the recommendations of the 9/11 Commission, the WMD Commission, and the Markle Task Force (which informed both Commission reports).
- The Intelligence Reform and Terrorism Prevention Act of 2004 and the 9/11 Commission Recommendations Implementation Act of 2007 required transformation of the intelligence community to achieve information sharing.
- Pursuant to the 2004 law, President Bush, the Program Manager for the Information Sharing Environment (PM-ISE), the Director of National Intelligence (DNI), and others have issued initial policy guidance reflecting the new "need to share" or "responsibility to provide" principle.

Yet old habits die hard. The "need to know" principle and stovepiping of information within agencies persist. Cultural, institutional, and perceived technological obstacles have slowed the implementation of laws intended to facilitate the flow of information and create new ways of collaborating. Much more needs to be done to develop policies to assure both the public and government officials that privacy and security are protected while information is shared.

The Information Sharing Environment (ISE) created by Congress was intended to change the way government conducts the business of policy making based on information gathered. It had intended a "virtual reorganization of government" of communities of interest working on common problems across agency boundaries and between federal, state and local governments, and the private sector—wherever important information could be found.

While the National Counter Terrorism Center (NCTC) and the Office of the Director of National Intelligence (ODNI)—and to some extent the wider Intelligence Community (IC)—have made significant progress on information sharing, their work is far from complete. A 2008 review by the Inspector General of the 500 Day ODNI Plan indicated that the IC still has a long way to go on

collaboration and information sharing.[1] Information sharing outside the IC—as well as information sharing across the law enforcement, domestic intelligence, and foreign intelligence communities—remains problematic. So, too, is information sharing related to US persons. The Department of Homeland Security and the Federal Bureau of Investigation have engaged state and local law enforcement through fusion centers, but the role and future of these centers are uncertain and the sharing of information with them has been uneven. Information-sharing practices are still a hodge-podge because too much discretion has been left to each agency. While Congress and the Executive Branch have generally set out the basic policy structure for an effective information sharing framework, they should give agencies government-wide policy guidance on hard issues such as privacy, identity management, discoverability, and authorization.

Now is the moment for breakthrough progress on information sharing. Action at the start of the Obama administration is required. It is much better to build the house right the first time rather than remodeling it later. The Markle Task Force takes heart from the early actions of the Obama administration:

- First, the Obama administration has embraced information technology—and technology is now widely available both to help solve the hard issues mentioned above and to protect civil liberties.
- Second, the DNI signed a new Intelligence Community Directive (ICD 501) on January 21, 2009 mandating wide-ranging actions to promote information sharing, including the ability to discover and request information from all IC elements, who now have a "responsibility to provide" such information.
- Third, the Secretary of the Department of Homeland Security issued an Action Directive on State and local information sharing on her very first day in office, calling for "an evaluation of which activities hold the most promise for achieving the smooth flow of information on a real-time basis."

Now is the moment for breakthrough progress on information sharing. Action at the start of the Obama administration is required.

[1] See *Follow-up Report of the 500 Day Plan, Part 2*, available at http://www.dni.gov/500-day-plan/500%20Day%20Plan%20Follow%20Up%20Report%20part%202.pdf.

- Fourth, President Obama has affirmed the need to establish an integrated, effective and efficient approach to address 21st century threats. In *Presidential Study Directive 1*, he has called upon the Homeland Security and Counter-Terrorism Assistant to the President to review how to strengthen interagency coordination of the full range of homeland security and counterterrorism policies, including information sharing.

It is time to reaffirm our nation's commitment to improving information sharing by accelerating implementation of the laws and policies Congress put in place to shift government from a "need to know" to a "need to share" paradigm.

President Obama has also called for a new way of doing business. In light of the current financial crisis and growing budget pressures, we need to do more with less. President Obama created the new position of Chief Performance Officer to ensure that the government operates more efficiently. Improving the government's ability to share information will enhance our national security and it will increase efficiency by enabling government to "know what it knows" through collaboration by an integrated interagency team. An effective information sharing framework is not only important to protect against terrorism; it will make the government more effective in areas like energy security, bio-defense, and healthcare as well.

There is also a clear connection between cybersecurity and information sharing. The same technology that will help improve information sharing is a critical part of protecting against cyber threats. For example, regular, automated compliance and behavior audits will not only protect privacy and make possible authorized use of information: they will greatly enhance the government's ability to monitor misuse of its information networks and potential attempts to compromise the data on such networks or the networks themselves.

With better information, government officials will be able to make better informed decisions. Overcoming persistent barriers to information sharing requires strong, sustained leadership from the top and accountability throughout the government. Therefore, we urge the President and the Congress to:

- Reaffirm information sharing as a top priority.
- Make government information discoverable and accessible to authorized users by increasing the use of commercially available off-the-shelf technology.
- Enhance security and privacy protections to match the increased power of shared information.
- Transform the information sharing culture with metrics and incentives.
- Empower users to drive information sharing by forming communities of interest.

Ensuring that the Right People have the Right Information at the Right Time while Protecting Civil Liberties and Privacy is Central to National Security

As the 9/11 attacks demonstrated, good information is fundamental in order to understand and respond to 21st century national security threats. Without comprehensive information, decision-makers operate with a limited understanding of a threat or the best means to address it. In order to improve security, data from federal, state, and local agencies, as well as foreign and private sector sources, must be accessible to provide a more inclusive picture. Such information must be available in time-critical situations and in ways that are tailored to facilitate decision-making and action at all levels. This does not mean the creation of large centralized databases. Rather, it means the ability of users to locate relevant information across the government and to gain timely access for authorized use of that information.

An effective information sharing framework is necessary to achieve the goal of improved information sharing. This information sharing framework should be a decentralized information network as described in the Markle Task Force's past reports.[2] Its governance should require a user to provide a predicate in order to access data under an authorized use standard. To establish a predicate, an analyst seeking information would need to state a mission- or threat-based need to access the information for a particular purpose. Under this authorized use model, the information sharing framework would provide role-based access with robust monitoring of data use and auditing that would protect both the security of the information and privacy because real-time electronic records of data use and each person's predicate would be created, allowing auditors to ensure that use of information is consistent with the authorized use.

In an effective information sharing framework, information is not simply shared without restraint. The framework should govern sharing in accordance with government-wide policies that are designed to effect a virtual reengineering of government information management that increases collaboration by allowing communities of interest to form across parts of the government, while protecting against misuse and abuse. When government officials have the capacity to locate relevant information and make sense of it, the right people can find the right information in time to make better-informed decisions—including the prevention of terrorist attacks.

At the same time, information sharing will succeed only if accompanied by government-wide policy guidelines and oversight to provide robust protections for privacy and civil liberties. Without such protections, public trust will be lost, third parties will not cooperate with the government, and government employees will neither be empowered to share nor have confidence that shared

---

[2] The Markle Task Force's second report, *Creating a Trusted Network for Homeland Security* (2003), advocated a "decentralized network" that the Markle Task Force called the Systemwide Homeland Analysis and Response Exchange Network (SHARE). Earlier Task Force reports also support the crafting of a "national framework" or "networked, decentralized system." See also *Protecting America's Freedom in the Information Age* (2002). All reports are available at http://www.markle.org/.

information is private and secure. Absent measures to promote the reliable and accountable use of personally-identifiable information, an information sharing framework will risk undermining the values enshrined in our Constitution and laws.

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

These twin challenges—safeguarding civil liberties and enhancing information sharing—have been the focus of the Markle Foundation Task Force on National Security in the Information Age, co-chaired by Zoë Baird and Jim Barksdale. The Markle Task Force, created in 2002, has included distinguished security experts from the past five administrations, as well as experts on technology and civil liberties. The Markle Task Force's three reports[3] call for the adoption of a set of capabilities to help intelligence and law enforcement agencies "connect the dots" from dispersed bits of data, while preserving privacy and civil liberties.

President Bush, Congress, and the 9/11 Commission adopted most of the Markle Task Force recommendations:

- The Intelligence Reform and Terrorism Prevention Act of 2004 required the creation of an ISE as recommended in the Markle Task Force's first and second reports.
- The 9/11 Commission Recommendations Implementation Act of 2007 adopted many of the recommendations from the Markle Task Force's third report. Both laws established requirements for information-sharing policies and technologies as the Markle Task Force recommended.
- Amendments to Executive Order 12333 gave the DNI new authority over any intelligence information collected that pertains to more than one agency, and directed the Attorney General to develop guidelines to allow intelligence agencies access to information held by other agencies.
- Many intelligence, law enforcement, and national security agencies have also published strategies reflecting the "need to share" paradigm advocated by the Markle Task Force. Of particular note, the DNI signed Intelligence Community Directive 501 on January 21, 2009, mandating wide-ranging actions to promote information sharing across the Intelligence Community.

Hard work is still needed, however, to implement and institutionalize the sharing principles that will turn this policy vision into reality. Loopholes to prevent information sharing and collaboration must

[3] The three Markle Task Force reports are *Mobilizing Information to Prevent Terrorism* (2006), *Creating a Trusted Network for Homeland Security* (2003), and *Protecting America's Freedom in the Information Age* (2002). All reports are available at http://www.markle.org/.

be closed. For example, one senior official told the Markle Task Force that some agencies rely on their authority under Executive Order 12598, the order that establishes the classification system, as a basis for withholding data. Such inconsistencies with Executive Order 12333 and ICD 501 need to be resolved in favor of maximum information sharing. Best practices must be expanded across all levels of government and beyond the world of counterterrorism.

To assist the new administration and Congress, the Markle Task Force convened a Steering Committee to conduct a series of interviews[4] to assess progress on the implementation of information sharing policy. Common themes and findings emerged from these interviews, forming the basis of the five recommendations that follow.

Five Recommendations to Accelerate Creation of an Information Sharing Framework

1. Reaffirm Information Sharing as a Top Priority

Strong, Sustained Leadership from the Top is Required. While initial steps by the new Administration are commendable and promising, President Obama, Director of National Intelligence Dennis Blair, Attorney General Eric Holder, and the new Congress must provide strong, sustained leadership to reaffirm information sharing as a top priority. A waning sense of urgency in the seven years since the 9/11 attacks means that old habits of withholding information are returning. Top down leadership, to reaffirm the importance of information sharing, is necessary. The President should convene a Cabinet meeting to affirm information sharing as a top priority and to help overcome the bureaucratic resistance and turf wars that stymie progress.

One important way to achieve the new administration's priorities would be for President Obama to move the Program Manager for the Information Sharing Environment (PM-ISE) into the Executive Office of the President (EOP). The reason for such a move is clear. It will enable the PM-ISE to carry out its statutorily required government-wide authority[5] to coordinate the policies and

---

[4] Members of the Steering Committee conducted interviews at the Office of the Director of National Intelligence, the Office of the Program Manager for the Information Sharing Environment, the National Counterterrorism Center, the Office of Management and Budget, the Department of Homeland Security, the Senate, the House of Representatives, the Federal Bureau of Investigation, the Department of Justice, and the Government Accountability Office. The Steering Committee also conducted individual interviews with Presidential Adviser for Counterterrorism and Homeland Security John Brennan, former Director of National Intelligence Admiral Mike McConnell, and 9/11 Commission Vice Chair Lee Hamilton.

[5] *Intelligence Reform and Terrorism Prevention Act of 2004*, Pub. L. No. 108-458, 118 Stat. 3638 (2004), states that the PM-ISE is "responsible for information sharing across the Federal Government" and that he "shall have and exercise government wide authority."

procedures necessary for an effective information sharing framework, and give the PM-ISE White House backing to carry out its mission. Currently, the PM-ISE lacks policy clout and is seen (incorrectly) as an adjunct to the Intelligence Community. Elevating the PM-ISE into the EOP will ensure that the PM-ISE is able to coordinate across agencies effectively in order to improve the way our government shares information.

Regardless of where the PM-ISE is situated, the President should ensure that it is fully integrated into, and has a lead role in coordinating, all information sharing policy development and implementation across the government, including the intelligence, law enforcement, and homeland security communities. Otherwise, wasteful duplicate efforts are inevitable as individual agencies try to address information sharing independently. The approach proposed here is a more efficient and effective way of governing, consistent with President Obama's efforts to change the way government does business.

Improving the government's ability to share information will enhance our national security, improve privacy, and will increase efficiency by enabling government to "know what it knows" through collaboration by an integrated interagency team.

Ordering a High-Level Review. The President should also order an initial 60-day high-level review of the current policy and privacy guidelines and processes for the ISE to be completed by May 15, 2009. Our discussions with senior officials reveal that departments and agencies have widely differing priorities and perspectives with respect to information sharing. President Obama should demand an assessment of the state of the ISE on an annual basis thereafter, in order to ensure government-wide focus and coordination.

The Administration should release public reports on the results of its 60-day review, the status of implementation, and each annual review thereafter. In addition, Congress should hold hearings on the 60-day review and on each annual report to assure that information sharing remains a high national priority.
As part of this 60-day review, the new administration should apply ISE best practices to areas of national security concern in addition to terrorism, such as cybersecurity, nuclear proliferation, energy security, and climate change. To date, the ISE has been used primarily to facilitate the flow of terrorism-related information. The Obama administration should also focus directly on the overlapping worlds of law enforcement and domestic intelligence, because the sharing of information

between the law enforcement community and the intelligence community—a major lapse on 9/11—has always been critical to our recommendations. Tension persists between the intelligence and law enforcement communities, but the Markle Task Force encourages continued work on robust pilots that test concepts that could improve the way the two communities work together. Such pilots have reportedly been very successful in resolving information sharing disputes, and some are still underway. The Obama administration should establish a review process to transfer best practices from successful pilots to the broader intelligence and law enforcement communities.

2. Make Government Information Discoverable and Accessible to Authorized Users by Increasing the Use of Commercially Available Off-the-Shelf Technology

Increased Discovery. Perhaps the single most important step to foster an effective information sharing framework is to give users the ability to discover data that exists elsewhere—a capability that can simply be called "discoverability." The traditional information sharing model requires either the sender to know what information to send to whom ("push") or requires the end-user to know who to ask for what ("pull"). Whether push or pull, there are too many doors on which to knock. The chances of the right data holder and the right end-user locating each other and sharing the right information are slim at best.

Consider an analyst working in a counter-proliferation unit. How would this analyst come to realize that there is information directly related to his or her topic in the anti-money laundering unit? Without the ability to discover who has what information, these two units, even if they are working in the same building, are unlikely to recognize that they have related data points. Once an analyst knows where related information is located, the information access framework becomes more effective—because the analyst knows exactly who to ask for what.

Discoverability is therefore the first step in any effective system for sharing information. For this reason the Markle Task Force's third report emphasized the importance of establishing "data indices" as a critical precursor to information sharing.[6] Such directories serve as a locator service, returning pointers to data holders and documents based on the search criteria used. If information is not registered in data indices, then it is essentially undiscoverable. Think of data indices as a card catalog at a library. In this analogy, every aisle of the library is the equivalent of an isolated information silo. It would be unimaginable to roam the aisles expecting to find a relevant book. Rather, the card catalog provides a user with pointers to the location of books.

Privacy and security protections are enhanced through this recommended approach to discoverability. Locator and topic information are transferred to the index, but the underlying information isn't transferred until the user requesting it is authorized and authenticated. Further, with emerging technology that allows for removal of personally identifiable information (PII)—so

---

[6] Markle Task Force report *Mobilizing Information to Prevent Terrorism* (2006), pp. 46, 61.

called anonymization—the index can be created without any information that identifies an individual by name or other specific identifier. Therefore, the risk of unintended disclosure of PII contained in the data indices is reduced.

Data needs to be tagged at the point of collection with standardized information that can be indexed and searched. Many agencies, however, do not adequately tag and index their data, so it is not readily discoverable, which undermines not only an agency's ability to share the data with others, but also the agency's ability to share within its organization.

The ODNI has recognized the need for data to be tagged and indexed at the point of collection. As noted above, the DNI recently signed ICD 501, which establishes policies for discovery that require IC agencies to make all information collected and all analysis produced available for discovery by automated means. ICD 501 is an important step toward increased discovery because it creates a "responsibility to provide" information. Although ICD 501 tackles a number of hard questions, its implementation presents challenges and many important details need to be resolved. Moreover, ICD 501 only applies to the IC. An effective information sharing framework will require increased discoverability across the government, so that data users (analysts, operatives, and decision-makers) will be able to find and have access to a variety of information, including raw and finished intelligence, across agency lines.

The President should place a high priority on discoverability as the first step toward effective information access. The technology is readily available. What is needed now is clear government-wide policy guidance, accountability, and the painstaking work of implementation. The Obama administration should establish a policy obligating all agencies with a national security mission to make their data discoverable. This policy should require departments and agencies to:

- Tag their data at the point of collection.
- Contribute key categories of data (e.g., names, addresses, passport numbers, etc.) to data indices.
- Follow through on implementing widely available means to search data indices.

Such a policy is essential because discoverability is a critical precursor to effective information access.

Authorized Use and Identity Management. Privacy concerns must be paramount. Improved discoverability must go hand in hand with a trusted system that will facilitate access to the data indices and the information these indices point to (in the library analogy, access both to the card catalog and the book itself). An authorized use standard provides a model for building such a trusted system. Such a standard can bridge the gap between technology and policy by overcoming some of the systemic challenges of classification, data categorization, and compartmentalization that inhibit the flow of information to those who need it. Under such a standard, an agency or its employees could obtain mission-based or threat-based permission to discover, access, or share information, as

opposed to the current system that relies on place-of-collection rules, US persons status, and originator control limitations.

Congress asked the President to consider adoption of an authorized use standard in the 2007 9/11 Commission Recommendations Implementation Act. In his March 2008 "Feasibility Report" to Congress, the PM-ISE discussed numerous potential obstacles that he viewed as limiting the feasibility of implementing an authorized use standard. None of the objections cited in the report, however, were technical in nature. Commercial off-the-shelf technology, which continues to become more widely available, enables the use of such a standard even in today's environment of multiple and differing authorities and standards across the government.

The Steering Committee believes that a combination of high-level policy attention from the President and Congress and appropriately deployed technology can allow phased implementation of an authorized use standard. Such a standard does not require amendment of statutes, such as the Privacy Act, and it would be in full compliance with the vital principles underpinning the constitutional, statutory, and regulatory requirements currently in place. ICD 501 has started the IC down the path toward phased implementation of an authorized use standard by its incorporation of many principles from the Markle Task Force's previous work. For example, ICD 501 requires that information collected or analysis produced must be available to authorized IC personnel who have a mission need for information and an appropriate security clearance.

The main hurdle that is often asserted by some as preventing implementation of an authorized use standard is the lack of an effective identity management system, a system that verifies the identity of individuals in a network and controls their access to information by associating user rights and restrictions with each individual and his or her role. The ODNI is currently trying to complete the plan for an "Enterprise Architecture" to put technology in place that will enable identity management across all of the IC agencies, which, in turn, will make possible discoverability, disclosure control, and information access.

Overcoming identity management obstacles must be a priority for the Obama administration so that an authorized use standard can

The five recommendations in this report are neither complicated nor technically difficult. What is required to make information sharing happen is leadership to implement what is already written in statute, to overcome bureaucratic inertia, and to seize this moment for progress.

be implemented to enable selective revelation of discovered information based on roles, missions, and legal authorities. Technology to implement such a standard is commercially available today and phased implementation should begin now. Using existing technology to create an effective system for identity management will not only help improve information sharing: it will also be an important tool to enhance cybersecurity because it will identify all data users and, with appropriate protections, flag attempts to go beyond authorized access and use, or to cause damage to systems or information.

Role of Congress. The Congress should hold hearings to oversee the development of the information sharing framework, including how much data is discoverable and the status of progress on implementation of an authorized use standard. Congress should make sure these efforts are adequately funded.

3. Enhance Security and Privacy Protections to Match the Increased Power of Shared Information

Enhanced Information Security. Greater sharing of sensitive information increases the risk of damaging security breaches. The Markle Task Force has always recognized the legitimacy of security concerns with a "need to share" culture. Therefore, increased sharing must be accompanied by protections to assure that information is used in an appropriate manner. Counterintelligence technology already exists that can help create an environment where sharing can increase, because users trust the security measures that are in place.

Immutable audit logs should be used to protect privacy and security of information. Additionally, regular, automated compliance and behavior audits are an indispensable element of an information sharing framework. Such audit capabilities enable oversight and accountability and are a critical protection against misuse and abuse. Real-time audits of user compliance and behavior and immutable audit logs should be implemented now. They are integral to the Obama administration's efforts on information security technology. Such audits and network monitoring will also play an important role in protecting against cyber threats.

Greater Privacy Protection. No information sharing framework will succeed unless the American people are confident that it will respect their privacy and protect against inappropriate disclosure. Therefore, clear, transparent, and consistent policies are necessary to protect privacy and civil liberties. The ODNI and several other agencies now have Civil Liberties and/or Privacy Officers in place, but many agencies do not have clear policies to implement. In addition, agency heads should ensure that these officers are engaged at all stages of the policy development and implementation process. To date, PM-ISE guidelines and associated documents are more advisory than directive—they tell the agencies that they must address various privacy and security principles, but do not tell them how to do so. The guidelines state, for example, that all agencies must comply with the Privacy Act, but the Privacy Act does not address many of the hard questions surrounding who gets what information for what purpose under what standard of justification. The Obama administration must

promulgate government-wide policies on privacy and civil liberties that provide direction on hard issues and provide consistency, even as they allow agencies the flexibility that their different missions and authorities require.

Both the premise and the goal of the ISE are to use information in new and more powerful ways. Accordingly, building the ISE should entail the development of new and more powerful privacy protections. As the 9/11 Commission stated, the increase in governmental power "calls for an enhanced system of checks and balances." So far, however, the privacy guidelines issued for the ISE do not require agencies to provide any more protections than they offered before the ISE. Where there have been improvements, such as the Department of Homeland Security's development of the Traveler Redress Inquiry Program for travel-related problems, they have been spurred largely by Congressional and media attention, not by administration initiative.

Government-wide, there should be measurable changes:

- Auditing of both data quality and data flows.
- Enhanced fidelity of watchlists.
- Deployment of access and permissioning systems based on carefully defined missions and authorities.
- Clear predication for collection and retention of data.
- Redress systems that offer a meaningful opportunity to challenge adverse action and that ensure that corrections or qualifications catch up with disseminated data.

Improvements to enhance privacy should not be viewed as impediments to efficacy. Indeed, many of the measures that should be taken to improve privacy protection will actually enhance the effectiveness of the ISE by improving the reliability of information.

To revive one new oversight mechanism that was supposed to play a key role, the President and Congress should act expeditiously—within the next 60 days—to nominate and confirm members to the Privacy and Civil Liberties Oversight Board. Over 18 months ago, Congress re-chartered the Board to strengthen its independence and authority, but the new Board has never come into existence. The statutory charter for the new Board gives it a role both in providing advice on policy development and implementation and in reviewing specific programs and other government actions relating to terrorism.

Technology is also a critical tool for protecting privacy. To create public trust and ensure user confidence, the ISE should include tools to minimize the risk of unintended disclosure of PII. These include tools for anonymization, strong encryption, and digital rights management. The PM-ISE's determination that adequate removal of PII via data anonymization is technologically infeasible given complications arising from integration with existing systems, processes, and technology should be

revisited. A number of technologies are commercially available today that can facilitate an array of privacy and civil liberties protections, as well as information security measures.

Congress should engage in vigorous oversight with respect to privacy to make sure that the laws adequately protect privacy and civil liberties. The administration should fully inform the relevant committees and appropriately cleared staff of the challenges the government faces as a result of rapidly developing communications technology and of tools the administration is currently employing to collect information, including any new technology that may be needed to adequately collect and analyze information.

Information sharing is not only about technology. It is about establishing a collaborative environment with a clear purpose: ensuring that the right person has access to the right information at the right time under the right conditions to enable the most informed decisions.

4. Transform the Information Sharing Culture with Metrics and Incentives

Improved Metrics. Mission-oriented metrics are necessary to change the "need to know" culture that persists in many agencies. Past Markle Task Force reports discussed the need to establish performance metrics and self-enforcing milestones for the information sharing framework. In our second report[7], for instance, we provided a detailed set of questions Congress and others could use to evaluate progress made in information sharing and analysis. These 24 questions focused on whether:

- Roles, responsibilities and authorities were clarified.
- Progress was made to remove roadblocks to share information within the federal government.
- Intelligence was produced for a set of new customers.
- Communications and sharing was being promoted with state and local governments and the private sector.
- Overall analysis was improved.
- The capabilities of state, local and private sector entities were being improved.

[7] Markle Task Force report *Creating a Trusted Network for Homeland Security* (2003), page 26, Exhibit F.

To establish these metrics, as part of the initial 60-day review, the new administration and Congress should develop key questions in order to evaluate and measure agencies' performance in meeting essential information sharing and analysis objectives.

One of the first metrics should focus on discoverability because data indices are necessary to enable an effective information access framework. This metric should measure what percentage of an agency's data holdings have been registered in the data indices directory. Using the analogy from recommendation three, this metric would measure how many of the library books have a card in the card catalog. This could be accompanied by ongoing tests across organizations on how the ISE scores according to certain critical system requirements (akin to the Quality Assurance scenarios used in the private sector).

Accountability and Transparency. Once improved metrics are in place, agencies should be held accountable for reaching certain benchmarks or milestones. The Obama administration should couple program funding with how well they increase discoverability. Programs that do not make their information discoverable by putting their data in the index should get less funding. This type of financial accountability is logical because data held by a system that is not discoverable to the community at large is less useful and less valuable. This system of discovery metrics and accountability would significantly reduce the voluntary aspect of exposing select data with data indices, and provide clear information about who is contributing the most to the shared library and whose data is most useful.

Agency level accountability must also be accompanied by individual accountability. Penalties should be widely known, proportionate to the misuse or failure, and applied consistently. Field officers and mid-level analysts should have a special confidential channel to call senior leadership's attention to their belief that critical information is not being shared. This channel would send a clear message of individual accountability—that information sharing is not someone else's responsibility, but critical to the mission and part of everyone's job.

Driving Cultural Change with Performance Incentives and Training. Individual performance incentives and training are two important tools that can change agency culture in favor of information sharing. The government has put in place some training and policies to institutionalize sharing incentives, but implementation at the agency level is lacking.

For example, the PM-ISE issued a plan in 2006 requiring that agencies develop the following:

- Tailored training programs based on their unique business processes, missions, program, and policy needs.
- A core training module that will serve as the common educational baseline for the ISE.
- Incentives to adopt the ISE culture that hold personnel accountable for the improved and increased sharing of information.

Based on agency self-reporting, the PM-ISE found in June 2008 that fewer than 50 percent of agencies had adopted such training programs and personnel incentives. Moreover, there has been little assessment of the quality of any of the programs the agencies have adopted. PM-ISE guidance released on September 24, 2008 aims to make information sharing a factor in annual performance appraisals for employees of agencies that are members of the Information Sharing Council and others who handle terrorism-related information. The ODNI is still working on uniform training across the IC elements and on adding information sharing as a factor in performance evaluations throughout the IC.

The Obama administration must focus on improving incentives to share information because they can accelerate cultural change where the "need to share" or "responsibility to provide" culture has not fully taken root. Many individuals still perceive risk and penalties for sharing information that might later be claimed to have been unauthorized or ill advised. They believe they are more likely to get in trouble for sharing too much information than too little.

Three specific examples of incentives and training that could drive cultural change are outlined below. The Obama administration should:

- Integrate information sharing into performance reviews and budget and personnel resource allocation for all agencies that have a national security mission.

- Create an information sharing award. This award should be given to the agency or unit within an agency that has been most successful at making its data discoverable. This award would highlight the overall value of information sharing to national security, and help facilitate the necessary culture shift.

- Increase joint duty in the IC, in order to build a sense of trust and community. As in the military, the IC is instituting the practice that promotion to senior levels requires a tour of duty at another agency. A broader concept of joint duty, especially among mid-level employees, will foster a sense of community that is not narrowly focused on each agency's separate mission.

The heart of the matter is for employees at every level to understand why information sharing is valuable to *them*. As noted below, information sharing works well in Iraq and Afghanistan because the sense of shared mission is great. The Obama administration should take the lessons learned in the field and make them work back home.

5. Empower Users to Drive Information Sharing by Forming Communities of Interest

Users Should Drive Information Sharing. The information sharing framework must enable users to form communities of interest and drive information sharing. Users must become active participants in improving their own information base. They must consistently ask whether the best possible information is available to accomplish their mission. When they insist on better information, more effective practices are likely to be put in place to align information flows with their needs.

Individual users—whether agents on the street, analysts, or senior policymakers—require access to relevant information if they are ever to understand threats, discover actionable intelligence, and perform their jobs. Therefore, users must drive policies, procurement, and resource allocation in order to drive information sharing. Systems need to be designed with a focus on decision-making and users' goals rather than simply exchanging data for the sake of doing so.

Examples. Successful examples of user-driven information sharing should be studied and the best practices should be applied broadly throughout the information sharing framework. Concrete illustrations of user-driven information sharing follow:

First, the Global Maritime Domain Awareness Program (GMDAP) is a successful real-world example of users embracing and driving information sharing. The program, developed by the Department of Transportation and the Navy, tracks the movements of more than 10,000 vessels from over 40 nations in real-time. Built at low cost in just one year, GMDAP aggregates information from many sources using existing technology that is easily scalable and accessible over the web. The program has been successful for the simple reason that when users saw its value, they reached out to others in their community of interest to improve their information base. GMDAP has been called a "wiki on the waves"[8] because of the cooperation it has fostered, not only among federal agencies, but between participating nations. Since its inception, GMDAP participation has expanded from five countries to 40, with another 40 nations evaluating GMDAP participation. When end-users drive adoption, the incentives to share align naturally and sharing does not need to be forced from the top down. GMDAP has even fostered the sharing of maritime data between countries that typically do not cooperate, such as Pakistan and India. Having more participants allows users of GMDAP to see additional boats in the waterway, providing strong incentives for users to find others to join them in sharing. Users become the agents of change in order to improve their own knowledge about other boats in the water. Information sharing is no longer a vague concept, but an important tool to accomplish the user's mission.

---

[8] Harvard Kennedy School's Ash Institute for Democratic Governance and Innovation, *Global Maritime Domain Awareness Wins Innovations in American Government Award*, September 8, 2009. Available at http://content.knowledgeplex.org/streams/ksg/AshInstitute/09.09.08_GlobalMaritimeAwareness.pdf.

Second, the wars in Iraq and Afghanistan offer another powerful example of user-driven information sharing, where people from different agencies focus on a single mission and work together on the battlefield. One specific example is the Army's Distributed Common Ground System (DCGS). DCGS overlays a broad range of information (signals, geospatial, human, and open sources) from the tactical, theater and national level and combines it in a single place using an internet-based program. Individual military services and agencies see the value of putting their information into a sharing system like DCGS, because in Iraq and Afghanistan they face a common threat and share a common mission. Far away from Washington, they are also less constrained by agency stovepipes. The users demand, and then by their participation help achieve, an improved overall information base.

Finally, A-Space is the latest example of an information sharing tool made powerful by user participation. A-Space is MySpace for intelligence analysts. It allows analysts to sign up for topics and connect with colleagues who are focused on the same area. They can post questions to each other. In only ten weeks, more than 4,000 analysts have joined A-Space and created communities of interest to share information. A-Space is successful so far because of large user participation, especially by analysts who already use social networking sites and understand how a tool like A-Space can help them accomplish their mission. It is too early to tell if analysts will share all important information, yet A-Space has the potential to create the necessary culture within the analytic community to break down agency stovepipes. Commercially available technologies can assist A-Space in achieving the Markle Task Force's information sharing vision. Broader application of the A-Space example should also be explored, such as the current plan to create a C-Space that will allow collectors to share information and to connect the analytic and collection communities.

Focus on People and Policies, Not Just Technology. Technology can assist, but the fundamental hurdles to information sharing are not technical. Indeed, commercial off-the-shelf technology can provide solutions to technical issues that have been repeatedly cited as hurdles by senior government officials. The network environment that will truly facilitate information sharing relies on much more than simply building and deploying a technical architecture. It is a combination of people, processes, policies, and cultures that leverages advances in information technology and the best thinking in the private sector about the use of information.

It is our firm belief that rapid progress on developing an effective information sharing framework is the single most important step our new leaders can take to improve the national security of the United States. The five recommendations for the President and Congress in this report are:

- Reaffirm information sharing as a top priority.
- Make government information discoverable and accessible to authorized users by increasing the use of commercially available off-the-shelf technology.
- Enhance security and privacy protections to match the increased power of shared information.
- Transform the information sharing culture with metrics and incentives.
- Empower users to drive information sharing by forming communities of interest.

These recommendations are neither complicated nor technically difficult. What is required to make information sharing happen is leadership—to implement what is already written in statute, to overcome bureaucratic inertia, and to seize this moment for progress.

Appendix A:
Summary of Specific Recommendations

The Markle Task Force urges the President and Congress to:

1. Reaffirm information sharing as a top priority.

A. President Obama should *move the PM-ISE into the Executive Office of the President* in order to ensure that the PM-ISE has (i) government-wide authority to coordinate policies, and (ii) White House backing to carry out its mission.

B. President Obama should *order an initial 60-day high-level review of the current policy and privacy guidelines and processes for the ISE* to be completed by May 15, 2009, and should conduct similar reviews on an annual basis thereafter in order to ensure government-wide focus and coordination. The administration should release public reports on the results of the initial 60-day review, the status of implementation, and each annual review.

1) The initial 60-day review and each annual review should *apply ISE best practices more broadly to areas such as cybersecurity, nuclear proliferation, energy security, and climate change.*

2) The initial 60-day review and each annual review should focus directly on the *overlapping worlds of law enforcement and domestic intelligence.* The administration should continue to *work on robust pilots* that test concepts that could improve the way the two communities work together, and should establish a process to *transfer best practices* from successful pilots to the broader intelligence and law enforcement communities.

C. The President should *convene a Cabinet meeting to affirm information sharing as a top priority* and to help overcome the bureaucratic resistance and turf wars that stymie progress.

D. Congress should hold hearings on the initial 60-day review and on each annual report to assure that the issue remains a high national priority.

2. Make government information discoverable and accessible to authorized users by increasing the use of commercially available off-the-shelf technology.

A. The Obama administration should establish a *policy obligating all agencies with a national security mission* to make their data *discoverable.*

1) This *policy should require* that departments and agencies: (1) tag their data at the point of collection; (2) contribute key categories of data (e.g., names, addresses, passport numbers, etc.) to data indices; and (3) follow through on implementing widely available means to search data indices. Such technology is readily available. (ICD 501 is a step in the right direction.)

2) This clear government-wide policy guidance must be accompanied by *accountability* and the *painstaking work of implementation* because increasing discoverability is a critical precursor to effective information access.

B. The information sharing framework should begin *phased implementation of an authorized use standard* using *commercial off-the-shelf technology*, which could enable the use of such a standard even in today's environment of multiple and differing authorities and standards across the government.

C. The information sharing framework should address *identity management obstacles* by adopting technology that is available today so that an authorized use standard can be implemented to enable selective revelation of discovered information based on roles, missions, and legal authorities.

D. Congress should hold hearings to oversee the development of the information sharing framework, including how much data is discoverable and the status of progress on implementation of an authorized use standard. Congress should make sure these efforts are adequately funded.

3. Enhance security and privacy protections to match the increased power of shared information.

A. The information sharing framework should *increase information security* by including implementation of *real-time audits* of user compliance and behavior and *immutable audit logs* that record how a system has been used, because these measures will create an environment where users trust the security that is in place and thus sharing can increase.

B. The Obama administration must promulgate *government-wide policies on privacy and civil liberties* that are directive on hard issues and provide *consistency*, even as they allow agencies the flexibility that their different missions and authorities require.

C. The new administration should make measurable government-wide changes with respect to privacy in the following areas:

1) *Auditing* of both data quality and data flows

2) Enhanced fidelity of *watchlists*

3) Deployment of *access and permissioning systems* based on carefully defined missions and authorities

4) *Clear predication* for collection and retention of data

5) *Redress systems* that offer a meaningful opportunity to challenge adverse action and ensure that corrections or qualifications catch up with disseminated data

D. The President and Congress should *nominate and confirm members to the Privacy and Civil Liberties Oversight Board* within the next 60 days.

E. Agency heads should ensure that their *Civil Liberties and/or Privacy Officers are engaged at all stages of the policy* development and implementation process.

F. The information sharing framework should include *technological tools* to minimize risk of unintended disclosure of personally identifiable information, including tools for *anonymization, strong encryption, and digital rights management*. Such technologies are commercially available today.

G. Congress should engage in *vigorous oversight with respect to privacy* to make sure that the laws adequately protect privacy and civil liberties. The administration should fully inform the relevant committees and appropriately cleared staff of the *challenges* the government faces as a *result of rapidly developing communications technology* and of *tools the administration is currently employing* to collect information, including any new technology that may be needed to adequately collect and analyze information.

4. Transform the information sharing culture with metrics and incentives.

A. The new administration must use *mission-oriented metrics* to change the "need to know" culture that persists in many agencies. To establish these metrics, as part of the initial 60-day review, the new administration and Congress should develop key questions in order to evaluate and measure agencies' performance in meeting essential information sharing and analysis objectives.

1) One of the first metrics should focus on *discoverability* by measuring what percentage of an agency's data holdings have been registered in the data indices directory.

2) This could be accompanied by ongoing *tests across organizations* measuring how the information sharing framework scores according to certain critical system requirements (akin to the *Quality Assurance scenarios* used in the private sector).

B. The administration should *hold agencies accountable* for reaching specific benchmarks or milestones by *using program funding incentives*. (*ex.* Programs that do not make their information discoverable by putting their data in the index should get less funding.)

C. The information sharing framework could also increase *individual accountability* by creating a *special confidential channel for field officers and mid-level analysts* to call senior leadership's attention to their belief that critical information is not being shared. Penalties for failure to share information should be widely known and consistently applied.

D. The Obama administration must use *individual performance incentives* and *training* to accelerate cultural change. For example:

1) By *integrating information sharing into performance reviews and budget and personnel resource allocation* for all agencies that have a national security mission.

2) By *creating an information sharing award*. The award could be given to the agency or unit within an agency that has been most successful at making its data discoverable.

3) By *increasing joint duty* in the IC and instituting the practice that promotion to senior levels requires a tour of duty at another agency. This would help build a sense of trust and community within the IC.

5. Empower users to drive information sharing by forming communities of interest.

A. The information sharing framework must enable users to form *communities of interest* and drive information sharing.

B. *Users must become active participants in improving their own information base* by consistently asking whether the best possible information is available to accomplish their mission.

C. The information sharing framework needs to be *focused on decision-making and users' goals* rather than simply exchanging data. This will empower users by allowing users to drive policies, resource allocation, and procurement.

D. *Successful examples* of user-driven information sharing should be studied and *the best practices should be applied broadly throughout the information sharing framework*.

E. The *information sharing framework's* focus must be *on people and policies*, not just technology.

Appendix B:
Commercially Available Off-the-Shelf Technology

The Markle Task Force believes there now is available cost-effective, commercial off-the-shelf technology to implement critical elements of the Markle Task Force's vision, including:

- Systematic controls for the implementation of an "authorized use" standard, including full compliance with related legal requirements in statutes such as the Intelligence Reform and Terrorism Prevention Act and the 9/11 Commission Implementation Act. Such technology enables each data object down to the field level, to be tagged, synchronized, and tracked with attributes such as date of change, user's name, and clearance level, and modifications. Without source attribution as a data pedigree, it is not possible to establish "authorized use" or auditing thereof.

- Discoverability of data (through the use of data indices consistent with recommendations from earlier Markle Task Force reports) across national security classification levels, with controllable types of access, from "silent hits" to partial access to full access, and the ability to monitor decisions of a component *not to share* data. Such technology can now achieve levels of performance and scalability in the billions of records and thousands of transactions a second. Such discoverability indices have been demonstrated successfully, in publicly available settings, with structured and unstructured data alike.

- Selective revelation, to technologically enforce "authorized use" and access rules allowing individuals to see data only to which they are entitled based on their clearances, role, mission, and authorities of the entity at which they work, and their actual, individual missions. Importantly, the technology allows both for different access rules based on individual legal authorities and authorized uses of multiple government entities, and for dynamic revisioning of such access rules as a result of, e.g., gathering of additional information or legal authority to meet required predicates for access to sensitive U.S. Person data, changes in threat level, and the like.

- Anonymization technology, which permits disparate data holders to create data indices of anonymized data elements. Such technology enables information discovery across agencies or across components within agencies in a manner that provides higher levels of protection, particularly for personally identifiable information. Such forms of "discovery without disclosure" will be useful when the sharing entities are less likely to share otherwise (e.g., classified compartment to compartment, cross-agency, public-private, or even country-to-country).

- Immutable audit trails to enable accountability and oversight entities to gain certainty on how systems are used. This will ensure that such use complies with policy and law, and will enhance confidence that the audit trail has not been tampered with, even by the database administrator.

- Real-time tracking of analytical activities to ensure users are engaging the system in a manner consistent with their mission authorities and responsibilities. This audit capability is important for many reasons, including privacy and civil liberties concerns, as well as to meet operational, counterintelligence, and security requirements.

- Real-time "data tethering" capabilities, across federated data sources, to ensure that any information transferred between systems, particularly about individuals, is constantly updated and subjected to correction and redress.

- Underpinning these capabilities, a robust, enforceable, and fully monitorable identity management and authentication capability, eliminating what many individuals the Steering Committee interviewed assessed to be the principal remaining constraint to full implementation of the Markle Task Force's key recommendations.

Commercial off-the-shelf technology capable of delivering these elements is available today, including for use on open platforms. It is critical that the foundational technology for the Information Sharing Environment be open platform, so that best-of-breed elements can be selected and integrated. For example, unstructured entity extraction,[9] data indices, anonymization technology, and other privacy-enhancing technologies should be able to be incorporated on a modular basis without any major re-engineering efforts and should work seamlessly with all legacy hardware and software systems. Particularly important, such open platform technology can be readily combined to allow for analysis both of structured and unstructured information, in a highly privacy and civil liberties protective manner.

[9] This class of technology is used to select key words out of text documents (e.g., selection of names from a newspaper story).

The Markle Foundation®
10 Rockefeller Plaza
16th Floor
New York, NY 10020
Tel: 212.713.7600 ▪ Fax: 212.765.9690
www.markle.org
www.markletaskforce.org