Information Sharing in the 21st Century

The Way Forward

REPORT TO THE MARKLE FOUNDATION OF THE
COLUMBIA UNIVERSITY CAPSTONE TEAM

May 2012

A Project of

School of International & Public Affairs
Columbia University
New York, New York

[This page is intentionally left blank]

Table of Contents

Overview

In the decade following the 9/11 terrorist attacks on the United States, the nation undertook a number of major changes to deal with the new threats and shortcomings identified in domestic intelligence and law enforcement. New legislation established a Department of Homeland Security, a Director of National Intelligence, a National Counter-Terrorism Center, as well as the legal basis for more effective collection and sharing of important information among a multitude of responsible agencies, including the Intelligence Community and federal, state, local, and tribal law enforcement agencies. Certainly this has been an enormous task, and one that is still ongoing. While substantial progress has been made, a number of problems and shortcomings have been identified that still require attention.

Over the past decade the Markle Foundation has been at the forefront of analysis in this area. The Markle Foundation has focused on how best to mobilize information and technology to advance national security while protecting essential civil liberties. The Markle Task Force on National Security in the Information Age has advocated meeting current national security challenges by enabling the exchange and discovery of information across government in a trusted manner. It has suggested the development of particularized privacy policies and the adoption of an "authorized use" concept.

Counter-terrorism efforts among the nation's intelligence and law enforcement agencies have included a significant attempt to move to an information-sharing environment, both domestically and internationally. Security, privacy and political concerns have all posed problems to achieving an ideal information sharing environment. In light of these current challenges, a Capstone team of graduate students from Columbia University's School of International & Public Affairs (SIPA) has undertaken a research effort to support The Markle Foundation's ongoing work to expound on the information-sharing environment, and to analyze where such efforts stand with existing impediments to achieve a more effective environment in the future.

Disclaimer

The following report was prepared by a Capstone team of graduate students from the School of International and Public Affairs (SIPA) at Columbia University for the Markle Foundation. This publication was produced to assist the Markle Foundation in their ongoing efforts in the critical area of U.S. counter-terrorism information sharing. While the team consulted with the Markle Foundation to produce this publication, it is not a Markle Foundation product.

Acknowledgements

The Markle Foundation Task Force on National Security in the Information Age was founded in the aftermath of the 9/11 terrorist attacks, and has been a bipartisan group of distinguished national security experts serving as leaders in the fields of technology and civil liberties. The Task Force has been dedicated to providing insight into this critical national security problem, focusing on how information can be used wisely and effectively to ensure security while fully respecting traditional civil liberties. For over a decade their efforts have produced various published reports, background papers, briefings, and meetings directed toward this goal.

We are grateful to Dr. Stefaan Verhulst, Director of Research at the Markle Foundation, as well as various members of the Markle Foundation Task Force on National Security in the Information Age for their assistance in this effort. We would also like to thank Professor Abraham Wagner, faculty advisor to the Capstone team as well as the School of International & Public Affairs (SIPA) at Columbia University for their support in making this effort possible.

On behalf of the Capstone team we would also like to express our sincere gratitude to the various individuals, including current and former U.S. Government personnel who have freely given their time in assisting this project.

Oyindamola Adegboro

John DeNicola

Kelsey Field

Evan Howlett

Takayuki Miyagawa

Rachel Paulk

Dara Stofenberg

Executive Summary

The U.S. Failed to Prevent the 9/11 Terrorist Attacks in Large Part Because of an Inability to Share Information Effectively, Both Within the Intelligence Community and With Law Enforcement Agencies. Subsequently the nation has undertaken major organizational and legislative changes that specifically target the problems in information sharing to support counter-terrorism efforts identified by the 9/11 Commission and others. In large part, these have sought to address the legal, cultural, and operational impediments to an information sharing environment. This has been an enormous task, amounting to the creation of a domestic intelligence capability and the integration of federal, state, local and tribal law enforcement into the broader national security community.

Legislation impacting information sharing has focused on providing a legal basis for disseminating sensitive information to new actors and altering the traditional "need-to-know" culture of the intelligence world. New laws, such as the Homeland Security Act of 2002 and the Intelligence Reform and Terrorism Protection Act of 2004—which reorganized intelligence agencies under the umbrella of a new Director of National Intelligence in an effort to garner greater intelligence collaboration—consistently fail to specify policies and procedures to ensure full cooperation and access to information.

In 2004, the Information Sharing Environment (ISE) Was Established to Facilitate the Exchange of Information Among Agencies as a Means of Enhancing U.S. Counter-Terrorism Efforts. Implementing and operating an effective Information Sharing Environment (ISE) has been a difficult task because of the size and scope of the Intelligence Community (IC), as well as the limitations on intelligence collection and sharing under existing statutes and Executive Orders from several Presidential Administrations. The challenge of addressing multiple issues engrained within agency culture, information security, the evolving concept of privacy protection, and architectural and technological frameworks has also hindered the information sharing process.

The Culture of Information Sharing

Although Advances in Information Technology and System Architecture are Important Elements for Proper Distribution, Culture Remains the Most Fundamental Impediment to Effective Information Sharing. Over the past decade the world has witnessed dramatic advances in information and communications technologies. At the same time as this technology was evolving, the nation embarked on the first major reorganization of national and homeland security since 1947. Bureaucratic resistance to change among the intelligence agencies, however, still persists. "Stovepiping" largely restricts the flow of information and obstructs a culture of integration. Training staff to both appreciate the importance of information sharing at all levels of operation and to share information effectively through existing and emerging mechanisms is essential to creating a "culture of trust."

Altering the culture of the IC will require further examination of the needs and functions of data stewards. Personnel and agency incentives, such as linking agency performance on

information sharing with program funding and offering an Agency Information-Sharing Award, should be presented to cultivate more meaningful change. Policies further encourage joint duty-like assignments will foster greater sharing and create communities of interest around specific topics. A culture that focuses more on inter-agency information sharing will enhance the integration of all counter-terrorism stakeholders, including those in the non-intelligence community.

Members of the non-Intelligence Community, such as state and local agencies and law enforcement, private entities, and the public are now essential counter-terrorism partners of the Federal Government. It is necessary that a unified, nation-wide training program for state and local officials and a consistent security policy for handling information be implemented in order to facilitate further information sharing among these actors.

Additionally, a federal vision is required to train and institute guidelines for local authorities so that they can establish good relationships with their local communities and collect information effectively from the public. These actions will further public awareness about the public's important role in counter-terrorism efforts.

Balancing the Responsibilities of Protection and Privacy

Sharing Information Among Governmental Entities Raises Many Concerns About The Protection of Privacy. In an environment where the sharing of information is actively encouraged for counter-terrorism purposes, additional care must be taken to ensure that individuals' privacy is respected and protected. Data entered into the Information Sharing Environment (ISE) must be adequately protected from unauthorized or inadvertent disclosure, unauthorized access and secondary use violations. It is critical that shared data is also verified vigorously for accuracy, completeness, and integrity.

The technology available to the IC, as well as federal, state and local law enforcement agencies, has rapidly advanced, making it easier to implement surveillance and monitoring systems. Existing legislation has proven inadequate to address the right to privacy in the world of ubiquitous public information created by technological advances.

Recently, the Supreme Court has begun to further address the issues related to privacy under the Fourth Amendment. Policies on privacy, civil liberties, and civil rights within the IC and the information sharing framework must be clarified to meet the evolving concept of privacy the Court has defined as well as constantly changing technological capabilities of the Government to collect, process and analyze data.

Currently, various interpretations of privacy policies exist across the Government. The lack of consistent interpretations of these policies has led to confusion on the analyst level. More work still needs to be done throughout the Government to clarify these issues and policies. There is also a need for a basic interpretation of key laws and statutes that govern the overall national security and law enforcement communities.

Maintaining Security for Shared Information

The Expansion of the Federal Government and Local Law Enforcements' Counter-terrorism Efforts After 9/11, Combined With The Increased Personnel Requirements of the War on Terrorism, to Create a Rapid Increase in the Number of Individuals Possessing Security Clearances. The dramatic increase in the number of cleared individuals requires additional procedural and personnel-based security policies to safeguard information from unauthorized disclosure.

The Federal Information Security Act (FISMA) of 2002 provides an important framework for safeguarding federal information and information systems, because it promotes information security that is based on risk assessments, cost effectiveness, and oversight. FISMA, however, is agency-oriented and lacks specific guidance for inter-agency efforts. Consequently, there is a need for an information security framework that is tailored to the ISE's needs.

While the concept of risk assessment outlined in Intelligence Community Directive Number 501 (ICD 501) is a necessary and important component of the Intelligence Community's information sharing policy, it too is incomplete. Risk assessment is a multi-dimensional process that requires a degree of standardized training and discipline. Accordingly, there is a need for a robust standardized risk management framework and training across the IC.

The Concept of "Authorized Use," Which Facilitates Greater Control Over Monitoring The Capability and Intent of Employees, Provides a New Operational Paradigm for the IC. "Authorized use," however, is predicated on the ability to define narrowly the core missions of ISE partner agencies and offices. In order to determine what type of information is necessary for whom and at which agency, there needs to be an unequivocal understanding of recipient partners' specific missions and designated roles. The main challenge to the creation of an atmosphere of trust within the ISE is the threat posed by ISE partners themselves—the insider threat. The IC must implement proper, government-wide procedures to identify and mitigate the insider threat.

Although the IC can be lauded for continuing information-sharing efforts in the aftermath of the *WikiLeaks* affair, the incident highlighted security vulnerabilities within the ISE. Government agencies have failed to integrate counter-intelligence procedures into some of their ISE activities, such as an implementation of audit logs to protect classified information from an insider threat. *WikiLeaks* also displayed the importance of creating common operational policies to ensure that agencies have an effective method for addressing insider threats. Moreover, universal policies will ultimately advance a culture of trust among ISE partners.

Architectures for Information Sharing

The ISE Requires a Secure, Interoperable Network to Function Successfully. Discoverability, tagging, auditing, "authorized use" standards, and anonymization are key information sharing architectural features that can strengthen the ISE's mission to enhance national

security. Integration and interoperability of Sensitive But Unclassified (SBU)/Controlled Unclassified Information (CUI) and Secret networks across federal and non-federal partners will ensure further collaboration.

Fusion Centers—Designed to Consolidate and Analyze Information—Exist at the Federal, State and Local Levels and are Chiefly Organized in Two Models: a Centralized Model, Represented by the National Counterterrorism Center (NCTC); and a Decentralized Model, Represented by Fusion Centers. Centralized models provide a structure for information sharing with unique advantages and challenges. They are arguably the easiest prototypes of information sharing to implement. To be effective, however, a centralized database requires: data to be populated and updated frequently; data to be submitted and catalogued in a standardized format; and an audit log to be maintained to monitor users' activities.

Decentralized models of information sharing have different advantages and disadvantages from centralized models, and can provide a viable alternative. The core goals of a decentralized model are to ensure collaboration among key intelligence partners and to foster an environment where contributing agencies are actively exchanging key pieces of intelligence. For this model to work effectively, true equality among partners is critical in the sharing relationship, as well as a shared responsibility for the final analytics product.

Both Centralized and Decentralized Information Sharing Architectures Have Shortcomings. In several key areas, one system may be better suited to perform a specific task, but neither system is flawless. Fusion centers and the NCTC represent two distinct models, both with many advantages but also shortcomings. With both systems currently operational, the IC is able to extract the positives from each model and incorporate them into a future system. Although there is current debate over which system to implement, the system of the future will most likely represent a hybrid model that incorporates aspects from both. It seems that "cloud computing" will help to resolve many of the shortcomings currently plaguing the existing systems.

While cloud computing will offer a modern IT platform that is capable of removing IT barriers for information sharing, other obstacles, such as cultural aversion to sharing, have to be addressed before any IT system—cloud or otherwise—is effective. The cloud will ensure that the most critical aspects of information sharing, discoverability, and access will be utilized. Nonetheless, cloud computing is incapable of ensuring an integrated IC community on its own.

Metrics for Information Sharing – How Well Are We Doing?

A Decade has Passed Since 9/11 Without Another Major Terrorist Attack Occurring on U.S. Soil. It is too early, however, to declare U.S. efforts to secure the homeland a definitive success. Luck has contributed significantly to the failure of terrorist plots over the past decade. The incompetence that has characterized several terrorist plots will ultimately end as individuals become more experienced and adapt. As a result, there still exists an urgent need to continue enhancing the mechanisms that facilitate information sharing. Today, counter-terrorism information sharing efforts remain insufficient to protect against

increasingly sophisticated actors. The answer to the question of whether the U.S. is truly safer today remains opaque. The effectiveness of counter-terrorism policies is inherently difficult to measure.

The IC has made significant progress in transforming its culture from one of "need-to-know" to "need-to-share." In a way, the information exposed by the *Wikileaks* incident is a testament to how far the IC has progressed culturally in the last ten years. Although many believed that the exposure would hinder the information sharing culture, the IC continued on the trajectory of becoming more cooperative. The IC must bear in mind, however, that appropriate security procedures and system architecture too are fundamental components of counter-terrorism information sharing efforts.

Interoperability Between IT Structures and Data in the IC is a Key Measure of Progress for Information Integration. Information sharing will never be fully automated without universal language and definitions for data, and a common platform for dialogue and exchange regarding implementation. Automated information sharing is only possible if information is stored on an accessible IT platform, which requires agencies to address any shortcomings in data treatment. Additionally, to continue the widespread dissemination of information, agencies must identify realistic training measures and procedures that respect their individual protocols for treating and handling collected data. The need for the ability to discover information has been addressed by the Office of the Director of National Intelligence (ODNI) and underscored in the Intelligence Community Directive Number 501 (ICD 501).

In order to support greater information sharing throughout the law enforcement, defense and intelligence, public safety, homeland security, and foreign affairs communities, the ability to discover information is crucial and becomes a necessary feature in any future architectural landscape. In 2009, the ODNI issued ICD 501, to "strengthen the sharing, integration and management of information within the IC, and establishes policies for: (1) discovery; and (2) dissemination or retrieval of intelligence and intelligence-related information collected or analysis produced by the IC."[1]

This directive emphasizes the importance of being able to discover information. The directive mandates "IC elements [to] fulfill their 'responsibility to provide' by making all intelligence-related information that IC divisions are authorized to acquire, collect, hold, obtain and analyze discoverable through automated means by "authorized IC personnel."[2]

In the Current Fiscal Environment, Budgetary Constraint is a Factor That Must be Addressed. The viability of expanding intelligence sharing under monetary restrictions is a daunting task, and decreasing budgets will be a challenge for all federal agencies and departments for the foreseeable future. Ironically for information sharing, budget constraints may help to increase sharing by encouraging efficiencies that can achieved through inter-agency cooperation, forcing a removal of stovepipes.

---

[1] Office of the Director of National Intelligence, *Intelligence Community Directive Number 501: Discovery and Dissemination or Retrieval of Information within the Intelligence Community* (Washington, DC, 2009), 1, http://www.dni.gov/electronic_reading_room/ ICD_501.pdf.
[2] *Ibid.*

Intelligence agencies and departments will no longer have the resources to engineer and implement their own systems. Fiscal constraint will force the IC to aggregate funds and develop collective systems that incorporate input from multiple members of the IC. Forced integration will help to standardize the systems and make them interoperable, such as efforts by NSA and CIA to spearhead the effort to design and implement a cloud system, estimated to be released in roughly two years.

The 2007 National Strategy for Information Sharing, Developed by the ISE, Has Strengthened Collaboration. Many agencies and departments have implemented the strategies recommended by the ISE. While there are areas that require improvement, in general the ISE has been instrumental in providing a framework and metric for success.

Several general key future initiatives that require future investment from the ISE include:

1. Acceleration of the development and adoption of common standards through common architecture and shared training initiatives.

2. Improvement of the interoperability of inter-agency networks.

3. Implementation of an inter-agency architectural system (Cloud System).

4. Fortification of means for rapidly disseminating both classified and unclassified terrorist information between federal, state, local and tribal entities.

5. Strengthening of intelligence sharing between the IC and State, Local, Tribal and Private Sector (SLTPS).

6. Streamlining and standardization of discoverability processes.

Federal counter-terrorism efforts will, out of necessity, continue to expand into the foreseeable future. An enhanced and more effective Information Sharing Environment will provide the responsible federal agencies, as well as state and local law enforcement authorities, with increased capabilities, notice, and information to use to combat the threats that potential terrorists present. The system will, however, require the constant attention and oversight of Congress and the American public to ensure that it is operating in a manner that: facilitates the useful sharing of information; protects intelligence sources and methods; respects individual privacy rights; and efficiently utilizes limited Government resources.

Introduction

In the decade following the 9/11 terrorist attacks on the United States, significant efforts have been made to improve the nation's ability to detect future attacks and respond effectively to the range of evolving threats. Major legislative and organizational changes have been made to U.S. intelligence capabilities to deal with new domestic threats as well as foreign adversaries, and to deal effectively with the new technologies employed by these adversaries. Key components of this approach have allowed for a better integration of intelligence and law enforcement activities at the federal level, as well as the inclusion of state and local law enforcement agencies in the counter-terrorism process.

Essential to these efforts has been the creation of an information sharing environment that is timely, securely and widely available to those throughout the country working to protect U.S. national security. Throughout this critical decade The Markle Foundation has been a staunch advocate promoting of the mobilization of information across agencies in order to enhance current national security policies.

A key focus of these efforts has been the elimination of the "stovepiping" of information and other impediments that hindered counter-terrorism collaboration prior to the 9/11 attacks. Although considerable progress has been made, continued agency resistance to change and various other obstacles continue to hamper the effective implementation of legislation that has been passed since 9/11 to promote and, in some instances, mandate inter-agency collaboration.

One significant obstruction to the wide sharing of information has been uncertainty about the legality of information sharing under existing statutes, new legislation, and recent court decisions on the constitutional right to privacy. As new legislation is enacted and laws are reviewed by the courts, a balance between liberty and security must be achieved that ensures that essential intelligence is collected and disseminated to the appropriate agencies while at the same time respecting the privacy rights granted by the U.S. Constitution and the Bill of Rights.

Apart from legislative and organizational changes, the past decade has also seen radical changes in technology, surveillance capabilities, as well as how the various federal courts have viewed these abilities. This delicate balancing act is further exacerbated by failures identified in intelligence and law enforcement efforts prior to 9/11: the fact that grossly inadequate counter-terrorism efforts and a failure to share information led to the disastrous losses of 9/11.

While legislators and policy makers have made concerted efforts to create and enforce an information sharing environment among intelligence and law enforcement agencies, decades of distrust, differing cultures, and competition for resources continue to obstruct major institutional change. Non-federal counter-terrorism units, such as the NYPD, have in many ways overshadowed the counter-terrorism capabilities of the FBI in the New York area, and demonstrate that earlier distinctions between domestic and foreign intelligence are obsolete. New organizational alternatives such as the National Counterterrorism

Center (NCTC), the various regional fusion centers, joint terrorism task forces (JTTFs), and joint regional intelligence centers (JRICs) have made substantial headway in meeting the goal for effective information sharing, but much remains to be done.

Despite major legislative efforts such as the Homeland Security Act of 2002 and the Intelligence Reform and Terrorism Protection Act of 2004, which sought to reorganize all intelligence agencies under the umbrella of a new Director of National Intelligence and ensure intelligence collaboration, laws have consistently failed to specify operating policies and procedures that would ensure cooperation and access to information.

This report was undertaken in an effort to first assess where the nation stands today with respect to information sharing and the progress made in the decade since 9/11, and to provide an evaluation of where the nation stands now in this critical area in terms of progress toward an optimal information sharing environment. Based on an assessment of specific metrics, a second objective has been to provide insight into how the nation can move ahead in meeting critical objectives for information sharing to support counter-terrorism efforts in the future.

Various studies and reports have addressed the current state of information sharing and the direction in which it may head. The present analysis, however, specifically targets how the relevant agencies might improve information sharing, decrease the risk of security breaches and leaks, and respect individual privacy rights.

In particular, this report addresses the need for strong leadership to encourage collaboration, and move from a "need-to-know" culture to one that is increasingly focused on the "need-to-share." Moreover, U.S. law needs to address the specific role that state and local law enforcement will play in national security, and how these organizations can meet their intelligence requirements when interacting with the relevant federal agencies. Finally, this report targets the current information sharing architecture, comparing the relative advantages and disadvantages of centralized and decentralized models in an effort to suggest possible improvements in the existing architecture that would facilitate increased information sharing.

Information Sharing – Where We are Today

Legislative History of U.S. Intelligence Activities Pre-9/11

The National Security Act of 1947

Reorganization of the U.S. Military and Intelligence Community. Following the end of World War II, the U.S. Government recognized the importance of establishing a national security system that balanced diplomacy, military strength and intelligence collection that was responsive to evolving Cold War requirements. The surprise attack on Pearl Harbor in 1941 and subsequent investigation into the intelligence failures led to Congressional demands for an overhaul of the wartime intelligence community to better coordinate between the competing agencies that existed at the time.[3] Congressional policy goals for the 1947 National Security Act were straightforward and clear:

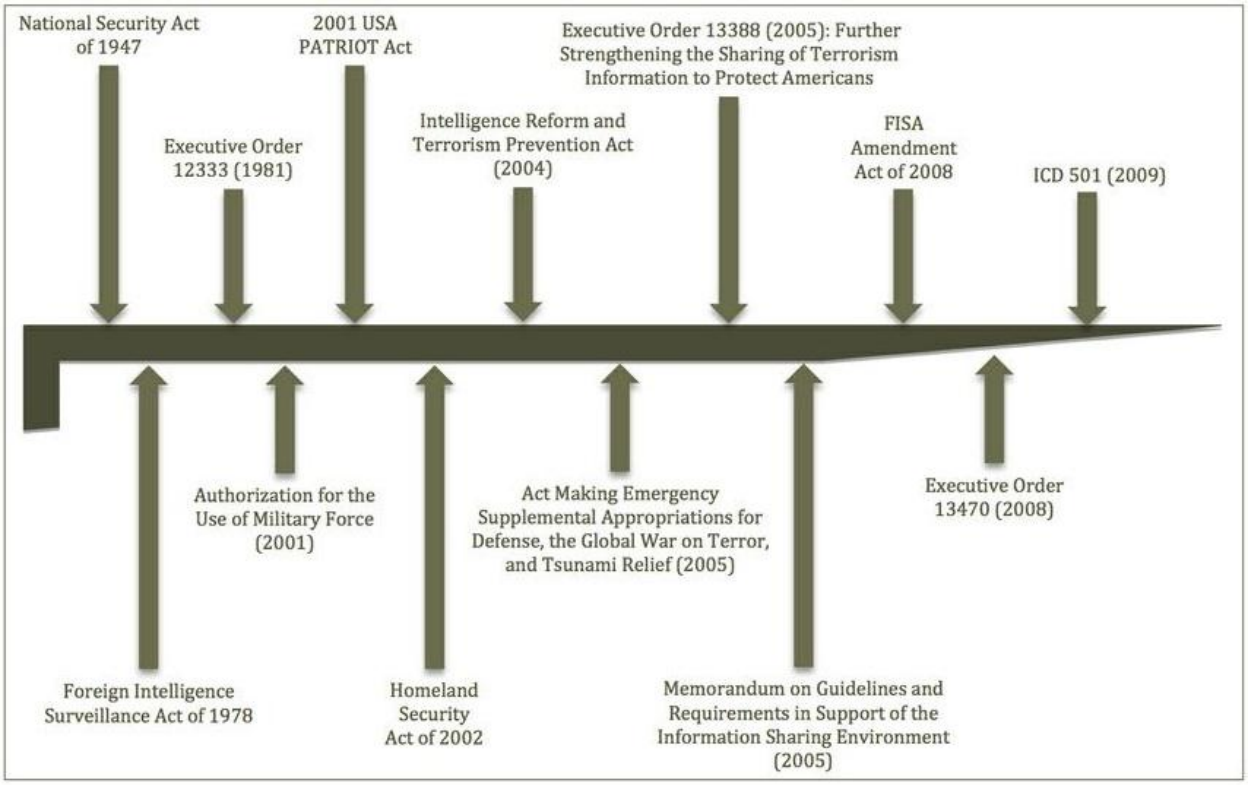

Fig 2.1 – The Evolution of Intelligence Law in the U.S.

[3] Michael Warner, "Legal Echoes: The National Security Act of 1947 and the Intelligence Reform and Terrorism Prevention Act of 2004," *Stanford Law and Policy Review* 17, no. 2 (2006): 303.

> "In enacting this legislation, it is the intent of Congress to provide a comprehensive program for the future security of the United States; to provide for the establishment of integrated policies and procedures for the departments, agencies, and functions of the Government relating to the national security; to provide three military departments for the operation and administration of the Army, the Navy (including naval aviation and the United States Marine Corps), and the Air Force, with their assigned combat and service components; to provide for their authoritative coordination and unified direction under civilian control but not to merge them; to provide for the effective strategic direction of the armed forces and for their operation under unified control and for their integration into an efficient team of land, naval, and air forces."
>
> *National Security Act of 1947*, July 1947

The re-organization of the national security establishment was a top-down approach ensuring the President would receive advice from a wide range of civilian and military personnel in order to make informed decisions.[4] Throughout WW-II, a general consensus understood that the U.S. required a small, centralized body to make executive decisions, with complete control over military forces, to ensure victory over Axis powers.[5] The National Security Act of 1947 reflected this policy, centralizing control over the military in the newly-created Department of Defense with a single Cabinet Secretary.

Signed into law on July 27, 1947, the Act established the framework for an integrated national security system. The Act also provided the basis for the creation of several security institutions, including the National Security Council (NSC), the Central Intelligence Group (CIG) – renamed the Central Intelligence Agency (CIA) the following year – and the Department of Defense (DoD), with the intention of institutionalizing the relationship between foreign and domestic security policy.[6]

The security re-organization and creation of the DoD also resulted in three military services – the Army, Navy and a newly created Air Force which had previously been a part of the Army, under the Department of War.[7] Although separated, the three services were placed under the control of the new Secretary of Defense, the DoD, and the Joint Chiefs of Staff as a means of ensuring collaboration. A critical responsibility for the Secretary of Defense was the role of principle advisor to the President, although this role was limited to matters that directly concerned the Department of Defense.[8]

---

[4] Charles A. Stevenson, "Underlying Assumptions of the National Security Act of 1947," *Joint Force Quarterly*, no. 48 (2008): 129-33, http://www.ndu.edu/press/lib/pdf/jfq-48/JFQ-48.pdf.
[5] Barry H. Steiner, "Policy Organization in American Security Affairs: An Assessment," *Public Administration Review* (1977): 359.
[6] Cody M. Brown, "The National Security Council: A Legal History of the President's Most Powerful Advisors," *Project on National Security Reform* (2008): *6*, http://www.pnsr.org/data/images/the%20national%20security%20council.pdf.
[7] Steiner, "Policy Organization in American Security Affairs: An Assessment," 360.
[8] Brown, "The National Security Council: A Legal History of the President's Most Powerful Advisors," 8.

A major consequence of restricting the scope of the Defense Secretary's advice involved an absence of intelligence beyond the capacity of the DoD being reported to the President.[9] While the Act created an Intelligence Community (IC), it failed to position the IC as a Cabinet-level department or create a Cabinet secretary as its highest vocal authority.

One critical aspect of the Act included the establishment of the National Security Council (NSC), composed by the President, the Secretary of State, the Secretary of Defense and the Director of the Office of Defense Mobilization (which would be merged into the Federal Emergency Management Agency, FEMA). The creation of the NSC was a Congressional effort to ensure that the President had access to a wide variety of military and civilian opinions, in order to prevent a re-occurrence of a problem experienced during the Roosevelt Presidency where the civilian viewpoint had been largely excluded.

The Truman administration, however, considered the NSC an attempt by policy makers to cap Presidential powers regarding national security decisions, and therefore purposefully maintained the NSC as a relatively weak institution.[10] Despite Truman's antagonism, the NSC had been purposefully formulated to remain a stable organization despite changes in leadership, with specific senior-level individuals participating in national security policy making on a consistent basis.[11]

Under the Act, a number of agencies were placed under the command of the DoD, including the Departments of the Army, Navy, Air Force, the War Council, the Joint Chiefs of Staff, a Joint Staff, the Munitions Board, and the Research and Development Board. Nevertheless, the CIA remained an independent agency placed under the jurisdiction of the NSC, as a means of coordinating intelligence operations of the various departments and agencies having interest or operations in national security.[12] A major factor in the creation of the CIA was the post-Pearl Harbor perception that the U.S. lacked a unified intelligence structure which prevented adequate intelligence analysis and access to senior-level decision makers.[13] The decision to separate the military services from the CIA, however, created a culture of competition, with the individual agencies excluding the others in the collection and dissemination of their intelligence.[14]

Ultimately the 1947 Act provided an institutional framework for each of the organizations and defined how they would contribute to national security. Additionally, it served as the foundation for intelligence activities conducted internationally and domestically, and remained substantially unaltered until the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). It provided a critical framework for the Intelligence Community, as the technological advancement of capabilities such as overhead photography and signals

[9] *Ibid*.
[10] *Ibid*.
[11] Steiner, "Policy Organization in American Security Affairs: An Assessment," 360.
[12] Brown, "The National Security Council: A Legal History of the President's Most Powerful Advisors," iii.
[13] Steiner, "Policy Organization in American Security Affairs: An Assessment," 360.
[14] *Ibid.,* 361.

intelligence greatly increased U.S. capacity for information collection during the Cold War era.[15]

Advancing intelligence collection capabilities empowered the CIA as the nation's primary foreign intelligence branch, though it remained excluded from any domestic intelligence mission by statute.[16] This mandate gave the CIA jurisdiction to support the President and execute clandestine operations abroad for national security goals, while also providing the NSC with accurate information for the assessment of national security threats.[17] To fulfill this objective, the CIA was allowed substantial independence from the other agencies, operating with an independent budget and access to intelligence collected by other IC agencies.

Although the Director of Central Intelligence (DCI) had the power to review and disseminate intelligence gathered by other agencies, restrictions significantly isolated the intelligence agencies from sharing information.[18] These measures prevented other intelligence and law enforcement agencies from accessing the majority of information collected by the CIA, as it was deemed out of the jurisdiction of departments and agencies whose primary responsibility was domestic security, largely considered a law enforcement matter.[19]

Domestic security remained largely the responsibility of the FBI, expected to prevent foreign penetration into the U.S. Yet the FBI was categorically restricted from performing domestic intelligence functions, explicitly categorized as not a domestic intelligence service, contrasting with the model of Great Britain's MI-5.[20] The decision to separate domestic from foreign intelligence collection was in large part an effort to ensure U.S. civil rights would not be threatened by collections tactics. Unlike the CIA, however, which was intended to be a clearinghouse of information, each of the domestic agencies operated on an independent basis, competing with one another to obtain and hold crucial information that would set them apart from the other services.[21]

Each agencies' relative operational independence compounded during the height of the Cold War, when suspicion and refusal to collaborate resulted in the "stovepiping" of information. Each of the military services, including the Department of State, maintained their own intelligence agencies which provided specialized tactical intelligence to their commanders, producing biased intelligence based on the military branch of the submitting agency.[22] In an effort to rectify this problem, President Kennedy tasked Defense Secretary Robert McNamara to consolidate the military intelligence units under a single director,

---

[15] Warner, "Legal Echoes: The National Security Act of 1947 and the Intelligence Reform and Terrorism Prevention Act of 2004," 303.
[16] *Ibid.*
[17] *Ibid.,* 309.
[18] John H. Hedley, "The Evolution of Intelligence Analysis," *Analyzing Intelligence: Origins, Obstacles,* ed. Z. Roger et al. (Washington, DC: Georgetown University Press, 2008), 21.
[19] *Ibid.*
[20] *Ibid.*
[21] Gregory F. Treverton, *Reorganizing U.S. Domestic Intelligence: Assessing the Options* (Santa Monica, CA: RAND Corporation, 2008), 8, http://www.rand.org/pubs/monographs/MG767.
[22] Hedley, "The Evolution of Intelligence Analysis," 21.

leading to the creation of the Defense Intelligence Agency (DIA) in 1961.[23] Under a classified directive the National Security Agency (NSA) was also created as a DoD agency to provide signals intelligence for the entire IC, as well as encryption and related security services to the entire Government as the Central Security Service (CSS).[24]

Title III of the Omnibus Crime Control and Safe Streets Act of 1968

The Role of Privacy in Electronic Intelligence Collection. To better define the balance between the rights of private citizens and the need of law enforcement to collect intelligence, Congress enacted the Federal Wiretap Act of 1968 as a part of the Omnibus Crime Control and Safe Streets Act.[25] Title III was in large part a reaction to the U.S. Supreme Court decision in *Katz v. United States* (1967), which overturned the Supreme Court decision in *Olmstead v. United States* (1928), and extended Fourth Amendment right to privacy protection to electronic communications where the Court now held that a citizen had a reasonable expectation of privacy in the use of the telephone and telegraph.[26]

The FBI's extensive use of wiretaps also significantly influenced Title III, as these wiretaps targeted a wide range of members of government, as well as Supreme Court Justices and Congressional staff.[27] Title III provided a means to systematize the legal access to electronic surveillance, with stringent requirements necessary to obtain a warrant for electronic surveillance in criminal investigations. The rapid advancement of technology and expansion of intelligence surveillance activities, however, demanded a re-assessment of the overall legal regime under which electronic surveillance could be conducted.

The Foreign Intelligence Surveillance Act of 1978 (FISA)

Congressional Oversight Streamlines Foreign Surveillance. Immediately following the 1973 Watergate scandal, the *New York Times* published a story accusing the CIA of operating large-scale domestic intelligence surveillance against anti-war dissidents, opposing political leaders and civil rights activists.[28] According to *Times* reporter Seymour Hersh, more than 10,000 American civilians had been victims of warrantless surveillance which included break-ins, wire-tapping and clandestine inspection of mail. The report provoked an outburst of public indignation and sparked demands to reign in the power granted to intelligence agencies.[29]

---

[23] *Ibid.,* 29.
[24] The agency still retains the formal title of National Security Agency/Central Security Service (NSA/CSS) and continues to provide these services to all Government agencies and departments.
[25] Shana K. Rahavy, "The Federal Wiretap Act: the Permissible Scope of Eavesdropping in the Family Home," *Journal of High Technology Law* (2003): 88.
[26] Prior to *Olmstead* in 1928 the Supreme Court had not considered the Fourth Amendment privacy issue in electronic intercept.
[27] Susan Landau, "National Security on the Line." *Journal of Telecommunication and High Technology Law*. 4, no. 2 (2006): 416, http://ssrn.com/abstract=1166155.
[28] Seymour Hersh, "Huge C.I.A. Operation Reported in U.S. Against Antiwar Forces, Other Dissidents in Nixon Years," *New York Times*, December 22, 1974.
[29] Brian A. Jackson, ed., *The Challenge of Domestic Intelligence in a Free Society: A Multidisciplinary Look at the Creation of a U.S. Domestic Counter-terrorism Agency* (Santa Monica, CA: RAND, 2009), 38.

A series of Senate Committees, including the Church and Pike Commissions, were established in order to investigate the allegations, all of which recommended different policy prescriptions for consolidating and streamlining the Intelligence Community, resulting in a series of Executive Orders that transformed the role of the DCI and vested Congressional oversight authority in both Senate and House select committees on intelligence.

Of the various committees established, the Church Commission was charged with the investigation of all intelligence agencies and activities, culminating in a report that outlined 183 policy change recommendations for the IC.[30] Following the release of the Church Committee Report in the 1970s, which revealed the FBI's domestic intelligence program known as "Operation CHAOS" included unlawful wiretaps and surveillance, Congress passed the Foreign Intelligence Surveillance Act of 1978 (FISA) to federally regulate intelligence collection.[31]

Prior to FISA, the Attorney General had the power to authorize the surveillance of foreign nationals and powers without any higher form of supervision, authority which the Church Commission called into question.[32] Consequentially, a newly established FISA Court was appointed to review government requests for electronic surveillance involving U.S. citizens and foreigners, which stipulated that domestic surveillance could only occur if it was in the pursuit of national foreign intelligence.[33]

FISA was intended to provide judicial supervision over the Executive Office that would serve as a checks and balances oversight of intelligence operations.[34] To obtain a warrant for electronic surveillance in pursuit of national security, one of the 11 judges on the Foreign Intelligence Surveillance Court (FISC) needed to identify probable cause to verify the intended target's status as a foreign entity. The FISC's primary objective, intended to facilitate a streamlined legal process, included ensuring foreign investigations were not impeded by bureaucracy.[35] Additionally, FISA provided legal coverage for the nation's telecommunications carriers, specifically AT&T at the time, whose assistance—essential to IC collection operations—risked targeting from federal lawsuits.

The decision to separate criminal investigations from intelligence operations in national security was influenced by the highly sensitive nature of the latter, as courts were concerned that the legal obstacles involved in a domestic surveillance warrant would hinder counter-terrorism efforts and the subsequent trials of suspected terrorists.[36] In the

---

[30] Richard A. Best Jr., *Proposals for Intelligence Reform: 1949-2004* (Washington DC: Congressional Research Services, 2004), 41.
[31] Thomas H. Kean et al., *The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States,* (Washington, DC: U.S. Government Printing Office, 2004), 95, http://www.gpo.gov/fdsys/pkg/GPO-911REPORT/pdf/GPO-911REPORT.pdf
[32] Hedley, "The Evolution of Intelligence Analysis," 29.
[33] Jackson, *The Challenge of Domestic Intelligence in a Free Society: A Multidisciplinary Look at the Creation of a U.S. Domestic Counter-terrorism Agency*, 38.
[34] Nora K. Breglio, "Leaving FISA Behind: The Need to Return To Warrantless Foreign Intelligence Surveillance," *The Yale Law Journal* (2003): 184.
[35] *Ibid.*
[36] *Ibid*., 185.

decades following the Church Committee and the Watergate scandal, the importance of protecting civil liberties experienced a renewed emphasis. Over time, this resulted in an extremely complex, bureaucratic process which dissuaded many from pursuing FISA warrants.

Executive Order 12333 (1981)

Further Defining the Centralization of the Intelligence Community. The Church Committee also resulted in a series of Executive Orders (EO) that defined the missions, responsibilities and roles of the various intelligence agencies. Addressing accusations of U.S. involvement in assassination attempts against foreign leaders, President Ford issued Executive Order 11905 in 1976 which instituted four important reforms:

1. Created a National Security Committee on Foreign Intelligence, to be headed by the DCI who would be the President's primary intelligence advisor and spokesperson for the greater IC.

2. Replaced the 40 Committee, a division of the Executive Branch of the U.S. Government which reviewed major covert actions, with the Operations Advisory Group, which would oversee covert activities. This group would be headed by senior White House, CIA, State Department, and DoD representatives.

3. Established a part-time Intelligence Oversight Board, who was to report illegal activity to the Attorney General and improprieties to the President.

4. Banned the practice of political assassination.[37]

The Ford administration's Executive Order reflected attempts to restrain the increasing power of the IC, and put into place legal standards for operations. Upon Ronald Regan's election in 1981, however, Regan enacted Executive Order 12333 to expand the IC's ability to conduct foreign intelligence operations. Additionally, Executive Order 12333 furthered prior assassination bans by declaring the illegality of political assassinations by a U.S. Government employee, or acting on the behalf of the Government.[38] All the bans, however, lacked a clear definition of "assassination," resulting in a somewhat cryptic understanding of what would constitute murder for political purposes.[39]

Finally, EO 12333 attempted to centralize intelligence, by granting the DCI "full responsibility for the production and dissemination of national foreign intelligence," with the expectation that agencies would cooperate across departments.[40] In spite of these efforts to promote information sharing, however, the DCI remained a weak institution that was unable to supersede the culture of "need-to-know" within the IC.

---

[37] Exec. Order No. 11,905 3 C.F.R. 11 (1976).
[38] Exec. Order No. 12,333 46 F.R. 59941 3 C.F.R. (1981). In actuality, EO 12333 did not expand greatly on the predecessor EO 12056.
[39] Elizabeth B. Bazan, *Assassination Ban and E.O. 12333: A Brief Summary* (Washington DC: Congressional Research Service, 2002), 2, http://digital.library.unt.edu/ark:/67531/metacrs2392/.
[40] Best, *Proposals for Intelligence Reform: 1949-2004,* 31.

Intelligence in the 1990s – A New Focus on the Third World and Non-State Actors

Meeting the New Threats. Proceeding the decades defined by expansions and retractions of the capacities of the intelligence agencies, the need for greater collaboration and improved information sharing became a critical goal in the aftermath of the 1993 World Trade Center attacks. With the demise of the Soviet Union in 1991, foreign intelligence began to focus on national security threats arising from non-state actors, such as terrorists, demanding new tactics and methods in gaining critical intelligence. The 1993 plot emphasized the changing security threats against the U.S., and the criticality of understanding the new enemy. Although the plot ultimately failed, the failure to disseminate intelligence collected by the different agencies was brought under scrutiny, leading to a series of policies and laws that further clarified the relationship between intelligence and criminal investigations, and the role that the individual intelligence agencies would play.

1995 Department of Justice Guidelines

Enactment of Information Sharing Procedures. Throughout the 1990's, the Intelligence Community underwent a series of institutional changes meant to counter inter-agency rivalry and promote information sharing. Evaluations of the situation at the time determined that the current state of the IC required a centralization of agencies to develop a cohesive community capable of providing timely and relevant intelligence briefings to the policy makers.[41]

In 1994, the court trial of Aldrich Ames, a spy whose conviction was jeopardized by the collaboration between the FBI and the criminal prosecutors, led to a review of information sharing oversight. The aftermath of the 1993 World Trade Center attacks catalyzed attempts to enhance intelligence sharing between local and federal agencies, resulting in the arrest of four men.[42] Under the guidance of Richard Struggs, acting head of the DoJ's Office of Intelligence Policy and Review, information sharing procedures for FISA materials began to be instituted in federal law enforcement.

FISA was extended in 1995 with the Department of Justice Guidelines which stated that information obtained in the course of foreign counter-terrorism relating to future terrorist attacks could not be exchanged with criminal investigators.[43] The "Procedures-for Contacts between the FBI and the Criminal Division Concerning Foreign Intelligence and Foreign Counterintelligence Investigations Guidelines" required that the Criminal Division be notified when foreign intelligence revealed that a federal crime was or would be committed.[44]

---

[41] *Ibid*.
[42] Kean et al., *The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States,* 88.
[43] Nathan Alexander Sales, "Share and Share Alike: Intelligence Agencies and Information Sharing," *The George Washington Law Review* (2010): 281.
[44] Barbara A. Grewe, *Legal Barriers to Information Sharing: The Erection of a Wall Between Intelligence and Law Enforcement Investigations* (Washington, DC: Commission on Terrorist Attacks Upon the United States, 2004), 2.

Although original drafts of the 1995 DoJ Guidelines stipulated that centralized intelligence sharing would be led by the Office of Intelligence Policy and Review (OIPR), which would be charged with collection and dissemination of intelligence, it was determined that intelligence agencies would be individually responsible for sharing relevant information.[45]

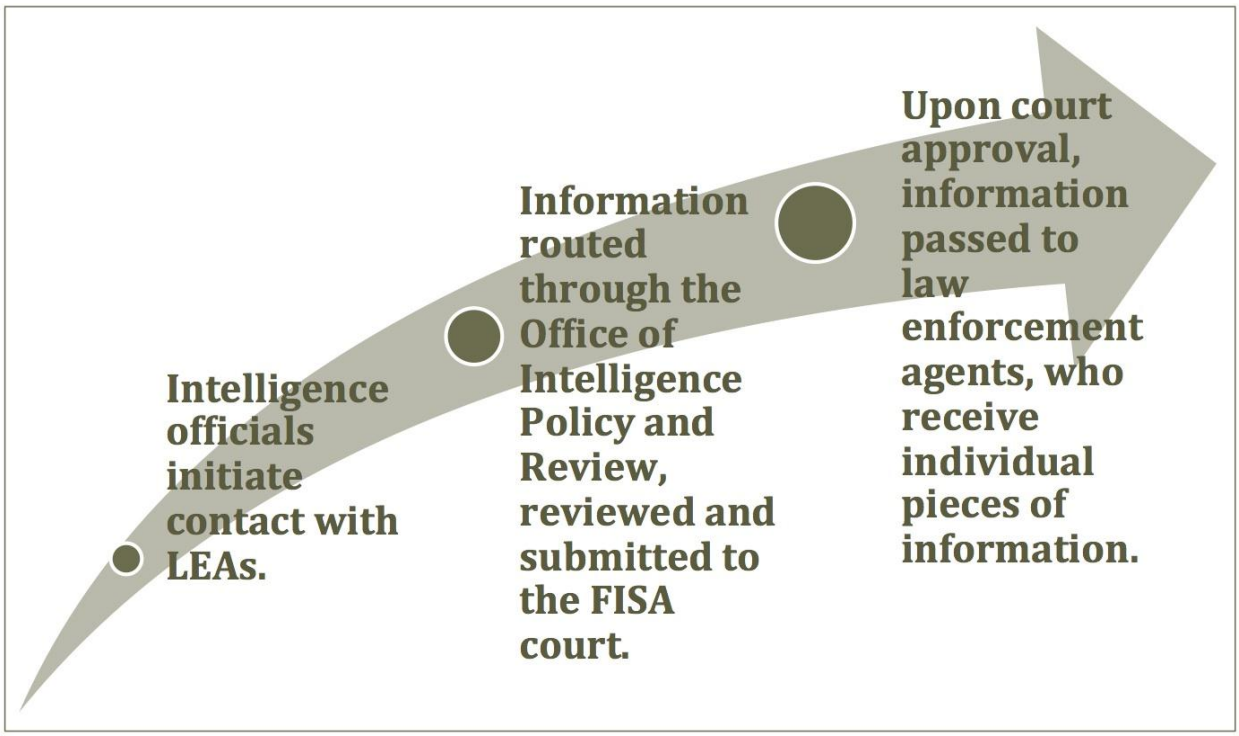

Fig 2.2 – Intelligence Flow and Approval under FISA

Although the DoJ guidelines did not specifically stipulate a "wall" between agencies, cultural attitudes exaggerated the regulations on information sharing. The OIPR became the single gatekeeper of information intended for distribution to the Criminal Division, threatening the FBI with the cessation of presenting warrant requests to the FISA court if its jurisdiction no longer included the regulation of information flows.[46] This perception was evident within other agencies, which would not cooperate with inter-agency employees working on criminal cases.[47] In reality, this refusal to cooperate resulted partially from underlying bureaucratic and culture issues, but a sincere concern also prevailed among the agencies that intelligence information used in trials would compromise sensitive intelligence sources and methods.

The 1878 Posse Comitatus Act also further hinders information sharing, as it prohibits the military from acting in a law enforcement capacity, with the intention of preventing undue policy influence.[48] Although the law was originally enacted to hinder a military coup of the U.S. Government following the Civil War, it has since been re-interpreted in the recent War

[45] *Ibid*.
[46] Kean et al., *The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States,* 95.
[47] *Ibid.*
[48] Sales, "Share and Share Alike: Intelligence Agencies and Information Sharing," 283.

on Terror. In the case of a domestic terrorist attack, Posse Comitatus prevents military services from pooling resources with other agencies, utilizing assets such as satellite imagery analysis or forensic DNA testing.[49]

Expansion of Surveillance Following 9/11 to Support Counter-Terrorism Efforts – Working to Promote an Information Sharing Environment

The United States of America Patriot Act of 2001

The U.S. Government Eases Constraints on Intelligence Sharing Between Law Enforcement and the Intelligence Community. The 9/11 attacks on New York and Washington D.C. marked a major turning point for the Intelligence Community and led to a series of major organizational and policy changes to the overarching structure of the national security community. An immediate assessment following the attacks concluded that excessive safeguards previously enacted to protect civil liberties resulted in dramatic damages to national security.[50] To counteract this imbalance, a series of legislation was introduced to mitigate the constraints placed on the IC. President George W. Bush signed the first piece of legislation, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, otherwise known as the USA Patriot Act, on October 26, 2001.

The USA Patriot Act made significant changes to the separation between law enforcement and foreign intelligence officials and eased many of the prior restrictions hindering intelligence sharing. The FISA Amendments within the Patriot Act altered many of the original provisions of the Church Committee, resulting in redefining the importance of foreign intelligence as a "significant purpose" but no longer a primary reason for covert operations.[51] The 2008 FISA Amendments Act includes the following key provisions:[52]

1. Section 215 authorized the collaboration between federal authorities and law enforcement officers for investigations of foreign powers and their partners, allowing for the sharing of intercepted information between local and federal authorities.

2. Traditional wiretapping, internet activity, email and voicemail can now be monitored with limited court oversight.

3. Section 206 permits multi-point, or "roving" wiretaps, which addresses the introduction of cellular technology versus traditional landlines.

---

[49] *Ibid.*
[50] Jackson, *The Challenge of Domestic Intelligence in a Free Society: A Multidisciplinary Look at the Creation of a U.S. Domestic Counter-terrorism Agency*, 43.
[51] Jason B. J Jones, "The Necessity of Federal Intelligence Sharing with Sub-Federal Agencies," *Texas Review of Law and Politics* (2011): 192, http://www.trolp.org/main_pgs/issues/v16n1/Jones.pdf.
[52] The Constitutionality of the 2008 FISA Amendments Act is currently being challenged in federal court in New York, under *Amnesty v. Clapper* (SDNY). Presumably this challenge will again go to the Second Circuit Court of Appeals and the Supreme Court.

4. Protects telecommunications companies from lawsuits for "'past or future cooperation' with federal law enforcement authorities and will assist the intelligence community in determining the plans of terrorists."

5. Increased the time for warrantless surveillance from 48 hours to 7 days, if the FISA court is notified and receives an application, specific officials sign the emergency notification, and relates to a U.S person located outside of the U.S with probable cause they are an agent of a foreign power.

6. Permits the Director of National Intelligence and the Attorney General to jointly authorize warrantless electronic surveillance, for 1-year periods, targeted at a foreigner who is abroad.

7. Allows eavesdropping in emergencies without court approval, providing that the Government files the required papers within a week.[53]

Section 203 of the Patriot Act amended the Federal Rules of Criminal Procedure (FRCrP) to permit the sharing of grand jury information involving foreign intelligence with federal law enforcement. It further stipulated that law enforcement officers are mandated to share information dealing with foreign intelligence gathered under Title III with federal law enforcement officers.[54] The Act lacked, however, any specific consequences for refusal to collaborate and did not target a main proponent of "stovepiping," traditionally the IC culture.

The Patriot Act further addressed the legal and perceived restraints on the flow of information. Section 504 states intelligence officials "may consult with Federal law enforcement officers to coordinate efforts" regarding national security.[55] Section 905 additionally supports this collaboration, mandating the Attorney General disclose foreign intelligence acquired by the DoJ for criminal investigation with the CIA. While the Act allowed information to flow freely between various government agencies, it lacked the ability to incentivize the agencies to do so. As such, the culture of "need-to-know" continued post 9/11, straining U.S. efforts at counter-terrorism.[56]

Homeland Security Act of 2002 (HSA)

Creating the Department of Homeland Security. Following the enactment of the Patriot Act, several flaws surfaced in its legislation and related Executive Orders; the Homeland Security Act of 2002 (HSA) attempted to address these shortcomings. The HSA created the Department of Homeland Security as a Cabinet Department, uniting 22 agencies under one authority to promote information sharing. This constituted the largest reorganization of national security since the creation of the Defense Department in 1947, and reflected a concerted effort by the White House to encourage the IC agencies to expand inter-agency information sharing.[57] Specifically, Section 892 of HSA mandates that "all appropriate

[53] FISA Amendments Act of 2008, HR 6304, 110th Cong., 1st Sess., (July 10th, 2008).
[54] United States of America Patriot Act of 2001, H.R. 3162, 107th Cong. (2001).
[55] *Ibid.*
[56] Sales, "Share and Share Alike: Intelligence Agencies and Information Sharing," 284.
[57] *Ibid.*

agencies, including the intelligence community, shall, through information sharing systems, share homeland security information with Federal agencies and appropriate state and local personnel."[58]

Also important, Section 202 of the HSA dictated the Secretary of Homeland Security be given access to all information pertaining to threats of terrorism collected, possessed or prepared by the various intelligence agencies.[59] Within this stipulation, a singular authority collects and stores intelligence obtained by various federal agencies and is responsible for disseminating the information to interested parties.[60] Although the Act stipulates that federal agencies must work together in a consistent method to share intelligence information, it failed to include consequences for agencies that did not cooperate in information sharing efforts.[61]

The 9/11 Commission

Investigating the Vulnerabilities in the U.S.' National Security Strategy. To better understand the massive intelligence failures that led to the 9/11 attacks, President G.W. Bush, with support from key policy makers, created the National Commission on Terrorist Attacks Upon the United States, also known as the 9/11 Commission, and charged the Commission to investigate the specific failures allowing the attack to take place undetected. The 9/11 Commission's report, released in 2004, contained several major policy recommendations, including:

1. The Establishment of a National Counterterrorism Center (NCTC) built on the foundation of the existing Terrorist Threat Integration Center (TTIC). This NCTC should be a center for joint operational planning *and* joint intelligence, staffed by personnel from the various agencies.

2. The current position of Director of Central Intelligence (DCI) should be replaced by a National Intelligence Director with two main areas of responsibility: (1) to oversee national intelligence centers on specific subjects of interest across the U.S. Government; and (2) to manage the national intelligence program and oversee the agencies that contribute to it.

3. The CIA Director should emphasize: (a) re-building the CIA's analytic capabilities; (b) transforming the clandestine service by building its human intelligence capabilities; (c) developing a stronger language program, with high standards and sufficient financial incentives; (d) renewing emphasis on recruiting diversity among operations officers so they can blend more easily in foreign cities; (e) ensuring a seamless relationship between human source collection and signals collection at the operational level; and, (f) stressing a better balance between unilateral and liaison operations.

[58] Homeland Security Act of 2002, 6 U.S.C. § 892 (2002).
[59] Sales, "Share and Share Alike: Intelligence Agencies and Information Sharing,"283.
[60] *Ibid.,* 284.
[61] *Ibid.*

4. To combat the secrecy and complexity, the overall amounts of money being appropriated for national intelligence and to its component agencies should no longer be kept secret. Congress should pass a separate appropriations act for intelligence, defending the broad allocation of how these tens of billions of dollars have been assigned among the varieties of intelligence work.

5. Information procedures should provide incentives for sharing to restore a better balance between security and shared knowledge.[62]

A recurring theme among the policy recommendations in the report included the importance of information sharing in order to better "connect the dots." Following the release of the final report by the committee, various legislation, executive orders, and department guidelines have begun to implement policies to strengthen information sharing in the pursuit of national security.

Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)

Encouraging Change in the Intelligence Community. In an ongoing effort to force evolution within the Intelligence Community, the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 reorganized the IC under the Director of National Intelligence (DNI), to serve as the chief intelligence officer to the President and overall manger of the IC.[63] Furthermore, it charged the President with creating an Information Sharing Environment (ISE) and to issue guidelines for "acquiring, accessing, sharing, and using information."[64] The law also established an Information Sharing Council, in order to advise the President and the Program Manager regarding ISE policies, procedures, guidelines, and standards.[65]

Many of the policy reforms offered little guidance in the mission and methods of these newly created positions, and often were contradicted by other sections within the same legislation. For example, Section 1016 of IRTPA stipulated the creation of an "information sharing environment," intended to create a decentralized means of sharing information across the different agencies, and yet Section 202 envisioned that a central clearinghouse would hold all information.[66] Such negations in policy hindered the effectiveness of legislation created to promote intelligence sharing.

Executive Orders 13354, 13355 & 13356 (2004)

Information Sharing Guidelines for the Intelligence Community. In addition to legislative contradictions, policy enacted following the publication of the 9/11 Commission lacked strong mandates in order to ensure intelligence sharing was occurring between the agencies. Executive Order 13354, *Strengthening the Sharing of Terrorist Information to Protect Americans*, and Executive Order 13355, *Strengthened Management of the*

---

[62] *Ibid.,* 434.
[63] Calvert Jones, "Intelligence Reform: The Logic of Information Sharing," *Intelligence and National Security* (2007): 392.
[64] Richard F. Grimmet, *9/11 Commission Recommendations: Implementation Status* (Washington, DC: Congressional Research Services, 2006), 6.
[65] *Ibid.*
[66] *Ibid.*

Intelligence Community, both exemplified this issue. Signed by President Bush on August 27, 2004, both orders were meant to serve as the guidelines for the creation of an effective ISE.

EO 13354 authorized the creation of the National Counterterrorism Center (NCTC), a hub and spoke model for intelligence proliferation.[67] Under EO 13354, a centralized means of intelligence sharing was created, contrasting sharply with the prescriptions laid out in the 9/11 Commission Report which called for a decentralized model. However, EO 13354 was immediately succeeded by EO 13355 and EO 13356, signed later the same day.

EO 13355 served to amend a subsection of Regan's EO 12333, issued in 1981.[68] Bush's order gave the Director of National Intelligence (DNI) the responsibility of developing objectives and guidance for the IC and ensuring that information sharing actually occurred. EO 13356 charged the heads of the intelligence agencies with the responsibility for sharing information among each other.[69] In addition, EO 13356 directed that agencies be incentivized to share information and were individually responsible for removing all barriers that prevented collaboration.[70]

Executive Order 13388 (2005)

Strengthening Incentives to Share Information. Over time President Bush continued to issue Executive Orders attempting to strengthen prior legislation while providing a framework better enforcing information sharing. In 2005, President Bush signed Executive Order 13388, known as *Further Strengthening the Sharing of Terrorist Information to Protect Americans*, which revoked Executive Order 13356 which established the Information Sharing Council (ISC), and was expected to aid in the establishment of an interoperable information sharing environment as mandated by IRTPA.[71] More so, the order declared that agencies must give the highest priority to information sharing amongst the various intelligence agencies, while at the same time protecting the legal rights of American citizens.[72]

[67] Jones, "Intelligence Reform: The Logic of Information Sharing," 393.
[68] Grimmet, *9/11 Commission Recommendations: Implementation Status,* 70.
[69] *Ibid.*
[70] *Ibid.*
[71] Exec. Order No. 13,388, 70 Fed. Reg. 62023 (October 25th, 2005).
[72] *Ibid.*

Where We Are Now – A Decade After 9/11

Intelligence Community Directive Number 501 (2009)

Evaluating Progress 10 Years After 9/11. Following the election of President Obama, the new administration identified one of its core goals to include the protection of civil liberties coupled with the provision of the security of the American people. As the war in Afghanistan continues, however, and troops in Iraq have withdrawn, the importance of intelligence collection remains critical for U.S. national and homeland security.

President Obama has continued efforts to encourage information sharing among intelligence agencies. Intelligence Community Directive Number 501 (ICD 501), issued in 2009, targets the culture that prevented collaboration among intelligence units, stating that the "responsibility to provide" information between the agencies is imperative to national security.[73] The overall objectives of the directive include:

1. Foster an enduring culture of responsible sharing and collaboration within an integrated IC.

2. Provide an improved capacity to warn of and disrupt threats to the United States (U.S.) homeland, and U.S. persons and interests.

3. Provide more accurate, timely, and insightful analysis to inform decision making by the President, senior military commanders, national security advisers, and other Executive Branch officials.[74]

In an effort to reinforce the information sharing environment, the Obama Administration has integrated the Information Sharing Council into the White House policy process through the Information Sharing and Access Interagency Policy Committee (ISA IPC). Created in 2009, the ISA IPC encourages further consolidation of administration efforts to foster information sharing.

Although the Obama Administration has taken concrete steps to promote information sharing while protecting civil rights, the process remains challenged by an ever-changing environment, as technology and capabilities advance faster than legislation can be implemented. Striking the right balance of factors is critical for both the success of effective information sharing and also for the promotion of U.S. national security.

[73] Exec. Order No. 13,388, 70 Fed. Reg. 62023 (October 25th, 2005).
[74] Office of the Director of National Intelligence, *Intelligence Community Directive 206* (Washington, DC, 2006).

[This page is intentionally left blank]

The Culture of Information Sharing

Responsibility to Protect vs. Responsibility to Provide

Obtaining the Perfect Balance. Throughout the last decade, dramatic improvements occurred for national security through the advancement of critical technologies and continued efforts toward governmental reorganization. Much of the legislation passed after 9/11 encouraged the utilization and collaboration of intelligence collection capabilities; nevertheless, bureaucratic resistance to change among the intelligence agencies still persists, hindering the potential progress that could have been achieved over the past decade.

Culture Acts as an Impediment to Better Collaboration

Culture Remains the Most Fundamental Impediment to Expansive Information Sharing. During the Cold War, fear of Russian spies infiltrating the intelligence service created a culture of "need-to-know" and an aversion to information sharing. One principal consequence of this approach is its underlying premise that agencies are able to foresee which other agencies will require specific intelligence.[75] As a result, given this suspicious culture, departments chose to compartmentalize intelligence for fear that their information, sources, and methods would be exposed, a posture that has long outlasted the Cold War. Although counterintelligence concerns are still very much a major concern for the United States, such Cold War attitudes are no longer applicable for modern intelligence operations.

9/11 clearly demonstrated that "stovepiping" created a risk to national security which far outweighed the benefits of overprotecting information.[76] Although greatly transformed from 9/11, the inter-agency culture continues to be antithetical to sharing information; the "need-to-know" principle still pervades the intelligence community's (IC) culture. Though mistrust of the system and of other agencies will never fully disappear, it must be mitigated and managed appropriately to prevent over-classification and the unnecessary compartmentalization of data. Ending the culture of compartmentalization of intelligence is a major challenge, but must be addressed in order to ensure a culture of integration.

"Stovepiping" Inhibits Information Sharing

"Stovepiping" Largely Restricts the Flow of Information and Obstructs a Culture of Integration. By its very nature, "stovepiping" inherently opposes the concept of information sharing. 9/11 forced the IC to recognize the consequences of refusing to share intelligence in order to "connect the dots." Although the various intelligence agencies were all posited with ensuring national security, a complete failure occurred to move beyond the narrow viewpoint of an agency to more broadly analyze security threats. Consequently,

---

[75] Kean et al., *The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States,* 417.

[76] Program Manager, Information Sharing Environment, *ISE Annual Report to the Congress* (Washington, DC, 2011), 24.

the 9/11 Commission report outlined a series of critical deficiencies in intelligence sharing requisite for the promotion of a culture characterized by "need-to-share."[77]

Building Networks to Reinforce a Culture of Information Sharing

Concerted Efforts to Change Inter-Agency Culture. Despite significant obstacles, considerable gains occurred in improving the mechanisms for information sharing. The creation of the Terrorist Threat Integration Center and the National Counterterrorism Center (NCTC) following 9/11 provided intelligence analysts direct access to roughly 30 different networks. Additionally, the NCTC conducts a classified videoconference three times daily, 365 days a year, with over a dozen federal counter-terrorism partners. Success outside the NCTC, however, has not progressed as quickly.

Inter-agency cooperation certainly increased since the promotion of a "need-to-share" culture, but room remains for further progression. Although the Congress and Executive Branch have both laid out fundamental policy structures, a more focused and sustained vision that can align the many differing agency frameworks is required. This alignment is essential to provide a foundation for interagency cooperation, a critical component of information sharing. Historically, sharing discretion has been left to each agency, resulting in multiple strategies and methods that created competition among the IC. In order to combat "turf wars" and create "a culture of trust," an overarching system needs to be implemented to standardize the IC. To realize this objective, training should be standardized across all agencies and departments in the IC.

The Use of Standardized Training Modules

The Importance of Standardization Across the IC. Training staff to appreciate the importance of information sharing at all levels of operation and to effectively share information through existing and emerging mechanisms is essential to ensure progress.[78] Information sharing training not only emphasizes the importance of information sharing, but also encourages teambuilding, collaboration, and best practices by demonstrating the specific skill development needed to execute sharing activities.[79]

Currently, each department undertakes their own training structures that are agency specific. Standardized training modules introduced across the IC at all levels of management will enable consistency and ensure no one agency is able to operate at their own accord. Such training modules will be able to address not only the broad issues that challenge the IC, but will also identify issues that plague specific agencies. For example, the NCTC and the FBI's Terrorist Screening Center (TSC) are currently implementing a standardized training course that will help to facilitate, standardize, and improve watch listing policies across the IC.

This type of training needs to be further expanded to encompass a wider range of agencies and issues. Consequently, broader training will ensure that all agencies are following the

[77] Kean, *The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States,* 417.
[78] Program Manager, Information Sharing Environment, *ISE Annual Report to the Congress,* 26.
[79] *Ibid*.

same protocol and security policies when assessing intelligence data. Consistent and standardized training systems will aid in countering the inherent fear of sharing information. Increasing and improving mission-specific training programs will encourage further collaboration.

According to the ISE 2011 Annual Report, 10 out of 14 responding ISE departments and agencies have implemented mission-specific training which supports information sharing.[80] Nonetheless, this represents a mere 7% increase since 2010. Unfortunately, during tight fiscal times training of personnel is often one of the first programs to be cut, despite the importance of maintaining and expanding its current levels.

The unauthorized disclosures of classified data in *the Wikileaks* episode unfortunately exacerbated an already present lack of justified faith in the security system; however, *Wikileaks* itself has not stopped or hindered information sharing. A reversal of collaboration and a shift in the risk differential could have been a major impediment for continued cooperation.

Self Interest of the Data Stewards

A Ground-Up Federal Vision to Alter IC Culture. Mistrust of a greater information sharing model will never fully disappear. The inherent conflict between increased sharing and security requires proper management that levels out the two extremes. One way in which to help dampen down this natural mistrust of the system and promote cooperation is to implement an approach that focuses on the data stewards.

A new federal vision is required to alter the culture of the IC, but in order to do so a ground-up approach will be needed. The concept of self-interest must be assessed to encourage a change in agency attitude at a grass roots level. If the architectural perspective does not address the needs and mission of the data steward, little change will occur thereafter. Amending policies to expand data sharing will not alter behavior unless the role and mission of the data steward is first examined. When assessing interagency policy changes, two essential issues must be addressed:

1. Does it meet a mission that the data steward presently has?

2. Does it meet an obvious national security need?

If these issues are not addressed then altering the culture and behavior of those at the ground level will be even more problematic.

Positive reinforcement is an important element when addressing a cultural shift. At the agency or departmental level, program funding should be linked with agency performance on information sharing. If a certain agency or department is not meeting expectations in terms of inter-agency cooperation, applying monetary penalties could influence future managerial decisions.

[80] *Ibid*., A-2.

Encouraging the expansion of employee incentive awards for collaborative efforts will further help to drive the momentum. According to the ISE 2011 Annual Report, 86% of responding departments and agencies offer (or intend to offer) an award that involves information sharing directly or indirectly as a criterion.[81]

Incentivizing Information Sharing

Offering an Agency Information-Sharing Award. Although the figures have doubled from 2010, still only 43% of responding ISE departments have nominated an employee for a collaboration award. Only three agencies, the DOJ, DOT, and the FBI, however, report offering agency-specific incentives to encourage information sharing.[82] Current, only the DOT offers cash rewards to acknowledge employees' contribution in information sharing.

One important consequence of monetary incentives, however, is the sharing of information that is largely irrelevant. The sharing of information that is not deemed valuable, just for the sake of sharing, is not productive. A flood of unusable information will hinder the efficiency of the system and will not contribute to the overall goal of making the country more secure. It is important to emphasize that information sharing is a means to an end, and is not the final objective. Over-sharing without purpose is neither a productive nor a useful strategy. Once again, proper management and training are critical instruments that can curtail such a pattern if it is indeed occurring.

Joint Duty-Like Assignments to Foster Information Sharing

Utilizing Relationships Across Agencies to Encourage Change. In addition to incentives and training, policies encouraging joint duty-like assignments will foster greater knowledge sharing and create communities of interest around specific topics.[83] Combining representatives from a range of different agencies will help to avoid the bureaucratic clashes that prevent proper sharing. Fusion Centers at both local and regional levels could be used as models for how this could function.[84] Interagency personal relationships are perhaps the best method in combating the inherent mistrust that is present between agencies.

Data stewards are more inclined to share information when they network with colleagues from other agencies. One of the best methods to accelerate networking is to create roundtable discussions for specific topics where each agency or department is represented. Furthermore, there should be federal leadership that mandates that promotions to senior management must first require a tour of duty at another agency. This supplemental element should be added to already existing directives involved in the performance management system.

[81] *Ibid*., A-2.
[82] *Ibid*., 26.
[83] *Ibid*., xi.
[84] Jackson, *The Challenge of Domestic Intelligence in a Free Society,* 143.

Intelligence Community Directive Number 501 (ICD 501) requires all IC agencies to include sharing and collaboration in their performance management system requirements.[85] In 2011, employees that support ISE-related priorities in the 14 ISE departments indicated that their agency has incorporated information sharing and collaboration as a component of their performance appraisals, constituting 100% of the ISE agencies. This has increased by 14% from 2010.[86] However, broadening this trend to make it a key aspect in performance appraisals for *non*-ISE related responsibilities will help to accelerate further collaboration. For example, currently only 71% of ISE departments and agencies have included information sharing and collaboration as a component in performance appraisals of employees *without* direct ISE responsibilities.[87]

Throughout the last ten years the IC experienced a substantial change in how it conducts information sharing. Nevertheless, the most important changes in culture have not been advancing at the pace of other developments. Although technology is an important element in collaboration, it will not fix the bureaucratic issues that have plagued the IC. These issues should not be underestimated and methods that continue to alter the culture should continue to be implemented.

Rewarding behaviors that foster information sharing and adoption of collaborative cross-agency work teams, will improve performance throughout the Government and advance efforts conducted with non-governmental partners.[88] A culture that is more focused on information sharing for the federal agencies will contribute to a better integration of all stakeholders, including members of the non-intelligence community, most importantly state and local law enforcement.

Integration of Stakeholder Missions and Responsibilities

Information Sharing with State and Local Agencies Increasingly Important

National Security Challenges Have Expanded Beyond the Traditional Threats of the Cold War Era. Diffuse and ambiguous, today's security threats challenge any singular federal agency to effectively address them alone. Effective collaboration amongst multiple agencies and across federal, state, and local governments is critical.[89] The *National Strategy for Information Sharing* decrees, "State, local, and tribal authorities are critical to our Nation's efforts to prevent future terrorist attacks."[90] The attacks of 9/11 and subsequent terrorist plots have illustrated the possibility of terrorists living within local U.S. communities and engaging in criminal or other suspicious activities.[91] Incorporating local and state entities into counter-terrorism is an essential element in combating this diffuse threat.

---

[85] Office of the Director of National Intelligence, *Intelligence Community Directive Number 501: Discovery and Dissemination or Retrieval of Information within the Intelligence Community*.
[86] Program Manager, Information Sharing Environment, *ISE Annual Report to the Congress*, A-1.
[87] *Ibid*.
[88] *Ibid*., 25.
[89] Government Accountability Office, *Key Challenges and Solutions to Strengthen Interagency Collaboration* (Washington, DC, 2010), 1.
[90] Information Sharing Environment, *National Strategy for Information Sharing* (Washington, DC, 2007), 17.
[91] *Ibid*.

Despite the importance of top-to-bottom collaboration, the FBI has recently expressed that "since September 11th, intelligence operations have been transformed, with most efforts focused at the federal level. Less publicized are corresponding enhancements to state and local law enforcement intelligence operations."[92] Renewed leadership in addressing intelligence sharing progress from the Executive Branch will help to promote further collaboration.

Failure of Coordination between the FBI and the New York Police Department

The Importance of Collaboration is Exemplified by the Relationship Between the NYPD and the FBI. New York City has experienced first-hand the threat of international terrorism, and still remains one of the top targets for *al-Qaeda*.[93] Since 9/11, numerous plots against the city have been discovered or were unsuccessful in achieving their desired effect, such as the 2009 plot to bomb New York City's subway system. The ability to detect such threats has required collaboration between local and federal authorities. Despite success in preventing another 9/11, many cases exist in which the FBI and NYPD have failed to adequately share information, raising the potential for another attack.[94]

As the Associated Press has reported, despite the two agencies' attempts to collaborate, their efforts have been undermined by mutual suspicion.[95] More so, inter-agency distrust was exacerbated after the revelation of the NYPD's surveillance of Muslims in New Jersey. The New Jersey FBI office criticized the operation, stating the surveillance jeopardized trust between law enforcement and the public, as well as between government agencies.[96] Cooperation between the NYPD and the FBI is essential for the security of NYC and its surrounding areas, and collaboration between the two entities must become a priority. Tension and mutual distrust has not only permeated throughout the ranks of the NYPD and FBI but has now also expanded to affect other state and local entities.

State and Local Law Enforcement Agencies Lack Protection for Sharing Both Classified and Unclassified Data

Protecting the Agencies that Share. After 9/11, state and local law enforcement agencies were included in a new information sharing system. Despite efforts to collaboration, there remains further advancement in ensuring that state, and local agencies fully exchange information collected. One of the most important factors to be improved upon is the current lack of protection for state and local law enforcement agencies' that share classified data. Although state and local law enforcement officials may require access to classified information in order to properly protect their communities, in many cases they lack permission that would allow access to such information. Inability to access critical threat

[92] Federal Bureau of Investigation, *National Information Sharing Strategy 2011* (Washington, DC, 2010), 5.
[93] "Counterterrorism Units," New York Police Department, last modified March 30, 2012, http://www.nyc.gov/html/nypd/html/administration/counterterrorism_units.shtml.
[94] Adam Goldman and Matt Apuzzo, "Consequences for Security as NYPD-FBI Rift Widens," *Associated Press*, March 20, 2012, http://www.ap.org/Content/AP-In-The-News/2012/Consequences-for-security-as-NYPD-FBI-rift-widens.
[95] *Ibid*.
[96] Samantha Henry, "NJ FBI: NYPD Monitoring Damaged Public Trust," *Associated Press*, March 7, 2012, http://www.ap.org/Content/AP-In-The-News/2012/NJ-FBI-NYPD-monitoring-damaged-public-trust.

information is an unacceptable vulnerability for state and local law enforcement agencies, who are understood to be the first responders in the case of a terrorist threat, or another attack.[97]

In August 2010, the President issued Executive Order 13549 to all federal departments and agencies, outlining the Classified National Security Information Program, designed to safeguard and govern access to classified national security information shared by the Federal Government with state, local, tribal, and private sector entities. The Department of Homeland Security states that the Executive Order, along with the implementation guide published by DHS, will serve as the foundation for consistent information sharing security across the intelligence and defense communities. This will aid in further enhancing the confidence necessary to support the sharing of classified information.[98]

Historically, executive departments and agencies have employed more than 100 different policies for handling information that is not classified, and yet still requires protection. These classifications include "Law Enforcement Information," "For Official Use Only," "Sensitive Security Information," and "Limited Official Use." The agency-specific approach has created inefficiency and confusion, leading to a patchwork system that fails to adequately safeguard the information that requires protection while unnecessarily restricting information sharing by creating impediments.[99] Additionally, local law enforcement agencies may be reluctant to share sensitive federal information with other local law enforcement agencies, due to uncertainties of which security policy to apply.[100]

In November 2010, the President signed Executive Order 13556 *Controlled Unclassified Information*, establishing a program to manage all unclassified information requiring safeguarding or dissemination. The order designates the National Archives and Records Administration (NARA) as the federal agent to implement it.

NARA has been working with federal departments and agencies, as well as state and local agencies and other stakeholders to establish an executive-wide program. This is aimed at standardizing and simplifying the method in which agencies handle unclassified information that still requires safeguarding or dissemination controls.

The President and the Executive Branch of the federal, state, and local governments must strive to ensure that both the new programs for handling classified information and the ongoing program to standardize policies for unclassified information will be fully implemented. This will subsequently result in an efficient and appropriate flow of information between these bodies. Only standardized systems put forth at the federal level will alleviate the concerns of both federal and state agencies.

---

[97] General Accounting Office, Security Clearances: FBI *has Enhanced Its Process for State and Local Law Enforcement Officials* (Washington, DC, 2004), 1.
[98] Department of Homeland Security*, Classified National Security Information Program for State, Local, Tribal and Private Sector Entities Implementing Directive* (Washington, DC, 2012), 2.
[99] National Archives and Research Administration, *2011 Report to the President* (Washington, DC, 2011), 4, http://www.archives.gov/cui/reports/report-2011.pdf.
[100] The Task Force on Controlled Unclassified Information, *Report and Recommendations of the Presidential Task Force on Controlled Unclassified Information* (Washington, DC, 2009), 6.

Cultivating Understanding and Culture of Information Sharing

State and Local Officials that are Unaware of the Importance of the Information They Hold. Maurita Bryant, the first national Vice President of the National Organization of Black Law Enforcement Executives (NOBLE), expressed in her testimony for the Subcommittee on Counterterrorism and Intelligence that "local level information is not always shared because personnel may not think it is worth communicating on a national level."[101] The sheer magnitude of personnel across the country that work for state and local entities presents a unique challenge. Amending a culture that encompasses thousands of different units represents one of the most difficult tasks to manage.

DHS has named a top priority to be to establish a domestic information sharing capability with state and local officials, and should therefore implement a unified and standardized nation-wide information training program. By employing federal-led training programs, state and local agencies are introduced to the standardized policies and procedures that can be implemented across the country, while helping to build a culture of trust between agencies. Priority for the attendance of the training program should be given to senior officials of state and local agencies as opposed to lower-level personnel. The culture of an organization will not change without senior level support and participation. Providing both personnel and agency incentives will assist in the expansion of collaboration. Agencies that have a self-interest in the expansion of information sharing will likely see an increase of collaboration at a faster pace than those that lack the same incentive.

In addition to a training program, the Federal Government should also promote a guideline for information sharing that state and local officials can refer to. An expansion of existing programs such as the *Intelligence Guide for First Responders,* created by the Interagency Threat Assessment and Coordination Group (ITACG), should be implemented on a large-scale basis. Dissemination of such a guideline would provide an enhanced means for frontline officers to learn the importance of information sharing.

Information Sharing with Non-Government Actors

Understanding that Critical Infrastructure is a Prime Target. The attacks on the Madrid subway and London busses illustrates the fact that terrorists plot against critical infrastructure in order to frighten the public. Such knowledge makes it essential that the infrastructure sectors are able to share and receive pertinent information held by the Government and other infrastructure agencies.

Under the 1998 Presidential Directive 63, the Federal Government asked each critical infrastructure sector to establish a sector-specific information sharing organization that was capable of disseminating information about threats and vulnerabilities to the

[101] *Hearing on Federal Government Intelligence Sharing with State, Local and Tribal Law Enforcement: An Assessment Ten Years After 9/11*, Before the House Comm. on Homeland Security Subcomm. on Counterterrorism and Intelligence 112th Cong. (2012) (statement of Maurita J. Bryant, National Organization of Black Law Enforcement Executives), http://homeland.house.gov/hearing/subcommittee-hearing-federal-government-intelligence-sharing-state-local-and-tribal-law.

particular organization.[102] In response, sectors such as energy, financial services, information technology, and transportation have established "Information Sharing and Analysis Centers" (ISAC). As of April 2012, there are 16 ISAC Council members from a diverse mix of departments.[103] Additionally, the FBI's InfraGard and other partnerships run by DHS, help to facilitate the flow of information among critical infrastructures. [104] Terrorist-related information should also be provided by private businesses, as terrorists may try to acquire sensitive materials or carry out training within the private sector.

Information Sharing with Private Entities

The NYPD's "Operation Nexus" to Collect Relevant Information From Businesses and Enterprises. In March of 2011, the Analyst-Private Sector Program was launched as a joint ODNI and DHS I&A venture in which pilot project brought together experts from the private sector and experienced IC analysts in order to develop collaborative partnerships.[105]

To facilitate the flow of information between the private sector and the Government, federal, state, and local agencies need to fully utilize information-sharing structures and help to build trust among the many different partners. This will allow efficient and timely distribution of information to the appropriate people.

Information Sharing with the Public

Criticality of Public Sector Intelligence. In addition to information that is shared amongst the private and government community, intelligence gleaned from the public has proven to be a critical part of counter-terrorism efforts. For example, the attempted car bombing of Times Square in May 2010 was discovered by street vendors who then alerted an NYPD officer.[106] Collaboration with the public sector has been endorsed by various members of the Government, such as DHS Secretary Janet Napolitano who has stated that "we're safer when local law enforcement works together with the communities and citizens they serve."[107] In order to engage the public in preventing terrorism, the "If You See Something, Say Something" campaign has being launched in conjunction with the Nationwide Suspicious Activity Reporting Initiative (NSI).

The collection of intelligence requires assistance from local law enforcement, who provide a critical bridge in intelligence gaps between local, state and federal agencies. As such, local officers must be aware of the importance of their responsibilities. DHS is working to develop a "community-oriented policing curriculum" for state and local law enforcement agencies, focusing on better enabling frontline personnel to distinguish between illegal

[102] Directive 63 was later uploaded by 2003's Homeland Security Presidential Directive 7.
[103] "National Council of ISACS," ISACCouncil.org, last modified March 30, 2012, http://www.isaccouncil.org /index.php?option=com_content&view=article&id=83&Itemid=195.
[104] "Critical Infrastructure Sector Partnerships," Department of Homeland Security, last modified September 12, 2011, http://www.dhs.gov/files/partnerships/editorial_0206.shtm.
[105] Program Manager, Information Sharing Environment, *ISE Annual Report to the Congress*, 60.
[106] "Car bomb found in New York's Times Square," *BBC News*, May 2, 2010, http://news.bbc.co.uk/2 /hi/8656651.stm.
[107] "Hometown Security," Department of Homeland Security, last modified March 30, 2012, http://www.dhs.gov/files/programs/hometown.shtm.

criminal activities and potential national security threats.[108] A federal vision is required to train and institute guidelines for local authorities so that they can establish relationships with their local communities in order to effectively collect information.

Different local and state agencies throughout the nation practice distinctive and unique procedures to build local collaboration. The Federal Government should implement a series of recommendations that illustrate the models that have the highest degree of success across the country, which would help to foster inter-state collaboration while developing local intelligence collection practices.

Local communities may be hesitant to enter into relationships with law enforcement agencies if they perceive that they are viewed as incubators of violent extremism. In order to build trust between communities, local officers should hold regular roundtable discussions with community leaders, including those from community organizations, faith-based and education entities, and the media. Additionally, in order to build relationships and promote collaboration, local law enforcement should share threat-related intelligence that may affect surrounding areas to local leaders. This will contribute to the goal of public awareness that counter-terrorism efforts are not solely restricted to law enforcement, but rather it is an endeavor that requires public collaboration.

[108] Department of Homeland Security, *Next Steps: Supporting Community-Based Efforts to Reduce Violent Crime* (Washington, DC, 2010), http://www.dhs.gov/xlibrary/assets/fact_sheet_reduce_violent_crime_080310.pdf.

Balancing the Responsibilities for Protection and Privacy

> "The choice between security and liberty is a false choice, as nothing is more likely to endanger America's liberties than the success of a terrorist attack at home. Our history has shown us that insecurity threatens liberty. Yet, if our liberties are curtailed, we lose the values that we are struggling to defend."[109]
>
> *The 9/11 Commission Report,* Final Report of the National Commission on Terrorist Attacks Upon the United States, July 2004

There is a perception that efforts to increase national security must necessarily erode privacy rights. The legal authorities that govern the actions of the ISE and its partner agencies, however, are structured to be compatible with the constitutional protections of privacy, civil liberties, and civil rights. Although a complicated exercise, one of the principles that governs information sharing is the maintenance of these authorities to ensure that partners only obtain information that they are legally permitted to access.

A dynamic architecture, proper training to clarify rules and ambiguities, and oversight are critical elements of an information sharing environment that safeguards core American values and builds public trust. This section explores current counter-terrorism information sharing efforts through a privacy lens.

Information and Privacy Issues in Information Sharing

Types of Information of Importance to Counter-Terrorism

The Federal Government and its various organizations and agencies deal with a significant amount of information in the course of executing counter-terrorism operations and analyses. To help keep track of this information, and to identify what can and cannot be done with it, several broad classes of information have been created that categorize data based on its content or source. Each major information class has its own distinct rules and guidelines for collection, storage, dissemination, and general use, which are derived from a combination of Congressional legislation, Executive Orders, and agency leadership guidelines. Many of these information categories have overlapping definitions; therefore information is often given several different descriptive tags. The major information categories relevant to the Information Sharing Environment and the Federal Government's counter-terrorism work are outlined below.

Protected Information. Protected information is defined by the ISE's sharing guidelines as "information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and Federal laws of

[109] Kean et al., *The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States,* 395.

the United States."[110] This is the most broadly defined category of information, and as such the overwhelming majority of the information held within and transmitted through the ISE falls under this general category.

Terrorism Information. As defined by the Intelligence Reform and Terrorism Prevention Act of 2004, terrorism information refers to all information relating to:

> "(A) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism, (B) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations, (C) communications of or by such groups or individuals, or (D) groups or individuals reasonably believed to be assisting or associated with such groups or individuals." [111]
>
> *The Intelligence Reform and Terrorism Prevention Act of 2004*, December 2004

Terrorism information has its own set of rules surrounding how it can be utilized, stored, and analyzed, particularly if the information relates to a U.S. person. In many cases, data tagged as protected information cannot be utilized in any fashion except to determine if it constitutes or is related to terrorism information.

Homeland Security Information. There is substantial overlap between terrorism information and homeland security information, defined by the Homeland Security Act of 2002 as "any information possessed by a federal, state or local agency that relates to terrorist activities, suspected terrorists, or terrorist organizations, or information that will improve the response to terrorist acts."[112] Homeland security information is a primary category for the Information Sharing Environment, as mandated by the Homeland Security Act.

[110] Information Sharing Environment, *Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment* (Washington, DC, 2006), 1.
[111] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (2004).
[112] General Accountability Office, *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information* (Washington, DC, 2006), 2, www.gao.gov/new.items/d06385.pdf. Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2255 (2002).

Law Enforcement Information. The Information Sharing Environment's guidelines define law enforcement information as :

> "any information obtained by or of interest to a law enforcement agency or official that is (A) related to terrorism or the security of our homeland and (B) relevant to a law enforcement mission, including but not limited to information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counter-intelligence, or counter-terrorism investigation; assessment of or response to criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of, or response to, criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and victim/witness assistance." [113]
>
> *Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment,* December 2006

Law enforcement information differs from terrorism or homeland security information in that it relates primarily to purely criminal activity. It is predominantly the domain of law enforcement agencies, as opposed to the Intelligence Community.

Foreign Intelligence Information. As defined by the Foreign Intelligence Surveillance Act of 1978, foreign intelligence information refers to all "information that relates to, and if concerning a U.S. person is necessary to, the ability of the U.S. to protect against attack, sabotage, international terrorism, or espionage committed by a foreign power or an agent of a foreign power."[114] Foreign intelligence information is a primary qualifying factor for warrants issued for surveillance and physical or electronic searches involving the FISA Court, and separates intelligence-based surveillance operations from Title III criminal surveillance.

[113] Information Sharing Environment, *Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment*, 8.
[114] David S. Kris, "The Rise and Fall of the FISA Wall," *Stanford Law and Policy Review* 17 (2006): 495.

U.S. Person Information. The term "U.S. person" has varied definitions throughout the legislation, orders and guidelines that address terrorism and security. The National Counterterrorism Center (NCTC) defines a U.S. person as:

> "a United States citizen, an alien known by the intelligence element concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments." [115]
>
> *Guidelines for Access, Retention, Use and Dissemination by the National Counterterrorism Center and Other Agencies of Information in Datasets Containing Non-Terrorism Information*, March 2012

U.S. person information therefore refers to any information gathered from an individual or entity that is classed as a U.S. person. Collecting and analyzing U.S. person information carries a multitude of restrictions for the Intelligence Community and law enforcement agencies imposed by the Privacy Act, Freedom of Information Act, E-Government Act, Executive Order 12333 and the Fourth Amendment, among others, and remains a prescient issue in the ISE's development and operation.

Personally Identifiable Information (PII). The National Institute of Standards and Technology (NIST) defines PII as

> "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." [116]
>
> *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, Recommendations of the National Institute of Standards and Technology, April 2010

Personally identifiable information refers directly and exclusively to the type of data held by an agency or organization, and its qualification is independent from the source of the data. A large percentage of information present in the ISE is necessarily composed of PII, and its handling is one of the key privacy issues facing the ISE and its partner agencies.

[115] The National Counterterrorism Center, *Guidelines for Access, Retention, Use and Dissemination by the National Counterterrorism Center and Other Agencies of Information in Datasets Containing Non-Terrorism Information* (Washington, DC, 2012), Appendix 2, 1.

[116] Department of Commerce, National Institute of Standards and Technology, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII): Recommendations of the National Institute of Standards and Technology* (Washington, DC, 2010), 1, 2.

Unclassified Data. A wide range of information utilized by the Federal Government falls into the category of unclassified data, and a number of terms are used to categorize some of this information. Unclassified data requires some type of control, but cannot officially be classified under the statutory terms of official U.S. Government classified information.

Prior to 2008, the term "Sensitive But Unclassified" was used for this type of information and was defined as "the various designators used within the Federal Government for documents and information that are sufficiently sensitive to warrant some level of protection, but that do not meet the standards for national security classification."[117] A process is currently underway to change the labeling of this information to "Controlled Unclassified Information" and unify the Federal Government's rules and procedures for designating and handling this type of unclassified data.

U.S. Government Classified Information. Classified information is derived from a range of sources related to U.S. national security. Classified information carries a danger to national security if released to the public and, in many cases, involves sensitive intelligence sources or methods. It is currently governed by Executive Order 13526, signed by President Obama in December of 2009, but has been controlled by a series of laws and prior Executive Orders from several Presidents since World War II.[118] Classified information is categorized as Confidential, Secret or Top Secret, depending on its level of sensitivity and potential harm to U.S. national security interests.

In addition to these three levels of classification, the Intelligence Community and other government agencies have established various special access "compartments" for highly sensitive information that are far more restrictive. Access to compartmented data requires a more intensive personal background investigation and, in some cases, a polygraph examination. Information that requires these higher-level access restrictions is identified as Sensitive Compartmented Information (SCI) or Special Access Required (SAR).[119] Access to SCI or SAR information outside of the Federal Government was almost non-existent prior to September 11, 2001. The release of "sanitized" versions of this data is rare and handled on a case-by-case basis.

Access to Classified Information was Greatly Expanded Following 9/11. Prior to 9/11, access to classified information was largely limited to U.S. Government employees and cleared government contractors. Recognition of the "need-to-share" such information on a broader scale, including with state and local law enforcement agencies, led to new initiatives that granted an increasing number of non-federal employees and other contractors access to federal clearance programs.

The expansion of clearance-based access outside of the Federal Government has required that an increasing number of security clearances for personnel at the state and local level and has mandated the creation of infrastructure approved for the handling and

[117] President Barack Obama to Heads of Executive Departments and Agencies, Classified Information and Controlled Unclassified Information, 27 May 2009, Office of the Press Secretary, The White House, §2(a).
[118] Exec. Order No. 13,526, 3 C.F.R. 298 (2009).
[119] Since 9/11 there has been a large increase in the number of DoD Special Access Programs (SAPs) and information that is Special Access Required (SAR).

transmission of classified data across multiple levels. This rapid expansion of personnel cleared for access to classified information since 2001 has been a central cause for concern within the ISE and its partner agencies.

The Majority of State and Local Personnel Clearances are at the Secret Level. Moreover, in the post 9/11 environment, there is also a need for threat information to be disseminated to private sector partners who do not hold clearances. As a result, there has been a need for information to be sanitized for individuals with lower level clearances and those without clearances. The efficacy of efforts to sanitize intelligence for broad consumption also presents a number of privacy concerns.

Privacy Concerns of U.S. Persons

Sharing Information Between Governmental Entities Raises Many Concerns About the Protection of Privacy. Information sharing between federal, state, local and tribal entities is an absolute necessity in order to adequately protect and defend the nation from a variety of threats. The Information Sharing Environment was created specifically to address the threat of terrorism, which is "uniquely threatening and in combating terrorists more vigorous non-law enforcement approaches are considered more legitimate."[120] Expanded legitimacy, however, requires expanded precaution. In an environment where the sharing of information is actively encouraged for counter-terrorism purposes, additional care must be taken to ensure that individual privacy is both respected and protected.

Data entered into the Information Sharing Environment is assumed to be collected legally, thus the primary concern over privacy centers on how that information is stored and used once it is incorporated into government databases. Such data must be adequately protected against unauthorized or inadvertent disclosure, unauthorized access and secondary use violations, as well as vigorously verified for accuracy, completeness and integrity. Storage and transmission must also comply with established federal standards when classified data is involved.

Accidental Disclosure Can Cause Serious Harm. Data held by the ISE is necessarily of a sensitive and personal nature. Financial records, business records, personally identifiable information, telephone records, and numerous other categories of data can be particularly damaging to an individual if they are made public. Further, the mere knowledge that some types of data exist, such as criminal records, can be embarrassing and have otherwise negative consequences for an individual.

Inadequate disclosure controls also impact the dissemination of information to other government agencies. Information often has certain contextual elements around it, such as its source, reliability and relevance, that are known to the originating agency but are not evident to analysts of other agencies. This context can be essential to its full understanding. Disclosure to another segment of the ISE in improper fashion can remove the context around the data, often to the detriment of the ISE's mission and effectiveness.

[120] Richard A. Best, *Sharing Law Enforcement and Intelligence Information: The Congressional Role,* (Washington, DC: Congressional Research Service, 2007), 14.

The nature of counter-terrorism operations means that arrests or formal investigations based on faulty or misunderstood information can have extremely negative consequences for the individual or entity involved.[121] The IC and law enforcement agencies cannot afford to make such mistakes, therefore it is essential that all data integrated into the ISE be protected against all types of accidental disclosure, be it to the public or to one of the ISE's partner agencies.

Information Must be Protected Against Unauthorized Access. Title III of the E-Government Act of 2002 requires that the Federal Government create and operate adequate systems of information security to their databases and information systems.[122] These security systems range from restrictions on physical access to protections against digital intrusions to user authorization controls. Proper information security is especially important in centralized sharing systems such as the National Counterterrorism Center, because these systems maintain such a large volume of sensitive data on such a large number of people and entities.

Any security breach, either from an external entity or an internal threat, can result in a massive disclosure of sensitive and personally identifiable information to the public or to unauthorized parties. To protect against secondary use violations and to ensure privacy, authorized users should only be able to access the information that is relevant to either their agency's mission or to their individual investigation. Information that is included in the system but otherwise has no relevance should not be accessible.

The Accuracy of Data is Essential to Protect Both Privacy and the Integrity of Investigations. Counter-terrorism investigations are among the nation's highest priorities. Terrorism information often develops rapidly and requires quick, decisive action. Accurate, reliable data is absolutely required for this action to be effective, but also has implications for privacy. Action taken by federal, state, local or tribal entities based on faulty information shared through the ISE can have serious negative repercussions, both for any individual targeted by the operation and for the national security of the U.S.

[121] Center for Democracy and Technology, *CDT Analysis of Privacy Guidelines for the Information Sharing Environment for Terrorism Information,* (Washington, DC, 2007), 2.
[122] "FISMA: Background," National Institute of Standards and Technology, last modified August 17, 2010, http://csrc.nist.gov/groups/SMA/fisma/overview.html.

The Fair Information Practices Provide a Model for Protecting Privacy. The Fair Information Practices (FIP) are the foundation for the Privacy Act of 1974 and outline a thorough set of characteristics necessary for a system that both protects individual privacy and allows access to large amounts of data.[123] Many of the ISE's privacy policies include references to the FIP and use them as a baseline for developing effective privacy protections. The key elements of the FIP, along with their statutory requirements in the Privacy Act, are as follows:

1. *Notice*: Data collection efforts should be announced publicly, along with information that details the types of information being collected.[124]

2. *Purpose specification*: The specific purpose for any data collection should be included in the public notice.[125]

3. *Collection limitation*: Only the relevant and necessary information should be collected.[126]

4. *Retention limitation*: The Government should only maintain information for as long as it is needed.

5. *Use and disclosure limitation*: Information collected for a specific purpose should only be utilized for that purpose.[127]

6. *Data quality*: Data should be verified and checked for accuracy.[128]

7. *Data security*: Data should be maintained securely and protected from unauthorized access.[129]

8. *Individual participation*: Individuals should be able to petition the Government for access to their records.[130]

9. *Redress*: Individuals should be able to challenge data on the grounds of accuracy.[131]

10. *Accountability*: Information systems should have enforceable protections and audit procedures.[132]

---

[123] Center for Democracy and Technology, *CDT Analysis of Privacy Guidelines for the Information Sharing Environment for Terrorism Information,* 2,3.
[124] Privacy Act of 1974, 5 U.S.C. §552a(e)(2-4) (2006).
[125] *Ibid.,* §552a (e)(3).
[126] *Ibid.,* §552a (e)(2) and (7).
[127] *Ibid.,* §552a (b).
[128] *Ibid.,* §552a (e)(5).
[129] *Ibid.,* §552a (e)(10).
[130] *Ibid.,* §552a (c), (d) and (f).
[131] *Ibid.,* §552a (d) and (e).
[132] *Ibid.,* §552a (e)(9) and (10), (g) and (i).

These principles are included in various forms in most agency privacy policies and are codified in the Privacy Act, however issues remain with their effective implementation and use.

Privacy Guidelines for the Information Sharing Environment

The current Information Sharing Environment privacy guidelines are based on Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004, which requires the ISE to issue guidelines to ensure that privacy and civil liberties are protected within the ISE's systems.[133] These guidelines apply specifically to U.S. persons and are directed at all of the ISE's partner agencies.

Exemptions in the Privacy Act and Other Legislation Lessen the Protection of Privacy. The Privacy Act, Freedom of Information Act, E-Government Act, and others contain multiple exemptions for information held and shared by the Government that is related to law enforcement or intelligence matters. The ISE's agencies claim many of these exemptions, which allow them to opt out of the public notice requirements of existing privacy laws. This lessens public knowledge and oversight of the information held by the ISE's systems and has a negative impact on privacy protections. As detailed in the Fair Information Practices, public notice is integral to any data storage and sharing system if privacy is to be sufficiently protected. To truly enshrine privacy in the ISE, the guidelines should insist on the acceptance of all privacy laws without exemptions.[134]

Commercial Databases Need to be Addressed in the ISE's Sharing Guidelines. There are currently no rules or regulations regulating government use of commercial databases because they are not specifically addressed in the Privacy Act. These databases often contain large amounts of personally identifiable U.S. person information and are being increasingly used for counter-terrorism purposes.[135] Data mining operations, in particular, find great utility in the types of data held in many commercial databases. Their importance and relevance is clear, therefore privacy guidelines should be rewritten in the absence of Congressional legislation to include rules for using these databases.

Access to Data Through the ISE Should be Linked to Agency Missions, Not the ISE's Mission. The ISE guidelines state that any access to information shared through the ISE should be "consistent with the authorized purpose of the ISE."[136] The broad nature of these guidelines poses a number of problems. The ISE's counter-terrorism mandate can be applied to a broad list of missions to justify access to otherwise private, secure information.

The ISE's guidelines should insist that access to information through the ISE be reconciled with the mission or purpose of the requesting agency.[137] Access controls based on this

[133] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3666 (2004).
[134] Center for Democracy and Technology, *CDT Analysis of Privacy Guidelines for the Information Sharing Environment for Terrorism Information,* 5.
[135] *Ibid.,* 6.
[136] Information Sharing Environment, *Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment*, 2, 3.
[137] Center for Democracy and Technology, *CDT Analysis of Privacy Guidelines for the Information Sharing Environment for Terrorism Information,* 10.

standard would reduce the amount of unnecessary and irrelevant information analysts have access to through the ISE, which enhances the protection of privacy within the system while also reducing the level of excess noise that analysts must filter out.

Division of Responsibilities for Protecting Privacy

The ISE Should Hold Greater Responsibility for Protecting Privacy. The guidelines, however, place the burden of protection and verification on each individual agency. Each partner agency of the ISE is required to comply with all laws and the Constitution, and to identify and monitor the status of all laws and policies relevant to privacy and civil liberties.[138] The guidelines require every agency to identify any privacy risks in their own systems, seemingly without external assistance. The onus of responsibility for shared information is placed on the originating agency, not on the ISE as a whole or on the agencies utilizing the shared data. There are no ISE-wide standards for these responsibilities.

In the event that inaccurate data is detected by a sharing agency, that agency is required to notify the originating agency of the inaccuracy and request that it be corrected. If this is not done, the shared data must be deleted. There is no provision for the sharing agency to correct the data in its possession, even if it has the capability to do so.[139] By placing the responsibility for security, privacy, protection and accuracy on the individual agencies without top-down enforcement, the ISE's protection of them is only as strong as its weakest agency's privacy policy.

Conflicting Privacy Policies Among Agencies

Overlapping and Contradictory Privacy Policies Inhibit Effective Sharing. There are currently over 100 different privacy policies and sets of guidelines that apply to the Information Sharing Environment.[140] Each agency has its own rules and regulations concerning the use, dissemination and storage of its data. Because the ISE's guidelines require each agency to review and monitor all privacy laws and policies on an individual level, the multitude of privacy policies creates undue complications for sharing relevant information. Information shared through the ISE should instead be held to a unified set of privacy guidelines. This would eliminate confusion over how information should be handled and streamline the information sharing process.

NCTC Sharing Agreements

The National Counterterrorism Center Maintains Guidelines for the Acquisition and Dissemination of Information on U.S. persons. Acquisition of U.S. person information by the NCTC is governed by Executive Order 12333, the Privacy Act of 1974, and the various other federal laws and regulations that affect privacy. Such acquisitions by the NCTC are generally allowable so long as the NCTC has a reasonable belief that the information is, contains, or is essential to the understanding of terrorism information.

---

[138] Information Sharing Environment, *Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment*, 1.
[139] *Ibid.,* 3, 4.
[140] Center for Democracy and Technology, *CDT Analysis of Privacy Guidelines for the Information Sharing Environment for Terrorism Information,* 4.

For the NCTC, reasonable belief is

> "based on the knowledge and experience of counter-terrorism analysts as well as the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion that the information is terrorism information."[141]
>
> *Guidelines for Access, Retention, Use and Dissemination by the National Counterterrorism Center and Other Agencies of Information in Datasets Containing Non-Terrorism Information*, March 2012

The NCTC's Three Track System Governs Information Sharing Practices. Terrorism information in the NCTC's possession may be used for "analysis and integration purposes," included "in finished analytic products and pieces," used to enhance "records created within the Terrorist Identities Datamart Environment (TIDE), operational support, [and] strategic operation planning."[142] The information may also be disseminated to Intelligence Community elements and other federal, state and local counter-terrorism partners.[143] The NCTC's guidelines determine which of these uses are applicable and allowable through the establishment of three separate categories of information. These categories are based on NCTC's acquisition method, and each information track is given its own rules for use and sharing through the ISE.

Information acquired by NCTC personnel through account-based access to data held by another agency is categorized as track one information.[144] This level of sharing is the most limited, and requires a manual search by NCTC personnel on another agency's system. The NCTC's analyst is only able to access levels and categories of data as authorized by the partner agency. All other information is not viewable or accessible by the NCTC.

The second level of NCTC-acquired data is track two information. In a track two acquisition, the NCTC submits search queries to a partner agency, which the agency then reviews and runs through its systems. The data returned by the queries is transferred the NCTC.[145] Track two sharing is more extensive than track one, but still provides the NCTC with only the information returned via the search query. The NCTC does take official possession of the data. Information not returned from the search strings, however, remains exclusively in the control of the responsible agency. It is not shown to or shared with representatives of the NCTC.

The wholesale acquisition of another agency's database or databases by the NCTC is classed

[141]The National Counterterrorism Center, *Guidelines for Access, Retention, Use and Dissemination by the National Counterterrorism Center and Other Agencies of Information in Datasets Containing Non-Terrorism Information,* 4.
[142] *Ibid.,* 7.
[143] *Ibid.*
[144] *Ibid.*
[145] *Ibid.*

as track three information.[146] Here, the responsible agency provides the NCTC with a duplicate version of its original database, allowing the NCTC access to all records and information contained within it, regardless of relevance.

This represents the most extensive level of information sharing, and as such it is allowable under the NCTC's sharing guidelines only when the dataset is believed to contain "significant terrorism information" and track one and two acquisitions are deemed insufficient to satisfy mission need.[147] Despite these qualifications, the NCTC places the highest priority on track three acquisitions.[148]

All three tracks of information are restricted by requirements in the NCTC's sharing guidelines that any data acquired by the NCTC be reviewed and verified to contain terrorism information. Any and all information that is confirmed to not contain terrorism information must be purged from the NCTC's systems.[149] Until that review and classification is made, the data may only be analyzed for the purposes of determining its relevance to terrorism. The exception to use of non-terrorism information is pattern analysis, also known as data mining. Information acquired through any track may be used for pattern analysis according to federal guidelines, although this applies primarily to track three data due to its significantly larger size and scope.[150]

NCTC Data Retention is Time-Limited. The NCTC's guidelines provide up to five years for information held by the NCTC to be reviewed and classified as terrorism information.[151] During this time, the data may be utilized for pattern analysis but cannot be used for other purposes until its content is verified to contain or be related to terrorism information.[152] This timeframe was recently expanded from eighteen months. The increased timeline has privacy implications of its own, however exemptions in the Privacy Act and Freedom of Information Act allow the NCTC to withhold public notice of its data acquisitions, making it impossible for individuals to review or challenge the validity of their records. The extension of retention time from eighteen months to five years is therefore of secondary concern to providing notice that the records exist.

Data Accuracy is the Responsibility of the Originating Agency. The NCTC's guidelines assume that all information it is able to access through the ISE has been legally acquired.[153] This, like the ISE's sharing guidelines, puts the burden on the originating agency to verify that its data is legitimate and exempts the NCTC from this responsibility. The presence of

---

[146] *Ibid.*
[147] *Ibid.*, 9.
[148] Charlie Savage, "U.S. Relaxes Limits on use of Data in Terror Analysis," *New York Times*, March 22, 2012, http://www.nytimes.com/2012/03/23/us/politics/us-moves-to-relax-some-restrictions-for-counterterrorism-analysis.html?_r=1&pagewanted=all.
[149] *Ibid.*
[150] The National Counterterrorism Center, *Guidelines for Access, Retention, Use and Dissemination by the National Counterterrorism Center and Other Agencies of Information in Datasets Containing Non-Terrorism Information,* 10.
[151] *Ibid.*, 9.
[152] *Ibid*.
[153] Center for Democracy and Technology, *CDT Analysis of Privacy Guidelines for the Information Sharing Environment for Terrorism Information,* 2.

inaccurate records in NCTC-acquired datasets is a clear concern, especially in track three transfers that cannot, purely because of their size, be individually reviewed by the originating agency before they are sent to the NCTC.

The guidelines also govern the sharing of NCTC-owned information through the ISE, and again the central restriction is the terrorism information classifier. U.S. person information may be disseminated to other elements of the IC under several conditions, which also apply to data dissemination to state, local and tribal agencies:

1. The information is publicly available.

2. The other agency plans to make a determination about whether the information is terrorism information.

3. It "reasonably appears to constitute terrorism information, or reasonably appears to be necessary to understand or assess terrorism information."

4. The receiving element is "reasonably believed to have a need to receive such information for the performance of a lawful function."[154]

Bulk dissemination of NCTC data to other agencies requires the written approval of the NCTC's director and is only allowable in direct support of a counter-terrorism mission. The IC element receiving the information is also restricted from further disseminating it to other elements of the IC.[155]

Dissemination of U.S. Person Information Raises Secondary Use Concerns. The NCTC is legally allowed to disseminate U.S. person information that is not deemed to be terrorism information or related to counter-intelligence operations under the following conditions:

1. The receiving agency must have proper restrictions on access in place and privacy policies that have been approved by the Attorney General.

2. The Director of National Intelligence must certify that the dissemination is necessary and that mission need cannot be satisfied through alternate, more narrow forms of information sharing.

3. The Attorney General must approve the final sharing agreement between the NCTC and its partner agency.[156]

Transferring U.S. person information that has officially been determined to not relate to terrorism information or counter-intelligence operations raises clear secondary use concerns. Information acquired by the National Counterterrorism Center should not be disseminated to other law enforcement agencies for use in criminal investigation or

[154] The National Counterterrorism Center, *Guidelines for Access, Retention, Use and Dissemination by the National Counterterrorism Center and Other Agencies of Information in Datasets Containing Non-Terrorism Information,* 12, 13.
[155] *Ibid.*, 14.
[156] *Ibid.*, 15.

prosecution except in clear cases of imminent threat. The NCTC's sharing guidelines rely only on the individual judgment of the Attorney General and Director of National Intelligence instead of placing specific, objective requirements on such sharing.

The set of guidelines that the NCTC uses to govern its information sharing practices acknowledges the importance of privacy and civil liberties protections and implements several regulations to ensure that they are retained. A key issue, however, lies on the nineteenth page of the document. This page states that the guidelines

> "are set forth solely for the purpose of internal NCTC and ODNI guidance. They are not intended to, and do not, create any rights, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies, or entities, its officers, employees, agents, or any other person, nor do they place any limitation on otherwise lawful investigative or litigation prerogatives of the United States."[157]
>
> *Guidelines for Access, Retention, Use and Dissemination by the National Counterterrorism Center and Other Agencies of Information in Datasets Containing Non-Terrorism Information*, March 2012

This section identifies the central problem behind many of the guidelines governing information sharing in the ISE: these rules are simply guidelines and are not legally enforceable. The NCTC relies on the Privacy Act, Freedom of Information Act, and other legislation governing privacy for legal enforceability, but is able to avoid many legislative requirements by claiming the law enforcement and national security exemptions written into these pieces of legislation. These guidelines therefore do not provide concrete advancement in privacy protection beyond those already codified into law.

Secondary Use of Information Collected for Counter-Terrorism Purposes

The ability to make determinations regarding the sharing of information based on the Privacy Act's concept of "routine use" requires that the roles and missions of individual agencies be clearly outlined. It is impossible to determine "who gets what" without first deciding "who does what."[158] The clarification and limitation of authorities, however, is a sensitive issue of bureaucratic turf. Consequently, it has not been addressed. Attempts to bypass this issue have resulted in such definitions being left to individual teams and analysts. This is a cumbersome solution that amplifies ambiguity and perpetuates inter-agency rivalries.

A product of this ambiguity around roles and missions is the increasing potential for the secondary use of terrorism information. This concept is not clearly defined in any piece of legislation or guideline, but is more generally used to describe the use of information for

[157] *Ibid.,* 19.
[158] Russell Travers, "Information Sharing, Dot Connecting and Intelligence Failures: Revisiting Conventional Wisdom," (paper submitted to the Director of National Intelligence 2009 Galileo Awards Program, Washington, DC, August 2009), 9, http://www.nctc.gov/press_room/resources/2009_Galileo _Award.pdf.

any purposes other than the justification cited for its original collection.[159]

The Federal Government Must Restrict Its Expanded Powers in Counter-Terrorism Only to Its Counter-Terrorism Mission. The Information Sharing Environment comes with an inherent need to possess and analyze incredibly expansive amounts and types of information. Data mining operations, in particular, require immense databases containing myriad entries and categories of information to be effective. The use of this information must be carefully monitored.

The Privacy Act introduces the concept of "routine use" into federal law with section 552(a)(7), which defines the term as "the use of such a record for a purpose which is compatible with the purpose for which it was collected."[160] Although this was not created with terrorism investigations in mind, the expanded powers of the Federal Government in terrorism and foreign intelligence matters means that information will be acquired by means other than those that are approved by federal law when measured against the Fourth Amendment. The Government is able to access and compile databases of private information outside of the standard processes established for criminal and civil cases when dealing with terrorism. This affords counter-terrorism officials access to information that other law enforcement agencies or officials might not have, or even be legally able to have.[161]

Information that is collected under the FISA or as part of a data mining cannot be utilized in a criminal investigation without violating the rights of the targeted individual because it lacks the probable cause necessary for a criminal investigation. In order to protect individual privacy, careful attention must be paid to how this information is used. It would be improper for the Government to utilize information acquired through a counter-terrorism investigation in the investigation or prosecution of an individual or entity for criminal violations that do not involve terrorism. Information utilized in criminal or other investigations must only be collected through the officially sanctioned processes for those investigations.

The NCTC Guidelines Need Stronger Secondary Use Protections. The National Counterterrorism Center's information sharing guidelines establish a direct relation to terrorism as the primary requirement for disseminating information to other members of the IC or law enforcement agencies. This can either be in support of an ongoing investigation, if the information has already been classified as terrorism information, or to determine if the information held actually qualifies as terrorism information.[162]

Dissemination of U.S. person information in direct support of terrorism of foreign intelligence investigations is permissible at all times. The NCTC's guidelines do provide a

---

[159] New York Police Department, *Public Security Privacy Guidelines* (New York, NY, 2009), 4, www.nyc.gov/html/nypd/.../public_security_privacy_guidelines.pdf.
[160] Privacy Act of 1974, 5 U.S.C. §552a (a)(7) (2006).
[161] Kris, "The Rise and Fall of the FISA Wall,"517.
[162] The National Counterterrorism Center, *Guidelines for Access, Retention, Use and Dissemination by the National Counterterrorism Center and Other Agencies of Information in Datasets Containing Non-Terrorism Information,* 12.

process for disseminating non-terrorism information to another member of the IC or a law enforcement agency but that process, unfortunately, does not provide substantial safeguards against the secondary use of information. Sections IV(C)(1) and IV(C)(2) address these procedures.

Section IV(C)(1)(b) states that U.S. person information held by the NCTC may be shared with any "federal, state, local, tribal, or foreign agency that is reasonably believed to have jurisdiction or responsibility for the investigation or prosecution to which the information relates and a need to receive such information for the performance of lawful governmental function" if there "reasonably appears to be evidence of a crime."[163] This allows information or evidence of a crime that is uncovered during a counter-terrorism investigation to be shared with other agencies that have no counter-terrorism mission. If this information was acquired as part of a terrorism investigation through use of the Government's expanded powers, then it is possible that the receiving agency had no legal recourse to obtain the information on its own. This has severely negative implications for privacy.

Section IV(C)(2)(c) of the guidelines governs bulk dissemination of U.S. person information, which carries less secondary use dangers but is nonetheless important. The guidelines state that the information determined to not have any counter-terrorism or counter-intelligence value may be disseminated if:

1. The receiving agency has privacy policies approved by the Attorney General.
2. The receiving agency has access restrictions in place that meet the NCTC's standards.
3. The DNI is able to certify that the dissemination is mission-critical.
4. The DNI is able to certify that the need for the information cannot be satisfied by any other means.[164]

These certifications must be presented in the form of a written memo from the DNI to the Assistant Attorney General for National Security and include detailed information on the agent(s) responsible for the data. Once the proper filings have been made, the Attorney General must approve the final request.[165]

The potential implications of inadequate secondary use restrictions are illustrated in the 2003 joint investigation of Wornick Co. and Remedy Intelligent Staffing.

In 2003, the FBI received intelligence that al Qaeda was planning to poison Meals Ready to Eat, manufactured by Wornick, that were bound for U.S. troops in Iraq and Afghanistan. During the investigation, the FBI acquired the IRS tax information of Wornick's employees to assist in narrowing down potential links to al Qaeda within the company. After initial checks of Wornick's personnel, the investigation expanded to Remedy, a staffing company

[163] *Ibid.*, 14.
[164] *Ibid*.
[165] *Ibid.*, 15.

that provided many of Wornick's employees. The FBI obtained IRS data on Remedy's employees to help narrow down suspects.

The FBI learned from analysis of Remedy's IRS data that it was utilizing illegal labor to fulfill its clients' staffing requests and regularly falsified employee eligibility forms filed with clients and the Government. The end result of the FBI's investigation, originally a counter-terrorism operation, was not the arrest or conviction of several employees on charges of providing material support to al Qaeda or for plotting against the U.S., but rather the prosecution of Remedy for hiring illegal immigrants. Twenty-eight illegal Remedy employees were deported and one of the company's vice presidents was convicted.[166]

The importance of enforcing labor laws is unquestionable and many people would probably take no issue with the result of the Wornick/Remedy case. From a privacy standpoint, however, these events are troubling. The Federal Government gathered and analyzed what would otherwise have been private tax and financial information as part of their terrorism investigation. The processes for acquiring that information were therefore unique to the nature of terrorism investigations and not based on Title III requirements or Fourth Amendment search and seizure restrictions. An investigation of Wornick or Remedy based purely on labor violations would have been structured very differently.

It is imperative, therefore, that proper restrictions are placed on secondary use of information gathered for counter-terrorism purposes. Federal, state, or local investigations of regular criminal activity not related to terrorism must follow the rules and regulations that have been laid out to govern those investigations and not make use of information that has been acquired through the expanded scope and means afforded to counter-terrorism functions. Doing so would expand the Government's special powers in terrorism and foreign intelligence investigations into the realm of criminal and civil enforcement and contradict many of the protections placed on privacy by Congressional legislation and the Constitution. This concept should be firmly entrenched into all sharing guidelines for the ISE and its partner agencies.

Information Collected on U.S. Persons Requires Particular Care

The NCTC Defines a U.S. Person as Any U.S. Citizen, Permanent Resident or Entity (Incorporated or Otherwise) Based in the U.S. and Not Under Predominantly Foreign Control.[167] An individual or entity that falls into this category has a number of Constitutional and statutory rights that require certain levels of privacy protection, therefore information shared throughout the ISE necessarily has specific rules when tied to a U.S. person. The category of U.S. person information applies to much of the information held within the ISE, and especially to information gathered as part of data mining initiatives and other pattern-based analyses.

[166] Dalia Naamani-Goldman, "Anti-terrorism Program Mines IRS' Records," *Los Angeles Times*, January 15, 2007, http://articles.latimes.com/2007/jan/15/business/fi-reveal15.

[167] The National Counterterrorism Center, *Guidelines for Access, Retention, Use and Dissemination by the National Counterterrorism Center and Other Agencies of Information in Datasets Containing Non-Terrorism Information*, Appendix 2.

The Culture of the Intelligence Community Resists Written Rules. A number of high profile controversies concerning U.S. person information, such as Project Shamrock and Total Information Awareness (TIA), have sensitized the IC to privacy and civil liberties protections. Privacy concerns, based on these programs and other media attention, have shaped many of the IC's operational practices. From a policy perspective, however, the IC's performance in this arena has been lacking. Five years after the creation of privacy, civil rights, and civil liberties guidelines that apply to all ISE participants, several key ISE partner agencies and departments still have yet to develop privacy protection policies of their own, as mandated by IRTPA Section 1016(d).

While all ISE participants have appointed senior privacy and civil liberties officers, the nature of the IC's work has made ODNI, CIA and the Departments of Defense, Treasury and Energy hesitant to adopt published privacy guidelines. The IC's culture resists written guidelines and rules wherever possible, instead opting for a more general understanding of how things should be done.

This method generates more freedom of action for the IC but is not sufficient to ensure that privacy and civil liberties are properly safeguarded. The exponential increase in information and technology available to the IC over the last two decades, and especially since 2001, requires that written, enforceable guidelines be created. Accountability is essential to any privacy policy. General understandings are not enforceable, and therefore do not meet the minimum standards of accountability necessary to guarantee that privacy is being respected and guarded.

Additional Care Must Be Taken When Dealing with U.S. Persons. Currently, agencies that are authorized to collect and hold U.S. person information are only able to use the information for specific tasks. They also have a strict timeline that governs how long they are legally allowed to retain it for other purposes. The National Counterterrorism Center, for example, is allowed to hold information on U.S. persons indefinitely, provided that that information has been verified to contain terrorism information.[168]

Prior to receiving that designation, the NCTC may only analyze the information to determine if it does contain terrorism information.[169] A five-year time limit has been placed on this analysis, at which point the NCTC must either classify the U.S. person information as terrorism information, and therefore keep it indefinitely, or purge it from their systems.

A tag-based classification system can be utilized to ensure that the appropriate protections are provided to U.S. persons' information. Data should be tagged at collection to indicate whether it contains U.S. person information. The data tag can then be utilized in conjunction with an "authorized use" formula to deny access to analysts from departments and agencies that are not permitted to collect U.S. person information. Moreover, the inclusion of date fields on data files can be used to automate compliance on time period limitations that govern the storage of U.S. person information. If data is not given a terrorism information tag by the expiration of its time limit, it can automatically be deleted.

[168] *Ibid.*, 9.
[169] *Ibid.*, 4.

The Foreign Intelligence Surveillance Act of 1978 (FISA) and Privacy

The FISA Court System Controls Surveillance and Searches. The Foreign Intelligence Surveillance Act, passed in 1978, governs the U.S. Government's ability to place surveillance on individuals within the U.S. and U.S. persons abroad. It was established to "provide legislative authorization and regulation for all electronic surveillance conducted within the U.S. for foreign intelligence purposes."[170] The law has received significantly increased attention since the September 11, 2001 terrorist attacks and subsequent USA PATRIOT Act, and remains an integral part of the Federal Government's counter-terrorism efforts.

FISA establishes two courts to address the issue of surveillance. The first is the Foreign Intelligence Surveillance Court (FISC), comprised of eleven district court judges appointed by the Chief Justice of the Supreme Court. The second is the FISA Court of Review, which consists of three district or circuit court judges, also appointed by the Chief Justice.[171] The FISC reviews requests for surveillance and issues warrants when appropriate. The Court of Review serves as an avenue of appeal above the FISC, and has been convened only once since it was created by the FISA legislation.[172]

The Central Principle Behind FISA is Foreign Intelligence Information. As originally enacted, the FISA legislation states that the "primary purpose" of any FISA surveillance or search warrant must be to obtain foreign intelligence information.[173] This was interpreted by the Department of Justice and IC to mean that FISA warrants could not be utilized for law enforcement purposes, which were handled separately through procedures backed by the Fourth Amendment.[174] The FISA "wall" was thus created, which strictly divided intelligence operations from criminal investigations. This wall, it is important to note, was designed to separate intelligence agencies from the Justice Department, not to separate intelligence agencies from each other.[175] The wall only came into play if criminal prosecution was an end goal.

Recent Amendments to FISA Have Altered Its Effectiveness. As part of the USA PATRIOT Act, the FISA statutes were amended to change the "primary purpose" language to "a significant purpose."[176] This change, though seemingly minor, was designed to greatly expand the Government's ability to use the FISA system by lessening the degree to which foreign intelligence information was required to be a part of the investigation. The Justice Department issued a set of guidelines to accommodate compliance with this change.

In 2002, the FISA Court of Review convened for the first and only time to review a rejected FISA warrant request based on the new, amended legislation and corresponding implementation guidelines. The Court ruled that the original FISA law had been misinterpreted since 1978 and that the division between intelligence and criminal

[170] Kris, "The Rise and Fall of the FISA Wall," 487.
[171] *Ibid.*, 489.
[172] *Ibid.,* 488.
[173] Best, *Sharing Law Enforcement and Intelligence Information: The Congressional Role*, 3.
[174] Kris, "The Rise and Fall of the FISA Wall," 488.
[175] *Ibid.*, 499.
[176] *Ibid.*, 494.

investigations was not necessary based on the original text of the legislation. The Court broadly

> "held that FISA allows complete coordination between intelligence and law enforcement officials, even if such coordination results in what might be characterized as law enforcement 'direction' or 'control' of an investigation. Under the Court of Review's decision, FISA may be used primarily for the purpose of obtaining evidence to prosecute a foreign spy or terrorist, and prosecutors may provide *any* advice, including advice on the use of FISA itself, in furtherance of such a purpose."[177]
>
> *The Rise and Fall of the FISA Wall*, 2006

The court subsequently ruled that the changes to FISA included in the USA PATRIOT Act, however, changed the meaning of the law and overturned the original interpretation. Under the Court of Review's ruling, the Patriot Act codified the wall into existence.[178]

Attempts to expand FISA therefore backfired somewhat, and the changes to FISA via §218 of the USA PATRIOT Act ended up cementing foreign intelligence as a primary requirement for any FISA surveillance. From a privacy standpoint, however, these changes do not amount to much. According to former Associate Deputy Attorney General David S. Kris, "the wall does not provide much protection for privacy because it does not change significantly the kinds of searches or surveillances that actually occur."[179] The changes to FISA have dealt only with behind-the-scenes coordination between intelligence and law enforcement agencies, and have left who or what can be placed under FISA surveillance relatively unchanged since 1978.[180]

Changes to FISA Have Little Impact on Information Sharing Efforts. As a pure intelligence tool, FISA has no effect on information shared through the ISE. Its use becomes restricted only when criminal prosecution comes into play. It has not been upheld against the Fourth Amendment as a viable tool for criminal investigation and instead is allowed only because of the Government's "special needs" under the category of foreign intelligence.[181]

[177] *Ibid.*, 513.
[178] *Ibid.,* 514.
[179] *Ibid.,* 520.
[180] *Ibid.,* 519.
[181] *Ibid.,* 517.

FISA Has Additional Qualifications to be Used Against U.S. Persons. The requirements to apply FISA surveillance to a U.S. person are only slightly more restrictive than to a foreign national. The individual or entity must be classified as an agent of a foreign power before FISA surveillance can apply, however the requirements for this leave significant room for subjective judgment. There are four primary ways for a U.S. person to become classified as an agent of a foreign power under FISA:

1. Engage in clandestine intelligence gathering on behalf of a foreign power.

2. Engage in sabotage or international terrorism on behalf of a foreign power.

3. Knowingly aid and abet an entity engaging in intelligence gathering on behalf of a foreign power.

4. Knowingly enter the U.S. with a false identification on behalf of a foreign power.[182]

These requirements all indicate action, however the legislation makes copious use of the phrases "involved in," "may involve" and "are about to involve" when describing these requirements, which leaves significant room for intelligence or law enforcement officials to make a FISA case prior to the U.S. person actually committing any crime.[183]

Evolving Constitutional Concerns

The Technology Available to the IC and Law Enforcement Community Has Rapidly Advanced. Technology is omnipresent in today's world. Practically everyone has a cell phone, a computer and Internet access. These devices, which many people consider to be an integral and irreplaceable part of their daily lives, present new opportunities for the IC and law enforcement community to execute surveillance and monitoring. These communities have also advanced their monitoring technology and, as a result, intelligence agencies and federal, state and local law enforcement officials now possess increasingly sophisticated surveillance and tracking capabilities.

Rapidly Advancing Technology Has Challenged Existing Notions of Privacy. A new era for the Constitution's Fourth Amendment has arrived with the advent of advanced technologies, such as GPS tracking devices, cell phone triangulation, aerial surveillance and data mining technology efforts like the Total Information Awareness (TIA) Program.[184] Existing legislation has proven inadequate to address the right to privacy in the world of ubiquitous public information created by technological advances. This has forced the U.S. Supreme Court to address the issue reconsidering how it defines privacy under the Fourth Amendment.

---

[182] *Ibid.,* 492.
[183] *Ibid*.
[184] The text of the Fourth Amendment reads: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

The Supreme Court Has Steadily Advanced the Right to Privacy in the Face of Advancing Technology. The first landmark decision from the Supreme Court regarding surveillance was *Olmstead v United States*, decided in 1928.[185] The *Olmstead* decision upheld warrantless wiretapping as constitutional based on the idea that federal investigators did not enter the home or office of the defendant to install the tap, and therefore no search or seizure actually occurred. All evidence was collected "through the use of the sense of hearing."[186] The Fourth Amendment's protections, at this point, were only applied to physical intrusions.

The Court reversed the *Olmstead* ruling in *Katz v United States (1967)*.[187] The *Katz* decision created the idea of the "reasonable expectation of privacy," based on Justice Stewart's argument in the decision that the "Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."[188] The Court, with the *Katz* decision, began to recognize technology's role as a regular force in society.

The *Olmstead* decision restricted Fourth Amendment search and seizure restrictions only to physical searches and seizures. *Katz* took the completely different approach and addressed the concepts of search or seizure in a more theoretical way, emphasizing the spirit and nature of a search over the physical act. Physical intrusion onto private property was no longer required to claim Fourth Amendment protections.

The Court used the reasonable expectation of privacy standard again in 1979, in *Smith v Maryland*.[189] The suit was based on the installation of a pen register, a device that records the digits dialed into a phone but does not record conversations. Installation and use of the device was challenged on Fourth Amendment grounds because no warrant was issued for the surveillance. The Court ruled that the pen register did not qualify for Fourth Amendment protections because any individual dialing a phone cannot have a reasonable expectation of privacy, at least for the numbers being dialed, due to the fact that the numbers will be necessarily transmitted to the phone company and seen by a third party.[190] Today, pen registers continue to fall outside the scope of Fourth Amendment protection.

Technology again came into play in the 1984 Supreme Court case *United States v Karo*.[191] In *Karo*, Drug Enforcement Administration agents installed a tracking device onto a can of ether, which was sold via a government informant to a group of cocaine dealers. The tracking device allowed the DEA to monitor the can's location as it moved through the network's storage facilities. An arrest warrant was later issued based on location data acquired via the tracking device. In the decision, the Court took an interesting approach to

[185] Olmstead v. United States, 277 U.S. 438 (1928).
[186] *Ibid.*
[187] Katz v. United States, 389 U.S. 347 (1967).
[188] *Ibid.*
[189] Smith v. Maryland, 442 U.S. 735 (1979).
[190] *Ibid.*
[191] United States v. Karo, 468 U.S. 705 (1984).

dealing with the tracking device. The ruling argued that physically installing the device without a warrant did not constitute a Fourth Amendment violation because the drug network's members purchased it willingly. When the tracker was activated, however, the Fourth Amendment entered the picture. Tracking the can onto private property constituted a search, therefore a warrant was required.

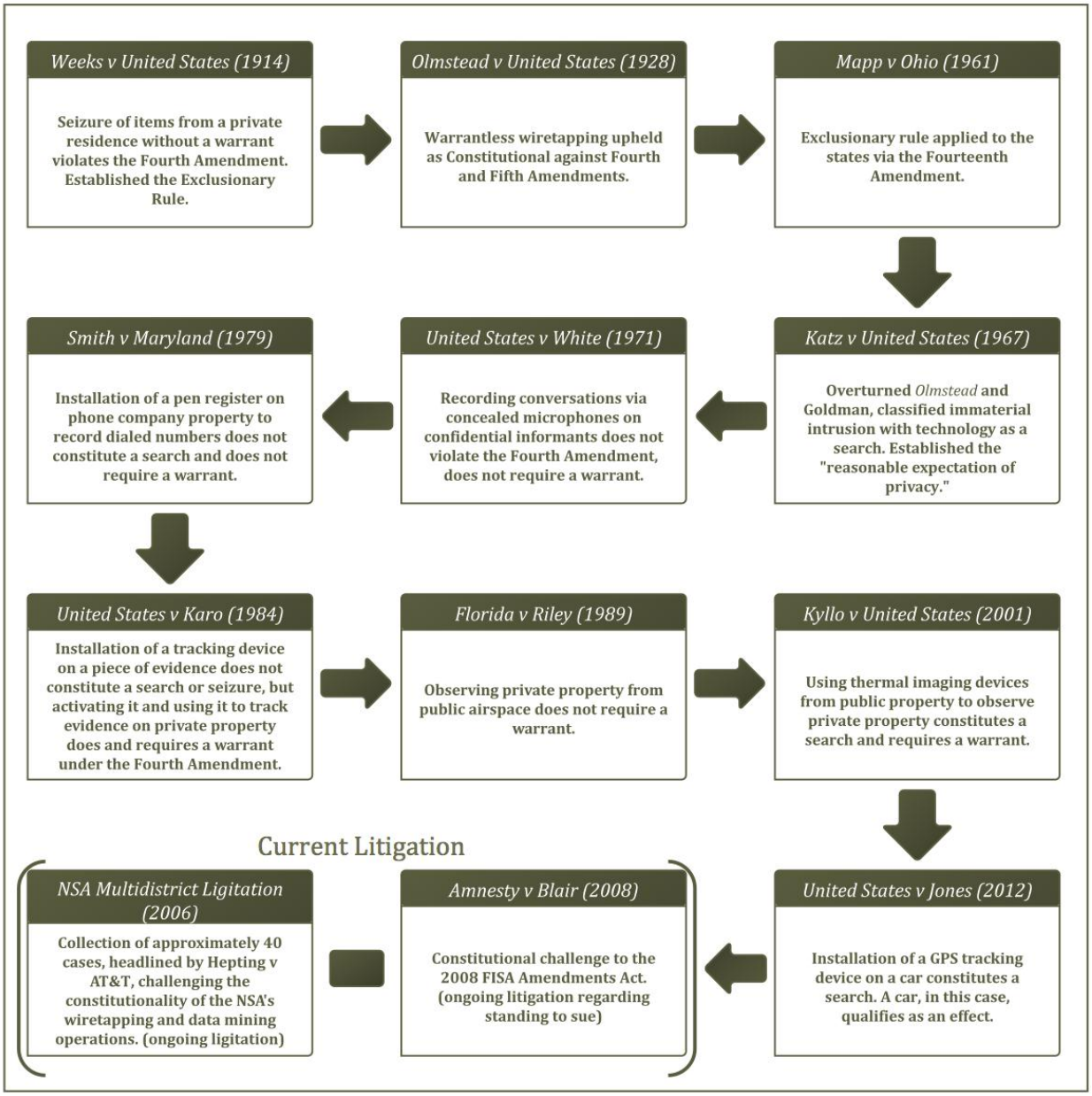

Fig. 4.1: Major Cases Involving the Fourth Amendment and Technology.

The Fourth Amendment was greatly expanded into the realm of technology with *Kyllo v United States (2001)*.[192] The issue in the case was the use of a thermal imaging device to monitor a private residence. The residence was suspected of housing marijuana growth facilities, so federal agents used the device from public property to analyze heat levels in

[192] Kyllo v. United States, 533 U.S. 27 (2001).

the home and determine if a greenhouse was present. The court ruled that use of the device constituted a search under Fourth Amendment criteria, and thus required a warrant. The decision was based on the idea that the thermal imaging violated the privacy that an individual can expect to have in his own home.

Justice Scalia, writing for the majority in *Kyllo*, recognized the growing importance of technology and addressed it directly in his opinion. He argued that

> "just as a thermal imager captures only heat emanating from a house, so also a powerful directional microphone picks up only sound emanating from a house-and a satellite capable of scanning from many miles away would pick up only visible light emanating from a house. We rejected such a mechanical interpretation of the Fourth Amendment in *Katz*, where the eavesdropping device picked up only sound waves that reached the exterior of the phone booth. Reversing that approach would leave the homeowner at the mercy of advancing technology--including imaging technology that could discern all human activity in the home. While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development." [193]
>
> *Kyllo v United States*, June 2001

The Court most recently addressed the Fourth Amendment in *United States v Jones (2012)*.[194] At the center of the *Jones* case was the installation of a GPS tracking device onto a suspect's personal automobile. The FBI and D.C. Metropolitan Police Department obtained a warrant to install the device but failed to do so within the allotted timeframe. Jones subsequently sued under the Fourth Amendment. In the decision, the Court ruled unanimously that the device's installation outside of the bounds of the warrant constituted a search under the Fourth Amendment and thus violated Jones' constitutional rights, however the Justices split 5-4 over the reasoning behind the violation.

The majority opinion, authored by Justice Scalia, argued that Jones' vehicle qualified as a personal "effect" under the text of the Fourth Amendment.[195] The majority's opinion was focused on traditional interpretations of the Fourth Amendment and did not directly address the use of technology in the case. Justice Alito, in the minority opinion, argued instead that the violation was based on the concept of reasonable expectation of privacy. As in Justice Scalia's opinion in *Kyllo*, Justice Alito acknowledged the rapidly increasing level of technology available to law enforcement officials and its expanding role in society. His decision was based on his belief that future tracking devices will not require a physical trespass to install, and was authored to provide guidance for similar cases in the future.[196] *United States v Jones (2012)* overturned *United States v Knotts (1982),* which found that electronic surveillance data could be utilized if the movements tracked occurred in public spaces.

[193] *Ibid*.
[194] United States v. Jones, 565 U. S. ____ (2012).
[195] *Ibid.*
[196] *Ibid.*

Current Litigation is Addressing the Issues of Wiretapping and Datamining. Two pieces of ongoing litigation address Fourth Amendment concerns in information collection and sharing. The first, *Amnesty v. Clapper*, was filed in 2008 by a coalition of parties led by the American Civil Liberties Union.[197] The suit challenges the constitutionality of the FISA Amendments 2008, which added several provisions to the 1978 FISA Act under a new title.[198] The ACLU argued that, as amended, FISA now violates the First and Fourth Amendments. The U.S. District Court for the Southern District of New York dismissed the case in 2009 on standing grounds, but the Second Circuit Court of Appeals reversed the dismissal on appeal and has remanded to case to the federal district court for trial on the merits of the case.[199]

The second case originated as *Hepting v. AT&T*, a class action suit filed in 2006 by the Electronic Frontier Foundation against AT&T. The suit argued that AT&T violated its customers' privacy rights by cooperating with NSA wiretapping and data mining programs. A multitude of other suits were filed against other telecommunications companies across the country during the same year. The related nature of the complaints drove the courts to consolidate the litigation within the United States District Court for the Northern District of California. The multi-district litigation currently encompasses over forty separate lawsuits and is still being disputed. [200]

Data Mining is Not Inherently Antithetical to Privacy

Since 9/11, Data Mining has Emerged as a Key Component of Counter-terrorism Initiatives.[201] Data mining is a catch a catch all phase for an analytical technique used to analyze data from different sources—including, in some instances, commercial data—in order to categorize it and identify relationships.[202]

[197] Amnesty v. Clapper, 09 F. 4112 (2nd Cir. 2011). Initially filed as Amnesty v. McConnell, the name of the defendant has been revised to reflect the current Director of National Intelligence.
[198] Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. Law No. 110-261, U.S. Statutes at Large (2008).
[199] "Amnesty et al. v. Clapper: FISA Amendment Act Challenge," American Civil Liberties Union, last modified February 12, 2012, http://www.aclu.org/national-security/amnesty-et-al-v-clapper.
[200] "NSA Multi-District Litigation," Electronic Frontier Foundation, last modified July 1, 2010, https://www.eff.org/cases/nsa-multi-district-litigation.
[201] Jeffrey W. Seifert, *Data Mining: An Overview* (Washington, DC: Congressional Research Service, 2004), summary, http://www.fas.org/irp/crs/RL31798.pdf.
[202]"Data Mining: What is Data Mining?" UCLA Anderson School of Management, http://www.anderson.ucla.edu/faculty/jason.frand/teacher/technologies/palace/datamining.htm.

> "Data mining involves the use of sophisticated data analysis tools to discover previously unknown, valid patterns and relationships in large data sets. These tools can include statistical models, mathematical algorithms, and machine learning methods (algorithms that improve their performance automatically through experience, such as neural networks or decision trees). Consequently, data mining consists of more than collecting and managing data, it also includes analysis and prediction."[203]
>
> *Data Mining*, An Overview, June 2001

Advancements in technology and an increase in information digitization have significantly enhanced data mining capabilities.[204] Data mining is widely used in both the public and private sectors for a variety of purposes. In 2005, the GAO reviewed five Government data mining programs, each employed for a variety of purposes, such as program management, law enforcement, and intelligence analysis.[205] In the counter-terrorism arena, data mining programs have focused on discovering relationships between known and unknown terrorists, detect the financing of terrorist activities, and watch listing.

Data mining is a buzz word that elicits a host of U.S. Persons and Secondary Use issues, concerning privacy. At its core, however, data mining is merely an analytic technique used to manage and make sense of large volumes of structured and unstructured data. It is the content of the data in the data sets that are being mined that determine the legality of data mining operations.

On the analytic side, the strength of the algorithms that a data mining project employs determines utility. An algorithm based on faulty logic can also have damaging effects on privacy. It is also a waste of Government resources—money, time, and human capital—which inevitably weakens counter-terrorism efforts.

A major concern with data mining is one that underlines information sharing in general: inaccurate data records. Privacy advocates note that inaccurate data, not only hinder national security but also endangers the privacy rights U.S. persons who are unfairly implicated as threats to national security. They also assert that data mining programs make it easier for the Government to access vast amounts of information about individuals. Government data mining projects often utilize private sector data that, privacy advocates argue, was originally collected with certain expectations of privacy.

There are a number of court cases being litigated that involve these key privacy issues. Thus, the constitutional limits on Government data mining projects are currently in a state flux.

---

[203] Seifert, *Data Mining: An Overview*, 1.
[204] The Constitution Project, *Principles for Government Data Mining: Preserving Civil Liberties in the Information Age* (Washington, DC, 2010), 8, http://www.constitutionproject.org/pdf/DataMiningPublication.pdf.
[205] General Accountability Office, *Data Mining: Agencies Have Taken Key Steps to Protect Privacy in Selected Efforts, but Significant Compliance Issues Remain (*Washington, DC, 2005), 11, http://www.gao.gov/assets/250/247433.pdf.

Since 2007, Data mining has been regulated by the Federal Agency Data Mining Reporting Act of 2007. The Act requires the head of any department or agency that is involved either developing or engaging in a data mining activity, in coordination with the organization's privacy officer, to submit a report to Congress. The report must include:

> "(A) A thorough description of the data mining activity, its goals, and, where appropriate, the target dates for the deployment of the data mining activity. (B) A thorough description of the data mining technology that is being used or will be used, including the basis for determining whether a particular pattern or anomaly is indicative of terrorist or criminal activity. (C) A thorough description of the data sources that are being or will be used. (D) An assessment of the efficacy or likely efficacy of the data mining activity in providing accurate information consistent with and valuable to the stated goals and plans for the use or development of the data mining activity. (E) An assessment of the impact or likely impact of the implementation of the data mining activity on the privacy and civil liberties of individuals, including a thorough description of the actions that are being taken or will be taken with regard to the property, privacy, or other rights or privileges of any individual or individuals as a result of the implementation of the data mining activity. (F) A list and analysis of the laws and regulations that govern the information being or to be collected, reviewed, gathered, analyzed, or used in conjunction with the data mining activity, to the extent applicable in the context of the data mining activity. (G) A thorough discussion of the policies, procedures, and guidelines that are in place or that are to be developed and applied in the use of such data mining activity in order to—(i) protect the privacy and due process rights of individuals, such as redress procedures; and (ii) ensure that only accurate and complete information is collected, reviewed, gathered, analyzed, or used, and guard against any harmful consequences of potential inaccuracies."[206]
>
> *Federal Agency Data Mining Reporting Act of 2007*, August 2007

The Federal Agency Data Mining Reporting Act of 2007 has added an important oversight function to Government data mining programs.

[206] Federal Agency Data Mining Reporting Act of 2007, 42 U.S.C. § 2000 (2007).

Legislative and Regulatory Assessment

The ISE Guidance Pamphlet on Civil Rights and Civil Liberties Protection States, "When Evaluating the Impact of the ISE on Civil liberties, it is Important to Keep in Mind the Legal and Cultural Importance of Civil Liberties in American Life."[207] This acknowledges that, like security, the protection of the privacy, civil liberties and civil rights of U.S. persons is a key obligation of the Government that must be central to information sharing practices.

To address this responsibility, the regulations and core pieces of legislation that govern information sharing incorporate the protection of privacy rights. These policies, however, must be clarified to meet the constantly evolving technological capabilities to collect, store, and analyze data that are available to the intelligence and law enforcement communities.[208] Moreover, the increasing role played by homegrown extremists drives a need for sophisticated privacy policies that enable the IC and law enforcement communities to protect against this threat while still safeguarding privacy. These policies must also incorporate methods for protecting privacy in an increasingly globalized society, which has made it difficult to differentiate between data collected from foreign and U.S. persons.[209]

An increasing amount of attention has focused on this area in recent years. Efforts have been made by the IC and policymakers to incorporate these nuances into privacy policies. More work still needs to be done throughout the Government, however, to clarify these policies. The lack of consistent interpretations of these policies across the Government has led to confusion on the analyst level.

The unprecedented nature of the 9/11 attacks created a tendency to over share information in the immediate aftermath of the tragedy that potentially violated privacy rights. In recent years, however, confusion about privacy policies has shifted the pendulum in the opposite direction and created a sensitivity to risk when it comes to sharing potentially critical information.[210] On the department and agency levels, unique and specific privacy policies are needed to cater to each organization's specialized legal authorities.

There is also a need for a basic level of clarification regarding key laws and statutes that govern the national security and law enforcement communities. This necessitates a degree of standardized training both within organizations, pursuant to their specific authorities, and across organizations, which acculturates individuals throughout these communities to the interpretations of key laws and regulations that govern ISE partner organizations with

---

[207] Information Sharing Environment, *Civil Rights and Civil Liberties Protections* (Washington, DC, 2008), 4, http://ise.gov/sites/default/files/CR-CL_Guidance_08112008.pdf.
[208] *Hearing on Information Sharing in the Era of WikiLeaks: Balancing Security and Collaboration,* Before the Senate Comm. on Homeland Security and Governmental Affairs, 112th Cong. (2011) (statement on Behalf of the Markle Task Force on National Security in the Information Age), 8, http://ise.gov/sites/default/files /Markle_Foundation_Written_Testimony_March2011.pdf.
[209] *Ibid*.
[210] *Ibid.*, 8.

different authorities. Increasing levels of standardization and transparency advances compliance, public trust, and national security.

The below assessment examines the efficacy of the privacy components of the primary laws and regulations that govern information sharing and the intelligence community.

The Privacy Act and Its Relevant Exemptions

The Privacy Act of 1974 Provides the Basis for the Federal Government's Privacy Policies. The Federal Government's collection, maintenance, use and dissemination of personally identifiable information is governed by the Privacy Act of 1974. The Act is the basis for the Fair Information Practices, which provide a multi-step guideline for formulating a privacy policy that effectively protects individual privacy.

The Privacy Act directly addresses government databases by creating the concept of a system of records. A record is defined as "any item, collection, or grouping of information about an individual that is maintained by an agency and contains his name or other personal information."[211] A system of records refers to "a group of records under the control of any agency from which information is retrieved by the name of the individual or by an individual identifier."[212] Under these definitions, most of the Information Sharing Environment's systems qualify as a system of records and are thus governed by the Privacy Act.

The central pillar of the privacy protections created by the Privacy Act is the Government's provision of public notice of its actions. The Act requires that any substantial modification of an existing system of records or the creation of a new system be accompanied by a notice posted in the *Federal Register* that explains how the information in it will be used and why it is necessary for the Government to acquire and hold it. This notification must provide a general overview of the system's operation and use, as well as inform individuals of the process for accessing or correcting the information relevant to them.[213] These concepts of notice, access and redress are the foundations of the Fair Information Practices.

The Act, however, allows exemptions for certain law enforcement activities.[214] These exemptions are designed to protect the integrity of active investigations but can undermine the protection of privacy if not properly monitored. For information used in criminal law enforcement, the Privacy Act allows agencies to exempt themselves from the requirements to provide individuals access to their records, to notify individuals of the purpose and use of collected information at the time it is collected, and the Act's requirements for maintenance of data.[215] Without the ability to access their records, individuals also lose the ability to verify and challenge them.

These exemptions therefore give broad leeway to agencies to not disclose the nature of the

[211] Privacy Act of 1974, 5 U.S.C. §552a (a)(4) (2006).
[212] *Ibid.,* (a)(5).
[213] *Ibid.,* (e).
[214] *Ibid.,* (j, k).
[215] *Ibid.,* (j)(2).

information they collect and maintain in systems of records, as the driving force behind such collection is often related to criminal activity. This is also the case for data shared through the ISE for counter-terrorism purposes.

The Freedom of Information Act and Its Relevant Exemptions

The Freedom of Information Act (FOIA), Originally Passed in 1966, Requires Certain Agency Records to be Disclosed to the Public Upon Request and Lays out the Procedures Necessary to Release Information Contained Within Them. As amended, it reinforces the right of an individual to view and verify his own records held by the Government that are laid out in the Privacy Act of 1974.

The Act, as expected, contains several specific categories of data that are exempt from requests for public disclosure. The exemptions with relevance to the ISE, outlined in subsection (b) of the legislation, are as follows:

1. Information sensitive to national security or foreign policy, and appropriately classified by the Executive.[216]

2. Information otherwise exempted from public disclosure by statute.[217]

3. Privileged or confidential personal information, such as trade secrets or financial data.[218]

4. Inter- or intra-agency memos that would only be accessible via litigation.

5. Personnel or medical files.[219]

6. Information that would interfere with law enforcement operations by disrupting legal proceedings, depriving an individual of a fair trial or endangering sources and methods.[220]

The Freedom of Information Act has undergone numerous expansions and contractions since its original passage in 1966, via both Congressional action and Executive Order. The relevant changes are outlined below.

The Privacy Act of 1974 contained several amendments to the FOIA. These amendments provide three rights to individuals:

1. The right for an individual to see the records related to him or her, subject to the Privacy Act's exemptions.

2. The right for an individual to amend his record if it contained inaccurate, incomplete or irrelevant information.

---

[216] Freedom of Information Act, 5 U.S.C. §552(b)(1)(A, B) (2007).
[217] *Ibid.,* (b)(3).
[218] *Ibid.,* (4).
[219] *Ibid.,* (6).
[220] *Ibid.,* (7)(A-F).

3. The right for an individual to sue the Government for violating these provisions, or for allowing others to see the record improperly.[221]

These criteria were designed to allow the Privacy and Freedom of Information Acts to work together to enhance an individual's ability to know what information the Federal Government holds on him or her.

The 1976 Government in the Sunshine Act directly amended the third exemption in the original FOIA. It detailed ten sub-categories of information that can be exempted from FOIA requests under the third exemption category.[222] The six relevant sub-categories are:

1. National defense information.

2. Information dealing exclusively with internal personnel operations.

3. Information accusing an individual of a crime.

4. Information that would constitute a privacy violation.

5. Information related to ongoing investigations with potential to negatively impact the investigation.

6. Information concerning legal proceedings that the agency is involved in.

Executive Order 12356, signed by President Reagan in 1982, dealt primarily with the procedures and system used by the Federal Government to classify data as U.S. Government classified information.[223] This classification system had a significant effect on the Freedom of Information Act. Subsections (b)(1)(A) and (b)(1)(B) of the FOIA allow any information deemed to have implications for national security or foreign policy, under criteria established by the Executive, to be exempted from public disclosure via a FOIA request.

The certification of the classification system by the Order therefore allowed all U.S. Government classified information to be exempted from FOIA requests under this provision. This greatly reduced the amount of information that could be released under FOIA and continues to disqualify a large amount of classified data held in the ISE from eligibility for FOIA requests.

The most recent changes to the FOIA came with Executive Order 13526, issued by President Obama in 2009. This order grants agencies the authority to retroactively classify data, even after it has been the target of a FOIA request.[224] Classifying the data officially tags it as sensitive to national security, and therefore again allows the Government to prevent its public disclosure under FOIA's exemptions.

---

[221] Privacy Act of 1974, 5 U.S.C. §552a (d) (2006).
[222] Government in the Sunshine Act of 1976, 5 U.S.C. §552b(c)(1-10) (1976).
[223] Exec. Order No. 12,356, 3 C.F.R. 166 (1983).
[224] Exec. Order No. 13,526, 3 C.F.R. 298 (2009).

Executive Order 12333 (1981)

Executive Order 12333, Signed on December 4, 1981 and Clarifies the Goals, Direction, Duties and Responsibilities of the Agencies and Departments That Make up the U.S. Intelligence Community and the National Security Council (NSC). The order has been amended on three occasions since 9/11 to comply with IRTPA and integrate additional recommendations from the 9/11 and WMD Commissions.[225] Executive Order 12333 and its amended versions—Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008)—have each set out to ensure the protection of U.S. persons' right to privacy.

The 1981 version of the order prohibits the collection, dissemination, or storage of non-publically available information concerning the activities of U.S. persons. A limited list of exceptions to this rule include participation in FBI investigations and other IC activities, espionage and counter-intelligence, activities that pose a clear threat to IC facilities and personnel, and "information collected, received, disseminated or stored by the FBI and necessary to fulfill its lawful investigative responsibilities."[226] This version clearly delineates the Intelligence Community's responsibility to protect the privacy rights of U.S. persons.

The events of September 11th, however, created the need for certain elements of the Intelligence Community to collect basic data on all U.S. air passengers flying within, to and from U.S. airspace in order to vet passengers against terrorist watch lists. The amended versions of EO 12333 incorporate this need, while also striving to protect privacy.

The current revision states that intelligence activities must continue "to protect fully the legal rights of all U.S. persons, including freedoms, civil liberties, and privacy rights guaranteed by Federal law."[227] It further requires that intelligence systems and architectures comply with "information privacy, and other legal requirements."[228] Lastly, it contains an oversight provision to ensure the compliance of IC organizations with privacy and civil liberties. While the amended version of EO 12333 contains important mandates to preserve the right to privacy, it is only as strong as initiatives to train those in the IC to understand its proper application to their everyday work and oversight activities that constitute a check on the IC, holding them accountable to the standards it establishes.

E-Government Act of 2002

The E-Government Act of 2002 is a Federal Law Created to Manage and Advance Electronic Government Services and to Promote Internet-based Information Technology as a Medium of Interaction Between the Government and U.S. Citizens.[229] A key component of the legislation establishes mechanisms for the protection of the right to privacy in government

[225] "Mission," National Security Agency Central Security Service, last modified April 15, 2011, http://www.nsa.gov/about/mission/index.shtml.
[226] Exec. Order No. 12,036, 3 C.F.R. 112 (1979).
[227] Exec. Order No. 13,470, 3 C.F.R. (2008).
[228] *Ibid*.
[229] E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat 2899 (2002).

information collection, as well as for existing PII data within electronic government information systems.[230]

The legislation introduces the Privacy Impact Assessment (PIA) as a tool to enhance privacy. The Act requires that an agency conduct a PIA on any newly-developed or modified IT system that "collects, maintains, or disseminates" PII and before initiating a new collection of PII that "will be collected, maintained, or disseminated using information technology."[231]

In accordance with policies and guidelines set forth by the Office of Management and Budget (OMB), PIAs examine the planned efforts of such initiatives in order to ensure that their handling of PII is in compliance with the relevant "legal, regulatory, and policy requirements" that pertain to privacy protections.[232] PIAs also address the risks and effects of the proposed initiatives. Where potential privacy risks are identified, the agency must explore alternative methods for handling information that mitigate those risks.[233] All PIAs include the following:

> "(I) [a description of] what information is to be collected; (II) why the information is being collected; (III) the intended use of the agency of the information; (IV) with whom the information will be shared; (V) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared; (VI) how the information will be secured; and (VII) whether a system of records is being created under section 552a of title 5, United States Code, (commonly referred to as the `Privacy Act').''[234]
>
> *E-Government Act of 2002*, December 2002

PIAs are intended to be public documents that promote transparency and accountability. The exercise of creating a PIA, its evaluation by the applicable agency's chief information officer, and its public availability present three opportunities to ensure that the right to privacy is protected when PII information is collected and shared.

A PIA ceases to be a public document, however, if agency's chief information officer determines that the PIA would reveal "classified, sensitive, or private information" that must be protected "for security reasons."[235] In these instances, although the first two checks are preserved, the public check on the right to privacy is removed and transparency is reduced. This is an inherent tradeoff when dealing with highly sensitive national security

[230] General Accountability Office, *Agencies Have Taken Key Steps to Protect Privacy in Selected Efforts, but Significant Compliance Issues Remain* (Washington, DC, 2005), http://www.gao.gov/new.items/d05866.pdf.
[231] E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat 2921 (2002).
[232] General Accountability Office, *Agencies Have Taken Key Steps to Protect Privacy in Selected Efforts, but Significant Compliance Issues Remain*, 24.
[233] Office of Management and Budget Director Joshua B. Bolten to Heads of Executive Departments and Agencies, M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, 26 September 2003, Executive Office of the President, Office of Management and Budget, §2A (f).
[234] E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat 2922 (2002).
[235] *Ibid.*

information. Nonetheless, the capacity of the first two checks to ensure an adequate level of accountability relies on the overall strength of oversight regarding the protection of the right to privacy within the agency and the intelligence community. A better understanding of these oversight processes in the public sphere will promote trust and strengthen efforts to protect national security.

It is important to note that for the purposes of a PIA, PII interpreted as information held in an "identifiable form," which is defined as "any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means."[236] The indirect component of this definition implies that data containing components or unique patterns that alone or together can be analyzed to determine identity is categorized as PII. This broad interpretation of PII has important implications for efforts to comply with privacy protections regarding the collection, sharing, and data mining of U.S. person information through technological based solutions, such as anonymization.

Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)

Public Law 108-458, Known as the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), was Enacted on December 17, 2004. It restructured counter-terrorism efforts and the intelligence community by establishing the Information Sharing Environment and the Office of the Director of National Intelligence (ODNI). Considerations for the protection of the right to privacy are interspersed throughout the new authorities created by IRPTA. These considerations represent several efforts to guarantee that the checks and balances necessary to safeguard privacy are in place as the Government works to implement the recommendations of the 9/11 Commission Report.

IRTPA identifies the establishment of "protections for individuals' privacy and civil liberties" as one of the key attributes of the ISE's operations along with the inclusion of "strong mechanisms to enhance accountability and facilitate oversight, including audits, authentication, and access controls."[237] The latter enhances both privacy protections and security. IRTPA requires the ISE to produce an annual Performance Management Report to Congress that includes efforts made by the Federal Government to guarantee "the accuracy of information about individuals" within the ISE, as well as "an assessment of the privacy and civil liberties protections of the ISE."[238] These measures seek to address key concerns of privacy advocates who argue that inaccurate U.S. person information not only hinders national security efforts but also constitutes a grave threat to the right to privacy.

Subtitle C of IRPTA, the Homeland Security Civil Rights and Civil Liberties Protection Act of 2004, amends the Homeland Security Act of 2002 to enhance the protection of privacy in Department of Homeland Security activities. Section 8303 of IRPTA greatly expands the role of the Officer for Civil Rights and Civil Liberties. The DHS Officer for Civil Rights and Civil Liberties is granted additional oversight authority to ensure that the Department's activities and programs are in compliance with "constitutional, statutory, regulatory, [and]

[236] *Ibid.*
[237] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3666 (2004).
[238] *Ibid*., 118 Stat. 3670 (2004).

policy" concerning the protection of the right to privacy, civil liberties, and civil rights.[239] The Officer of Civil Rights and Civil Liberties is also given a proactive role in the development and implementation of policies and procedures designed to incorporate the protection of privacy in the Department's programs and activities.[240]

Section 8304 of IRPTA expands the responsibilities of DHS Office of the Inspector General by incorporating the investigation of civil rights and civil liberties abuses into its duties. IRPTA also requires that the office's personnel receive "sufficient training to conduct effective civil rights and civil liberties investigations." [241] Moreover, IRPTA promotes for the coordination among DHS' Officer of Civil Rights and Civil Liberties, Office of the Inspector General, and Privacy Officer to allow the Department's efforts to protect civil liberties and civil rights to be efficient, thorough, and effective. These provisions have positioned DHS to be the ISE leader in the advancement of privacy, civil liberties, and civil rights protections. Its efforts in this arena are robust, transparent, and well-respected.

The Homeland Security Act of 2002 and IRTPA were amended on August 3, 2007 by Public Law 110-53, known as the Implementing Recommendations of the 9/11 Commission Act of 2007. Among the amendments was an emphasis on enhancing privacy protections under Title V—Improving Intelligence and Information Sharing within the Federal Government and with state, local, and tribal governments, and Title VIII—Privacy and Civil Liberties. The amendments further strengthen the authority of the DHS Privacy Officer to safeguard privacy, through granting the position an investigatory mission backed up with the power to access necessary documents and issue subpoenas subject to Secretary approval.[242]

Privacy protections set forth in IRPTA are expanded in Section 803 of the 9/11 Commission Act of 2007 through clarification of IRPTA's original mandate that "each executive department or agency with law enforcement or antiterrorism functions should designate a privacy and civil liberties officer." [243] Each of these organizations, including the Departments of Defense, State, Health and Human Services, Treasury and Homeland Security, the ODNI and CIA, are required to appoint a senior officer in this role to that their department upholds privacy and civil liberty protections prescribed by law, policy, and regulations in their counter-terrorism efforts.

The Act also grants privacy officers the authority to carry out periodic internal investigations to review the organization's compliance with privacy protections and complaints from individuals alleging that the organization has violated their right to privacy in some manner. Privacy Officers are subordinate to their agency or department head. Ultimately, the efficacy of the Privacy Officer's work is dependent on the level of cooperation granted by the agency or department head, who is instructed by Section 803 to provide adequate assistance in these endeavors.[244]

---

[239] *Ibid*., 118 Stat. 3867 (2004).
[240] *Ibid*.
[241] *Ibid*., 118 Stat. 3868 (2004).
[242] Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, 121 Stat. 358 (2007).
[243]Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3688 (2004).
[244] Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, 121 Stat. 360 (2007).

The 9/11 Commission Report (2004)

The 9/11 Commission Report, Released July 22, 2004, Posits Recommendations to Enhance the Nation's Counter-terrorism Abilities Based on Its Analysis of the Deficiencies that Failed to Prevent the 9/11 Attacks. The report acknowledges that counter-terrorism efforts adequate to meet "the real and ongoing threat" require a "shift of power and authority to the Government [that] calls for an enhanced system of checks and balances to protect the precious liberties that are vital to our way of life."[245] The report makes a number of recommendations to promote the protection of privacy, civil liberties, and civil rights in the Government's counter-terrorism efforts:

1. Guidelines for information sharing should contain safeguards that protect the privacy of those whose information is shared as a result.

2. Substantial changes in collection and sharing of intelligence call for the establishment of a Federal Government body with the mission of oversight to ensure the appropriate consideration of privacy concerns in counter-terrorism efforts.

3. Policy guidelines for information sharing and use should be overseen by a board within the Executive Branch to confirm the Government's commitment to the protection of the right to privacy, civil liberties, and civil rights.[246]

Together, these recommendations form a mandate for the Government to ensure that efforts taken to enhance information sharing in order to advance the efficacy of counter-terrorism initiatives also incorporate the protection of the right to privacy. Accordingly, endeavors to promote safeguards for privacy are evidenced by sections of IRPTA, Executive Order 13353, ICD 501, and the amended versions of Executive Order 12333.

Executive Order 13353 (2004)

Executive Order 13352, Issued on August 27, 2004 by President George W. Bush, Set Out to Reassert in Policy, the Government's Obligation to Protect the Right to Privacy in its National and Homeland Security Functions. As noted by Garrett Hatch in the Congressional Research Service report entitled *Privacy and Civil Liberties Oversight Board: New Independent Agency Status*, it was the embodiment of the 9/11 Commission's assertion of the need for "a board to oversee adherence to presidential guidelines on information sharing that safeguard the privacy of individuals about whom information is shared, and adherence to guidelines on the executive's continued use of powers that materially enhance security."[247] The order established the President's Board on Safeguarding American's Civil Liberties as the mechanism to oversee the performance of departments and agencies in fulfilling their

[245]Kean et al., *The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States,* 394.
[246]*Ibid.,* 395.
[247]Garrett Hatch, *Privacy and Civil Liberties Oversight Board: New Independent Agency Status*, (Washington, DC: Congressional Research Service, 2011), 1, www.fas.org/sgp/crs/misc/RL34385.pdf.

privacy protection responsibilities while carrying out their national and homeland security duties.

The President's Board on Safeguarding American's Civil Liberties unfortunately only represented the first unsuccessful expression of an effort to advance privacy protections in information sharing practices through an oversight board. The board has undergone multiple statutory reorganizations due to concerns regarding both a lack of authority and impartiality because of its original categorization as an agency within the Executive Office of the President (EOP).[248] The board was reconstituted as the Privacy and Civil Liberties Oversight Board (PCLOB) in August of 2007 by Public Law 110-53 as an independent entity and given the mandate "to ensure that efforts to combat terrorism do not encroach on vital freedoms."[249]

The board has also suffered from the failure of both the present and previous presidential administrations to staff it in an expeditious manner. Consequently, the board was only active for a brief period of time between May 14, 2006 and January 30, 2008.[250] The current administration did not nominate individuals to fill the board's remaining vacancies until December 16, 2011. At this time, Senate confirmation hearings have yet to occur for any of the board's five positions. The result has been the prolonged absence of any entity with the broad, independent oversight authority to ensure that counter-terrorism efforts do not infringe on privacy protections.

Intelligence Community Directive Number 501 (ICD 501) (2009)

Intelligence Community Directive Number 501 (ICD 501) Sets Forth a Policy for Information Sharing Within the IC, Made Effective January 21, 2009. Engrained in ICD 501's information sharing policy is an underlying mandate to ensure proper protection of the privacy and civil rights of U.S. persons, as required "by the Constitution, Federal Statutes, Executive Orders, Presidential Directives, court orders, and Attorney General approved guidelines," and consistent with the ISE's 2006 privacy, civil liberties, and civil rights guidelines.[251] Furthermore, ICD 501 asserts that plans to implement the policy it sets forth must address privacy.

The Directive also gives the ODNI Civil Liberties Protection Officer the mandate to assist components of the IC with the task of ensuring that their implementation of the Directive's policy is consistent "with applicable requirements to protect privacy and civil liberties." [252] The components of ICD 501 relating to privacy and civil liberties constitute an effort by the ODNI to safeguard the protection of the right to privacy in its initiative to transform the IC from a community composed of isolated stovepipes to an integrated one that emphasizes the importance of information sharing to advance national security.

---

[248] *Ibid*., summary.
[249] "Privacy and Civil Liberties Oversight Board Seats Remain Vacant," The Markle Foundation, last modified April 15, 2011, http://www.markle.org/news-events/connected-world-blog/privacy-and-civil-liberties-oversight-board-seats-remain-vacant.
[250] Hatch, *Privacy and Civil Liberties Oversight Board: New Independent Agency Status*, 4, 6.
[251] Office of the Director of National Intelligence, *Intelligence Community Directive Number 501: Discovery and Dissemination or Retrieval of Information within the Intelligence Community.*
[252] *Ibid*.

[This page is intentionally left blank]

Maintaining Security for Shared Information

> "Agencies that do not take adequate steps to ensure information security risk having information improperly exposed, altered, or destroyed." [253]
>
> *Data Mining, Agencies Have Taken Key Steps to Protect Privacy in Selected Efforts,* but Significant Compliance Issues Remain, General Accountability Office, August 2005

Security is a Vital Component of the Information Sharing Environment. Sharing of information and the security of information are, however, often conflicting objectives. The sharing of information inherently reduces its security. Some experts assert that rather than constituting a definitive tradeoff, the "need-to-share" and "need-to-know" exist on a spectrum and that the decision to emphasize one over another presents a false choice.[254]

To some within the Intelligence Community the word "share" represents an occupational anathema that requires the development of a new paradigm such as "authorized purpose"—a wordplay on "authorized use" that only differs in semantics—in order to fulfill the need that intelligence analysts, LEAs, and counter-terrorism officials across the Government have for certain sensitive information that resides outside of their agencies or departments.

In accordance with the later schools of thought, the ODNI has sought to update "need-to-know" with the concept of "authorized use" as a mechanism for incorporating "need-to-share" into "need-to-know." Here the emphasis is on an expansion of "need-to-know" based access, technical protections that limit—and when appropriate prohibit—the capacity to "misappropriate, manipulate, or transfer data," and auditing and monitoring actions as a counter-intelligence (CI) feature to detect anomalous activity.[255]

While the act of sharing information does expose it to more individuals, regardless of their "need-to-know," and thus reduces its security on an intrinsic level, the 9/11 events and foiled terrorist plots since then demonstrate the necessity of information sharing efforts within a secure context.

---

[253] Government Accountability Office, *Data Mining: Agencies Have Taken Key Steps* (Washington, DC, 2005), http://www.gao.gov/new.items/d05866.pdf.
[254] Richard A. Best, Jr., *Intelligence Information: Need-to-Know vs. Need-to-Share* (Washington, DC: Congressional Research Service, 2011), 13, http://www.fas.org/sgp/crs/intel/R41848.pdf.
[255] *Ibid*., 7.

Expansion of Security Clearances Following 9/11

> "The national interest requires that certain information be maintained in confidence through a system of classification in order to protect our citizens, our democratic institutions, and our participation within the community of nations. The unauthorized disclosure of information classified in the national interest can cause irreparable damage to the national security and loss of human life."
>
> *Executive Order 12968*, August 1995

The Expansion of the Federal Government and LEA's Counter-terrorism Efforts After 9/11, Combined with the Overall Personnel Requirements of the War on Terrorism, Led to a Rapid Increase in the Number of Individuals with Security Clearances. For example, the Government Accountability Office (GAO) reports that in FY 2003 DOD issued approximately "63,000 more eligibility determinations for industry personnel [i.e. civilians] in fiscal year 2003 than it did 2 years earlier, an increase of 174 percent."[256] More recently, the ONDI reported that the number of new security clearances issued between FY 2009 and FY 2010 increased by 45,076.[257] The number of individuals holding a Confidential/Secret Clearance on October 1, 2009 was 2,814,444 and 2,847,040 on October 1, 2010.

Top Secret Clearances were held by 1,406,571 individuals on October 1, 2009 and 1,419,051 on October 1, 2010.[258] The large and continually increasing number of security clearances issued, particularly those that are Top Secret, present a security challenge. Simply put, increased clearances equal increased risks for unauthorized disclosure of sensitive national security information. Nonetheless, there is a need for a large pool of individuals with clearances. The number of clearances is merely a reflection of the work being conducted to safeguard the Nation. There is a need to acknowledge, however, the drawbacks of having large numbers of cleared individuals and additional procedural and personnel-based security policies must be created to safeguard information from unauthorized disclosure.

Inclusion of State and Local Law Enforcement in Federal Systems

Prior to the 1990s, Federal Agencies and Departments Did Not Have the Authority to Grant Local LEAs Access to Classified Information. Following a series of DOJ memorandums in 1993 that vested this authority with the FBI, in 1995 Executive Order 12968 allowed the DOJ to disseminate classified information for "law enforcement or counter-intelligence purposes."[259] In 2002, the FBI Security Clearance Process Brochure outlined security clearance procedures for local LEAs. The security clearance investigation and adjudication

[256] Government Accountability Office, *DOD Personnel Clearances: Preliminary Observations* (Washington, DC, 2004), 12, http://www.gao.gov/assets/120/110903.pdf.
[257] Office of the Director of National Intelligence, *Annual Intelligence Authorization Act Report* (Washington, DC, 2010), 3, http://www.fas.org/sgp/othergov/intel/clearance.pdf.
[258] *Ibid.*
[259] Exec. Order No. 12,968 3, C.F.R. (1995).

procedures for local LEAs are the same as the ones utilized for FBI personnel.[260] In order for a local LEA officer to obtain a clearance, a state or local LEA official must make the determination that a member of their organization has a need. The official then contacts the FBI field office, which is responsible for establishing the officer's "need-to-know," and the appropriate level of clearance required in cases where "need-to-know" is established.[261]

The Department of Homeland Security Undersecretary for Intelligence and Analysis was granted the authority to provide state, local, private sector, and tribal personnel with security clearances under a series of amendments to the Homeland Security Act of 2002.[262] The majority of the clearances that DHS grants to these personnel is at the Secret level. Upon reviewing "specific mission requirements and compelling-need criteria," however, the DHS Chief Security Officer has the authority to grant Top Secret clearances and access to Sensitive Compartmentalized Information (SCI) to personnel at the state and local levels.[263]

From 9/11 to April 2004, the FBI granted 835 Top Secret Clearances and 2,021 Secret Clearances to state and local law enforcement officers.[264] Three years later, the GAO reported that in FY 2007, the FBI had provided 520 security clearances, mostly at the Top Secret level, to state and local fusion center personnel between October 2006 and April 2007.[265] In 2005, DHS had granted 325 security clearances to state and local level personnel.[266] In 2007, that number increased to 1,291.[267]

As in the Case of Security Clearances for Federal Personnel, the Increase in the Number of Clearances at the State and Local Levels Also Presents a Security Challenge. While it is necessary that LEAs have the clearances required to carry out their counter-terrorism responsibilities, there is also a need for increased safeguards to protect against the insider threat of unauthorized disclosure.

---

[260] Government Accountability Office, *Security Clearances: FBI has Enhanced Its Process for State and Local Law Enforcement Officials* (Washington, DC, 2004), 7, http://www.gao.gov/assets/250/242182.pdf.
[261] *Ibid*., 8.
[262] Department of Homeland Security, *DHS Instruction Handbook 121-01-007 the Department of Homeland Security Personnel Suitability and Security Program* (Washington, DC, 2009), 6, http://www.dhs.gov/xlibrary/assets/foia/instruction-121-01-007-personnel-suitability-and-security-program.pdf.
[263] *Ibid*., 4.
[264] Government Accountability Office, *Homeland Security: Federal Efforts Are Helping to Alleviate Some Challenges Encountered by State and Local Information Fusion Centers* (Washington, DC, 2007), 27, http://www.gao.gov/new.items/d0835.pdf.
[265] Shawn Reese, *State and Local Homeland Security: Unresolved Issues for the 109th Congress* (Washington, DC: Congressional Research Service, 2005), 11, http://www.au.af.mil/au/awc/awcgate/crs/rl32941.pdf.
[266] Government Accountability Office, *Homeland Security: Federal Efforts Are Helping to Alleviate Some Challenges Encountered by State and Local Information Fusion Centers* (Washington, DC, 2007), 27, http://www.gao.gov/new.items/d0835.pdf
[267] *Ibid*.

Federal Information Security Act FISMA (2002)

The Federal Information Security Act of 2002 (FISMA) is a Section of the E-Government Act of 2002. FISMA requires federal agencies "to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, modification or destruction…"[268] FISMA provides an important framework for safeguarding federal information and information systems.

FISMA promotes information security that is based on risk assessments, cost effectiveness, and oversight. FISMA, however, is agency-oriented. It lacks specific guidance for inter-agency efforts. Therefore, it is insufficient to ensure the underlying security of inter-agency information sharing efforts. While designers of information sharing architectures will benefit from the risk management and oversight concepts outlined in FISMA, there is a need for information security guidance that is more tailored to meet the unique needs of the ISE.

Risk Assessment and Management in Information Sharing

The Guiding Principles of the 1994 Joint Security Commission (JSC) Report is Still Highly Relevant Today. The JSC report asserted that there was a need in the IC to "provide a rational, cost-effective, and enduring framework using risk management as the underlying basis for security decision making."[269] The IC's information sharing policy, outlined in Intelligence Community Directive ICD Number 501, is based on a risk management approach.

Throughout the IC, the individuals who have collected data act as stewards, making individualized risk assessments to determine whether a piece of data can be shared with a requesting ISE partner. These determinations are made by weighing "the risks associated with providing the content of information collected or analysis produced against the risks associated with denying the request."[270] Elaborating on the nature of these two distinct types of risks, ICD 501 states:

> "a. Risks associated with providing information include, but are not limited to: risks to sources, methods, and activities; and risks of unauthorized or unintentional disclosure. b. Risks associated with denying a request for information include, but are not limited to: risks to mission performance; and risks of incomplete or erroneous analytic judgments informing policy or other decisions." [271]
>
> *Intelligence Community Directive Number 501*, January 2009

[268] E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2947 (2002).
[269] Joint Security Commission, *Redefining Security: A Report to the Secretary of Defense and the Director of Central Intelligence* (Washington, DC, 1994), executive summary, http://www.fas.org/sgp/library/jsc/index.html.
[270] Office of the Director of National Intelligence, *Intelligence Community Directive Number 501: Discovery and Dissemination or Retrieval of Information within the Intelligence Community.*
[271] *Ibid*.

The revelation of sources and methods has profound security consequences that should not be overlooked. Even when intelligence is used to make national security related operational decisions, sources and methods are inherently revealed in some capacity that impacts future collection ability. For example, in 1986 President Reagan decided to wage an aerial bombing campaign against Libya in Operation El Dorado as retaliation for a Libyan terrorist attack in West Berlin. This action revealed U.S. intelligence sources and methods in East Germany, which connected the Libyans to the attack.

Despite the utilization of this intelligence for operational ends, the revelation of U.S. sources and methods compromised future U.S. intelligence capabilities and inhibited the U.S. from being able to foil future Libyan plots in Europe. This example illustrates the critical importance of securing intelligence. It also demonstrates the delicateness involved in balancing the risks derived from both the revelation of sources and methods, and the denial of access.

While the concept of risk assessment outlined in ICD 501 is a necessary and important component of the IC's information sharing policy, it is also incomplete. Risk assessment is a multi-prong process that requires standardized training and discipline. Although the importance intuitive, individual judgment on the analyst level must not be diminished, there is also a need for a more robust standardized risk management framework and training across the IC.

The 1994 Joint Security Commission report outlined security risk as process involving a five-step procedure:

1. Asset valuation and judgment about consequence of loss.
2. Identification and characterization of the threats to specific assets.
3. Identification and characterization of the vulnerability of specific assets.
4. Identification of countermeasures, costs, and tradeoffs.
5. Risk assessment.[272]

The five-step procedure outlined above requires a level of discipline that is easily obscured by less thorough risk management directives. Currently, across the IC stewards are making information sharing decisions based on evasive risk assessment instructions. Although, the basic methodology is the same, one steward's standards for making an information sharing decision can be drastically different from another's. The space created for such divergences hinders information sharing, weakens security, and endangers national security. It also reduces trust within the IC, a vital component of information sharing. Therefore, there is a need for a degree of standardized training throughout the IC that educates data stewards to a basic criterion.

[272] Joint Security Commission, *Redefining Security: A Report to the Secretary of Defense and the Director of Central Intelligence.*

"Authorized Use" of Classified and Sensitive Data – Updating the "Need-to-Know"

The Concept of "Authorized Use" Provides a New Operational Paradigm for the Intelligence Community. At its most basic level, "authorized use" is predicated first on the ability to ensure that shared information can only be accessed by people with a legitimate need for that information. Second, it hinges upon defining the missions and roles of the people accessing shared information to determine legitimate use, and provides a new framework for working with information of a sensitive legal nature, such as information collected on U.S. persons or for a primary purpose uninvolved with counter-terrorism.

"Authorized use", rather than emphasizing "information sharing," a semantic trope largely unwelcomed by the IC, updates "need-to-know" for the technology-driven, modern era and incorporates the key principles underlying the "need-to-share," including a significant exchange of information among U.S. agencies. Under the principle of "authorized use," access to information is still limited by a "need-to-know," but better standards are in place for determining legitimate use and fostering access to information according to authorization.

The most critical aspect of authorizing users to access information includes their ability to handle information of a sensitive legal nature without the amalgamated, complex operational policies restricting access to this information currently. With the Supreme Court still addressing legal issues surrounding the collection of information on U.S. persons—dubbed the "Jane Fonda problem" during the Vietnam War era—use of domestic intelligence remains inconsistent. As a result, many IC professionals avoid U.S. person data because of the legal implications it carries. Similarly, confusion regarding the secondary use of data persists within the IC. Some examples of this include the use of cell phone location data to pinpoint an individual's location and the utilization of IP addresses to identify computer users.

The idea of "authorized use" is predicated on the ability to narrowly define the core mission of the receiving office or individual, as a general mission such as "counter-terrorism" or "national security" is too broad to warrant access to specific information.[273] Rather, a mission such as "tracing the flow of terrorist financing through the international banking system" or "examining the role of North Korea in the proliferation of nuclear weapons technology" are examples suggested for meriting an authorization designed to override data restriction.[274]

Defining Specific Missions and Designated Roles Creates the Opportunity for Determining What Type of Information is Necessary to Whom and at Which Agency. Additionally, "authorized use" also works as a vehicle for promoting trust among users working on similar issues at different agencies, as users must declare their purpose for accessing

[273] *Hearing on Information Sharing in the Era of WikiLeaks: Balancing Security and Collaboration,* Before the Senate Comm. on Homeland Security and Governmental Affairs, 112th Cong. (2011) (statement on Behalf of the Markle Task Force on National Security in the Information Age).
[274] *Ibid.*

information as well as their intended use for it.[275] An analyst sharing critical information within his or her organization's designated mission can rest assured that the system will deliver the information to other analysts working under similar missions, limiting the possibility of misuse or misinterpretation by other users in other agencies.

While mission definition is critical to "authorized use," the idea has been met with significant skepticism regarding its practical implementation. Given the globalized nature of counter-terrorism work and the interconnectedness of world affairs, the difficulty of determining access to specific areas of information encourages an imbalance between over or under-restricting information. Additionally, the level of granularity necessary to categorize and tag data, directing user authorization, has never been achieved in an enduring fashion on a multi-agency level. Rather, the sovereignty of each department handling information has overridden any widespread norms or practices regarding information sharing.

Insider Threats to Information Security

The Main Challenge to Fostering an Atmosphere of Trust Within an Information-sharing Environment Involves the Threat Posed by Authorized Users Themselves. In 1994, the Joint Security Commission (JSC) reported that "over the past 20 years the most damage to national security has been caused by individuals who are already cleared but who choose to sell classified information to foreign governments or to give it."[276] High-profile espionage cases such as Walker, Pollard, Ames, and Hiss serve as cautionary illustrations of agencies' vulnerability to their own employees.

The revelation of these double agents sparked an awareness for the necessity of stronger internal auditing policies, with the JSC recommending the creation of employee assistance programs to help guarantee that personnel do not become CI risks after they obtain a clearance, and also to provide better education and training for supervisors and coworkers to help them identify potential problems.[277] As a result of the JSC's findings, Executive Order 12968 of 1995, establishes stringent periodic reinvestigation standards for cleared personnel.

CI has been a critical component of most U.S. agencies' operational practices, with mixed results, but insider threat will continue to be a stumbling block for fostering greater trust among the IC until standardized policies are in place regarding thorough CI monitoring. Information sharing will suffer if agencies do not trust that a partner has proper procedures in place to identify and mitigate insider threat. The CIA and FBI have "robust" insider threat programs to identify suspicious user behavior, and the NGA, NSA, and NRO are following suit through recent enhancements to their audit and insider threat capabilities. Nonetheless, other agencies lag behind.[278]

---

[275] *Ibid*.
[276] *Hearing on Joint Security Commission,* Before the Senate Select Comm. on Intelligence, 103rd Cong. 933 (1994), http://www.intelligence.senate.gov/pdfs103rd/103933.pdf.
[277] *Ibid.*
[278] *Hearing on Information Sharing in the Era of WikiLeaks: Balancing Security and Collaboration,* Before the Senate Comm. on Homeland Security and Governmental Affairs, 112th Cong. (2011).

A Focus on Common Operational Practices Regarding Insider Threat Not Only Augments General Security, it Also Facilitates Cohesion and Cooperation Among Agencies. One example of a critical operating practice involves the use of audit logs to ensure the legitimacy of employee access to information. The *Wikileaks* disclosures to an Internet web site provides a general example of the importance of risk management regarding insider threat, but more significantly, a strong case for the use of monitoring and auditing procedures to determine anomalous behavior in accessing information. Ultimately, an auditing system was adopted by the State Department that included an automated function for determining anomalies that was paired with staff dedicated to analyzing these abnormalities.[279]

Capability and Intent in Risk Management

Measuring Capability and Intent is Necessary in a Risk Management System. The fundamental basis of risk management regarding threat assessment involves evaluating first the capability of the questioned asset, such as what information they can access, and second their intent, or what objectives an employee holds regarding use of information. The goal of counter-intelligence (CI) has always been to determine these internal threats, yet no government-wide standard exists across the agencies handling sensitive, and valuable information. Additionally, a common CI characteristic among the agencies involves an over reliance on polygraphs to root out underlying behavioral issues that could contribute to "mal-intent" in the future.

While polygraphs do serve a significant purpose in the clearance process, they cannot be trusted as the definitive standard for CI. A 1997 survey of 412 psychologists revealed they estimated the average validity of polygraph testing at about 61%, because the physical responses evaluated by the test are more indicative of guilt than lying.[280] For this reason, people with a low ethical threshold can pass a polygraph test repeatedly due to a critical lack of guilt regarding unethical behavior. This explains how individuals such as Aldrich Ames passed multiple polygraph tests while working as an active double agent in the CIA.

Double agents—an insider threat—are an inevitable aspect of intelligence work, and while polygraphs constitute a helpful step in building formative lifestyle assessments, they cannot be viewed as the ultimate authority on employee risk evaluations. Additionally, inescapable changes in life, such as a sick family member or unexpected financial loss, can turn an already-cleared employee into a compromised opportunist, utilizing information for financial gain to mitigate the new circumstances challenging their established standard of living.

"Authorized use" facilitates greater control over monitoring both the capability and intent of employees, as management can track both the information being accessed and also its use by the employee. Capability is predetermined through mission definition, as the information accessible to an analyst will hinge upon its relation to their covered issue. Additionally, anyone seeking access to additional information has to state their intention regarding its use.

---

[279] *Ibid.*

[280] Dan Vergano, "Telling the Truth about Lie Detectors," *USA Today*, September 9, 2009, http://www.usatoday.com/news/nation/2002-09-09-lie_x.htm.

The most important aspect of "authorized use" involves the use of audit logs and monitoring for abnormal behavior within the system itself, as this provides a more definitive picture of both capability and intent: what information is being accessed and whether it is appropriate given the role/mission of the employee. This is critical for effective CI and would prevent future iterations of double agents such as Hiss and Ames from long-term effectiveness and damage to U.S. intelligence goals.

Examining System Failures

System Failures Must Also be Addressed From a CI Perspective. Many note that the massive, unauthorized disclosure of classified data to the *Wikileaks* web site does not inherently represent a problem with information sharing as a concept, but rather a security and CI issue within an information sharing context. In fact, *Wikileaks* constituted a necessary wakeup call within the ISE. It provides a prime example of the importance of implementing the key aspects of "authorized use" and technology based CI initiatives, such as mission-based access to sources of information and automated audit logs. Were these systems in place, PCF Bradley Manning first would not have had widely unrestricted access to the vast repository of information available on the State Department's Net Centric Diplomacy (NCD) database, which he was able to access through SIPRNET, and second would have triggered automated alarms when he began downloading 1.6 gigabytes of classified data.[281]

Although the IC can be lauded for continuing information-sharing efforts despite *WikiLeaks*, the incident also highlighted the widespread shortcomings of governmental agencies in implementing policies such as audit logs to protect classified information from an insider threat. *WikiLeaks* also displayed the importance of creating common operational policies to ensure that agencies have an effective method for addressing insider threat and, as a result of these universal policies, which will ultimately advance a culture of trust among them.

[281] *Hearing on Information Sharing in the Era of WikiLeaks: Balancing Security and Collaboration,* Before the Senate Comm. on Homeland Security and Governmental Affairs, 112th Cong. (2011).

[This page is intentionally left blank]

Architecture for Information Sharing

Alternative Information Sharing Models

Creating a Comprehensive Information Sharing Environment. The Intelligence Community's inability to efficiently share critical pieces of information with other member agencies was illuminated in the tragic 9/11 attacks. The attacks highlighted various failures by federal agencies to effectively collaborate in order to fully recognize and ultimately thwart threats to the nation's security. Furthermore, 9/11 underscored a greater need for information sharing among agencies throughout the intelligence community.

Current efforts to move towards a comprehensive information sharing environment (ISE) involve linking law enforcement, public safety, homeland security, foreign affairs, defense, and intelligence communities at the federal, state, local and tribal levels. While these efforts constitute a step in the right direction, they must be accelerated in order to achieve an optimal level of integration. An environment of increased information sharing greatly helps to ensure the U.S.' security by collaboratively working to prevent tragedies such as the 2001 attacks from taking place in the future.

Departing from a culture that mandates a "need-to-know" philosophy and embracing recent calls for a "responsibility to provide" and "need-to-share" are imperative for the United States' current and future success in its counter-terrorism efforts. Fusion centers, designed to consolidate and analyze information, provide unique tools to facilitate these efforts and help to prevent future failures.[282]

Fusion centers exist at the federal, state and local levels and are chiefly organized in two models – a centralized model and a decentralized model. The National Counterterrorism Center (NCTC), serving as the nation's primary fusion center for all terrorism-related information, is considered a centralized model at the federal level. Conversely, the El Paso Intelligence Center (EPIC) is part of the national network of fusion centers and is considered a participatory member of the decentralized model.

Centralized Models for Information Sharing

Centralized models offer a structure for information sharing with unique advantages and challenges. Within a centralized architecture, participating agencies send their data to a central repository where it is organized and stored; users are then able to create queries and submit a request for information based on their specific need. The central repository fields these queries and directs them to the appropriate agencies.[283] To be effective, the centralized database must be both populated and updated frequently, data must be

[282] Eben Kaplan, "Fusion Centers," *Council on Foreign Relations*, February 27, 2007, http://www.cfr.org/intelligence/fusion-centers/p12689.

[283] Department of Homeland Security Data Privacy and Integrity Advisory Committee Chair Richard Purcell to Secretary Janet Napolitano and Chief Privacy Officer Mary Ellen Callahan, Report No. 2011-01, Privacy Policy and Technology Recommendations for a Federated Information-Sharing System, 31 January 2012, Department of Homeland Security, 7, 10.

submitted and catalogued in a standardized format, and an audit log must be maintained to monitor users' activity and the types of queries they conduct.[284] Arguably the easiest prototype of information sharing to implement, centralized models have significant benefits and shortcomings, discussed as follows:

Current Advantages of a Centralized Model

The Benefits of a Centralized Model. The centralized model holds numerous advantages for increased information sharing, and is capable of identifying and rectifying some of the major impediments to intelligence sharing. The benefits are outlined below:

Centralized Models Facilitate Discoverability. The core advantage of a centralized model is the central database contains information from a number of participating agencies. Having information submitted, organized, and stored in a centralized location, allows users to search for information from various agencies more easily. This centralized search capability for multiple agencies allows for greater discoverability.

Centralized Models Address "Stovepiping." A centralized model creates an authority capable of addressing sharing issues among contributing agencies and partners. The agency that manages the centralized data repository has the authority to grant specific users access to needed data, regardless of what their original data owners impose as particularly prohibitive restrictions on sharing their data. In this vein, a centralized model can help to reduce a user's unawareness of pertinent data by assessing the potential value of a given database and granting that user access accordingly.

Centralized Models Foster Collaboration. A centralized model fosters greater collaboration in that the central repository more efficiently links users who submit queries to agencies that possess such information. In this respect, users who may not have ordinarily collaborated with an agency before now have the potential to do so (more easily) based on their shared interest in related information.

Centralized Models Are More Cost Effective. A centralized model can be more cost effective than alternative approaches as they may reduce the potential for added costs often associated with the need for multiple hardware and software systems, additional space, personnel and databases (typical of decentralized models).[285] In a decentralized model, each agency has hardware and software unique to their needs. In order to share information with other member agencies, they have to acquire hardware and software to make the systems compatible. In a centralized model, each agency has hardware and software that easily facilitates the exchange between all agencies by having hardware and software compatible with the central repository.

---

[284] *Ibid*. Department of Justice, *Applying Security Practices to Justice Information Sharing: The Centralized Information Repository Model* (Washington DC, May 2007), http://it.ojp.gov/documents/asp/models/section3.html. Newton Howard and Sergey Kanareykin, *Analysis of Federated and Centralized Information Sharing Architectures* (Washington, DC: Center for Advanced Defense Studies, 2007), 3.

[285] United Nations Food and Agricultural Organization, *Improving Agricultural Extension: A Reference Manual* (New York, NY, 1998), http://www.fao.org/docrep/W5830E/W5830E00.html.

Centralized Models Remove Operational Inefficiencies. A centralized model has the ability to singularly define and execute any required updates in policy or structure.[286] The agency that manages the repository has the unique ability to define all of the security policies, requirements and practices for information access and use; this will also ensure that users can practically implement them in an effort to enforce security policy and to safeguard the integrity and availability of information.[287] In doing so, it largely helps to alleviate the issue of dealing with each participating agencies' respective policies. Additionally, it ensures that all participating agencies are subject to the same stringent requirements to access the central repository. This helps to assure that those authorized to access the information are allowed to, while still helping to maintain the security of the system.

Centralized Models Are More Secure. Not only is it easier for a centralized model to account for the integrity of data, with the right precautions, the probability that malevolent individuals can gain access to the database is reduced.[288] A centralized model, as compared to a decentralized model, provides fewer potential points in which an external threat can access the system. In a decentralized model, each agency becomes a link in the chain for information sharing. With every link–every potential point of entry–the system becomes more susceptible to the potential harm posed by external threats. This threatens the system's security by making it more vulnerable, in turn, providing a greater probability in which the system can be compromised.

Current Disadvantages of a Centralized Model

Weighing the Pros and Cons. In spite of the numerous advantages of the centralized model, there are several important disadvantages, outlined below:

Centralized Models Exacerbate Issues Regarding Data Legality. One of the core disadvantages regarding building a centralized database of information involves exacerbating the legal questions surrounding utilization of data. Issues such as secondary use are only magnified when wholesale pieces of data or entire databases are moved to reside in a central location. This creates the difficulty of guaranteeing such information continues to serve its primary purpose of collection. For this reason, integration of key stakeholders' information outside the IC is challenging for centralized models.

Centralized Models Create Greater Security Threats. Creating a central database capable of accessing broad swaths of information also creates a prime central target for malicious intent. While comprehensive security functions can be built into a centralized model, if an internal or external threat were to successfully compromise or breach the system's security, the intruder's increased ability to access information exponentially magnifies the threat to the IC community and greater national security.[289]

---

[286] Howard and Kanareykin, "Analysis of Federated and Centralized Information Sharing Architectures," 3.
[287] Department of Justice, *Applying Security Practices to Justice Information Sharing: The Centralized Information Repository Model.*
[288] Howard and Kanareykin, "Analysis of Federated and Centralized Information Sharing Architectures," 3.
[289] *Ibid*.

Centralized Models Discourages Agency Autonomy. In a centralized model, the agency that manages the repository controls the access to and distribution of the data it receives. As such, issues of autonomy are more difficult to reconcile as users partly lose ownership of their data.[290] Moreover, such power may enable a centralized model to lose and/or change its intended focus. If the agency that manages the data sees its primary purpose as facilitating information sharing at all costs, it may grant access in circumstances in which access is inappropriate. Conversely, the agency that manages the data believes its primary purpose is to prevent inappropriate access, it may deny access when access is appropriate and potentially valuable.[291]

Centralized Models Can Unintentionally Mandate Technical Changes. Centralized models require users submitting information to a centralized repository to conform to the way in which their central database is structured and the manner in which it operates.[292] As such, in some instances this may require users to acquire new tools, which allow them to adhere to the changes more easily. This process can create cumbersome technical requirements for agencies unprepared to restructure their IT systems or data formats.

Centralized Models Eliminate Necessary Context. A centralized model lacks the ability to provide an adequate context for the data it receives. While key facts are made available for users to search, an initial context that should add to the understanding of the data is lost. Centralized models would have less information about the limitations associated with particular data (and database). Moreover, they would have markedly less information about the initial intended uses of the data than the user.[293]

Centralized Models Potentially Detrimental to User Morale. A centralized model has the risk of partly demoralizing its users by decreasing their overall motivation and/or satisfaction. This decrease in motivation and/or satisfaction can stem from a user's feeling that:

1. They are less involved in/held less responsible throughout the (information sharing) process.

2. The centralized system may not be well customized to fit their specific needs.

3. They may receive a slower response time in routine operations and/or requests for needed changes within a centralized model.[294] Such effects could adversely affect a user's ability to productively contribute to the larger counter-terrorism effort.

Centralized Models Can Suffer Information Overload. Centralized models are inundated with data and risk a higher likelihood of being overwhelmed by volumes of information. As a result, it becomes harder for a centralized model to detect unnecessary and potentially

---

[290] *Ibid*.
[291] Department of Homeland Security Data Privacy and Integrity Advisory Committee Chair Richard Purcell to Secretary Janet Napolitano and Chief Privacy Officer Mary Ellen Callahan, Report No. 2011-01.
[292] Howard and Kanareykin, "Analysis of Federated and Centralized Information Sharing Architectures," 3.
[293] Department of Homeland Security Data Privacy and Integrity Advisory Committee Chair Richard Purcell to Secretary Janet Napolitano and Chief Privacy Officer Mary Ellen Callahan, Report No. 2011-01.
[294]United Nations Food and Agricultural Organization, *Improving Agricultural Extension: A Reference Manual.*

false information. Moreover, as information is moved from one agency to the central repository, elements of security, privacy and trust may become harder to implement and more difficult to guarantee.[295]

Example of a Centralized Model: The National Counterterrorism Center

A Centralized Approach to Protect the Homeland. Established in August 2004 by Presidential Executive Order 13354, the National Counterterrorism Center (NCTC) was established to "lead our nation's efforts to combat terrorism at home and abroad by analyzing the threat, sharing that information with our partners, and integrating all instruments of national power to ensure the unity of effort." The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 tasked the NCTC with the responsibility "to ensure the agencies, as appropriate, have access to and receive all-source intelligence products needed to execute their counter-terrorism plans or perform independent, alternative analysis" and "to ensure that such agencies have access to and receive intelligence needed to accomplish their assigned activities."[296]

Under the auspices of the Office of the Director for National Intelligence (ODNI), more than 500 personnel from more than 16 departments and agencies staff the NCTC. The NCTC maintains a partnership with the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), the Departments of Justice (DOJ), State (DOS), Defense (DOD), Homeland Security (DHS), Energy (DOE), Treasury (DOT), Agriculture (DOA), Transportation (DOT) and Health and Human Services (HHS), the National Geospatial-Intelligence Agency (NGA), the Nuclear Regulatory Commission (NRC) and the U.S. Capitol Police (USCP) among other departments and agencies to safeguard the nation's security.[297]

The NCTC serves as a central and shared knowledge bank on known and suspected terrorist and international terror groups, and fosters intelligence sharing throughout the intelligence and other notable communities. It does so, in part, by sharing detailed lists of terrorists, terrorists groups and worldwide terrorist incidents in the Worldwide Incidents Tracking System (WITS), the Terrorist Identities Datamart Environment (TIDE), and the annual reports on terrorism. The NCTC uses this information to analyze terrorism-oriented intelligence and write assessments and briefings for senior officials and policymakers.[298]

In supporting responses to terrorist incidents domestically and internationally, the NCTC plans counter-terrorism activities as directed by the President of the United States, the National Security Council, and the Homeland Security Council.[299] It also chairs interagency meetings and video teleconferences on terrorist groups, their capabilities, plans and intentions, and emerging threats to the United States' interests at home and abroad. Among its several other responsibilities, the NCTC also manages a Joint Operations Center

---

[295] Scott Shumacher, "How to Preserve Security and Autonomy While Meeting Information-Sharing Directives," *ISACA Journal* 6 (2009), 1.
[296] National Counterterrorism Center, *NCTC and Information Sharing: Five Years Since 9/11: A Progress Report,* (Washington, DC, 2006), 10, http://www.nctc.gov/docs/report_card_final.pdf.
[297] "Key Partners," National Counterterrorism Center, http://nctc.gov/about_us/key_partners.html.
[298] *Ibid.*
[299] "What We Do," National Counterterrorism Center, http://www.nctc.gov/about_us/what_we_do.html.

to provide unique insight and situational awareness of developing terrorism related worldwide issues and events.[300]

The NCTC faces several challenges while supporting counter-terrorism efforts. In its self-assessment "CTC and Information Sharing: Five Years Since 9/11: A Progress Report" the NCTC highlighted the following issues as challenges it still faces today:

1. Recognizing and designating "terrorism" information.

2. Protecting operationally sensitive information.

3. Ensuring that constitutional rights of individuals are not violated through information sharing practices.

4. Clarifying roles, responsibilities and information needs of the members of the counter-terrorism community.

5. Developing a considered approach to information sharing across federal, state, and local levels amidst an increasing number of networks and databases.

The NCTC continues to examine capabilities that will better allow it to integrate and assimilate the large volumes of terrorism information it receives.[301]

Despite these challenges, the NCTC has succeeded in creating a central location in which analysts from agencies throughout the intelligence community can convene. At the NCTC, these analysts have access to a host of networks and information systems spanning the intelligence, law enforcement, military, and homeland security communities. Through these networks and systems, analysts have access to foreign and domestic information pertaining to international terrorism and sensitive operation and law enforcement activities.[302] This access places the United States in a better position to counter terrorist threats.

As noted in previous sections, the NCTC holds counter-terrorism communitywide secure video teleconferences (SVTCs) thrice daily to ensure general awareness of ongoing operations and newly detected threats. These conferences allow participants to compare findings, highlight new threats and debunk erroneous threats.[303]

NCTC Online (NOL) and the NCTC Online CURRENT are classified NCTC repositories. These two sites make counter-terrorism products and articles available to users in federal agencies, departments, military services and major commands throughout the U.S. Government. The NCTC's Interagency Threat Assessment and Coordination Group (ITACG) facilitates information sharing between the intelligence community and state, local, tribal

[300] "How and Why We Do It," National Counterterrorism Center, http://nctc.gov/about_us/how_we_do.html.
[301] National Counterterrorism Center, *NCTC and Information Sharing: Five Years Since 9/11: A Progress Report,* 10.
[302] *Ibid.*
[303] *Ibid.*

and private partners in coordination with the Department of Homeland Security, the Federal Bureau of Investigation and other ITACG Advisory Council members. The NCTC successfully assists the ODNI Homeland Threat Task Force coordinates interagency collaboration and update senior policymakers about threats to homeland security weekly.[304]

While the NCTC is successful in many regards, it still faces major criticisms, such as the 2009 statement that NCTC had failed to heed warnings signs suggesting that Umar Farouk Abdulmutallab (the so-called "underwear bomber") was a threat to the United States, and may have harbored intentions to explode a commercial flight bound for Detroit, Michigan on December 25, 2009.[305] President Obama remarked, "this failure was not a failure to collect intelligence; it was a failure to integrate and understand the intelligence that we already had."[306]

While several within the intelligence community espouse that terrorist attacks succeed because of a lack of information sharing, the President's remarks suggest the greater issue is an inability to integrate and understand existing intelligence. Such sentiments feed into the existing culture that there is an increasing failure to "connect the dots." NCTC and CIA personnel who were responsible for watch-listing "did not search all available databases to uncover additional derogatory information that could have been correlated with Mr. Abdulmuttab."[307] As such, while it is crucial for the NCTC to facilitate information sharing, it is just as crucial that the NCTC and its partner agencies utilize all of the resources that the NCTC affords them.

In the future, the NCTC and its partners, must continue to be mindful of the enduring difficulties in the following areas: privacy, access, sources and methods, operational impact, liaison information, source credibility, information technology, access to state, local, and tribal governments and the private sector and data acquisition.[308]

Decentralized Models for Information Sharing

Analyzing Strengths and Weakness. Decentralized models of information sharing provide a viable alternative to centralized models, as some of the core issues involved with the centralization of data and information are eschewed through alternative information-sharing and storage structures. With a decentralized architecture, participating agencies retain control of their own databases and share relevant pieces of information when deemed necessary and appropriate by each agency. Task forces or initiatives are formed when a prescient issue surfaces which requires integrated decision-making and action.

---

[304] "Key Partners," National Counterterrorism Center, http://nctc.gov/about_us/key_partners.html.
[305] Eric Schmitt, "Director of National Counterterrorism Center is Resigning," *New York Times*, June 9, 2011, http://www.nytimes.com/2011/06/10/us/politics/10leiter.html.
[306] Richard A. Best Jr., *The National Counterterrorism Center (NCTC) – Responsibilities and Potential Congressional Concerns* (Washington, DC: Congressional Research Service, 2011), http://www.fas.org/sgp/crs/intel/R41022.pdf.
[307] *Ibid.*
[308] National Counterterrorism Center, *NCTC and Information Sharing: Five Years Since 9/11: A Progress Report,* 10.

Partnerships across the state, local and tribal levels are encouraged, as all relevant stakeholders are encouraged to participate in meetings and initiatives.

The core goals of a decentralized model are to ensure collaboration among key intelligence partners and to foster an environment where contributing agencies are actively exchanging key pieces of intelligence. For this model to work effectively, true equality among partners is critical in the sharing relationship, as well as a shared responsibility for the final analytics product.

Current Advantages of a Decentralized Model

Assessing the Impact. As with the centralized model, there are numerous advantages to the decentralized model, as stated below:

Decentralized Models Lessen Legal Issues Regarding Data Usage. Decentralization of data helps with handling the legal issues involved with secondary use, as data needs to reside at the agency where it is collected and shouldn't be moved wholesale to a different location. Since information can be shared on a case-by-case basis, it will facilitate the proper channeling of information for secondary use. As such, it will not further exacerbate the current debate regarding transferring large chunks of data around for unrestricted use.

Decentralized Models Encourage Data Security. A decentralized model of information sharing allows for greater IT security as each agency retains their individual IT databases and storage. Creating an overarching database of information, the crux of a centralized model, creates a significant risk regarding data vulnerability because it establishes a significant target for cyber-terrorism or insider threats. Retaining multiple databases and data repositories prevents the relative ease of a malicious user gaining access to a broad swath of information by accessing one data system.

Decentralized Models Allow Agency Autonomy. Similarly, with this model each agency is allowed to continue its own maintenance of data networks, as well as handle their sources and information according to policy. While trust among shared partners is necessary, a decentralized approach to information sharing does not require trust in shared operational policies or technological security, as the agencies are not required to release sensitive information into a universal data repository accessible to multiple partners. Rather, agencies are allowed greater autonomy in determining what information to share, who can have access to the information, and how it is used collaboratively to promote U.S. national security.

Decentralized Models Use Existing Technical Structures. With a decentralized model, agencies are allowed to keep their own systems and databases, rather than changing their existing operational infrastructure to conform to the data requirements of a centralized system. This removes a cumbersome responsibility for agencies not capable of allocating resources toward a large-scale IT update, although it can complicate the IT automation preferred for information sharing if different syntax and semantics are utilized among sharing partners.

Decentralized Models Preserve Necessary Context. Since agencies are allowed operational autonomy, decentralized models preserve the necessary context required for disseminating and interpreting types of information. IC agencies naturally handle different types of information and have various policies in place for how information is handled and processed within their specific agency. For example, the Secret Service processes threats to presidential security, which vary dramatically in credibility. Allowing another agency to access and process these threats, without an understanding of the context with which the Secret Service determines the threat credibility, encourages faulty decision-making and unnecessary strain in the information sharing structure.

Decentralized Models Facilitate Positive Relationships Among Agencies. The individual initiatives and groups actively involved in information-sharing in a decentralized system of sharing engender trust among the contributing partners through facilitating familiarization of cross-agency counterparts. This familiarization breeds greater knowledge among attending agencies of who is accessing their information and how is it used in the overall sharing process. Encouraging personalized, networked relationships is a critical component to bridging existing cultural antipathy toward releasing critical information.

Current Disadvantages of a Decentralized Model

Potential Challenges of Decentralization. As outlined below, there are numerous obstacles that would have to be addressed with a decentralized model. They include the following:

Decentralized Models Stymie Discoverability. Without a single repository for information or connection among agency databases, a decentralized model lacks the infrastructure to facilitate information discoverability. Technological initiatives, such as metadata and tagging, are not adopted by multiple partners using a single database. Instead, multiple systems are utilized. This stymies efforts to universalize data mechanisms intended to facilitate discoverability across multiple partnering agencies.

Decentralized Models Allow "Stovepiping" to Persist. Without a central authority mandating which information should be shared, agencies can continue creating "stovepipes," or barriers to which information is shared and who is granted access to such information. Stovepipes are a key characteristic of moving from "need-to-know" to "need-to-share" with the ISE, and decentralized models' inability to address this issue places the models at a significant disadvantage.

Decentralized Models Are Less Cost Effective. Since each agency retains its own data systems, structures, and personnel, each agency is responsible for maintaining significant IT resources and costs. IT duplication among agencies and processes—in addition to the resulting expenditures—lead to higher intelligence community IT costs and increase overall Federal Government spending.

Decentralized Models Exacerbate Operational Inefficiencies. While agencies are allowed operational autonomy, this autonomy results in a cumbrous sharing system burdened with multiple operational processes and standards. This creates problems when handling information of a sensitive legal nature, such as data collected on U.S. persons, which each

agency has different standards for handling. These distinctive policies limit the functional use and movement of information, which are critical aspects of agency sharing.

Decentralized Models Do Not Ensure Widespread Information Integration. Decentralized models also allow missions and roles to go undefined among partners, which inhibits agency accountability for participation in information sharing. Cultural inertia already predisposes agencies against sharing information, and without a strong central authority monitoring agency involvement, sharing is easily neglected. Although these issues can be somewhat mitigated through special task forces and sharing initiatives, they fail to create the type of widespread information integration necessary for addressing national security threats in the modern century.

Examples of a Decentralized Model - The Fusion Centers

The Implementation and Success of Fusion Centers. Currently, fusion centers operate in each of the 50 states, with additional centers based in major urban areas. Although the actual number varies, there are currently 77 fusion centers located throughout the U.S.[309] Created following the attacks on 9/11, they provide an information-sharing mechanism responsible for ensuring the integration of federal, state, local, tribal, and territorial agencies in national counter-terrorism issues. DHS reports that fusion centers are responsible for "the receipt, analysis, gathering, and sharing of threat-related information, and have additional responsibilities related to the coordination of critical operational capabilities."[310]

While fusion centers are not federally controlled or mandated, they are considered "the highest priority for the allocation of available federal resources," in addition to funding from state and local resources.[311] In 2007, the National Strategy for Information Sharing (NSIS) established funding and interoperability guidelines for the Federal Government in supporting fusion centers, stating that the Federal Government better structure the allocation of its resources to ensure that funding "collectively supports the development of a national network of fusion centers; and effectively balances the need for supporting SLTT, as well as federal, imperatives."[312] The NSIS laid out guidelines prioritizing federal funding for fusion centers, with "primary" fusion centers receiving federal resources before "recognized" fusion centers. Required criteria for primary fusion centers interested in federal funding include the following:

1. Designation as the primary fusion center by the Governor.

2. Oversight and management by a state or local government agency.

---

[309] "Fusion Center Locations and Contact Information," Department of Homeland Security, last modified March 12, 2012, http://www.dhs.gov/files/programs/gc_1301685827335.shtm.
[310] *Ibid*.
[311] *Ibid*.
[312] Program Manager, Information Sharing Environment, *ISE-G-112: Information Sharing Environment Guidance (ISE-G) Federal Resource Allocation Criteria (RAC)* (Washington, DC, 2011), http://ise.gov/sites/default/files/RAC_final.pdf.

3. Receipt of DHS certification of privacy, civil rights, and civil liberties protections and are determined to be at least as comprehensive as the Information Sharing Environment (ISE) Privacy Guidelines.

4. Implementation plan and procedures to fulfill responsibility as the focal point within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information, and for the coordination and execution of the statewide fusion process, including all fusion centers and other SLTT partners in its state or territory.

5. Achievement and maintenance of the *Baseline Capabilities for State and Major Urban Area Fusion Center* (Baseline Capabilities), as measured by the annual Baseline Capabilities Assessment (BCA).[313]

Recognized fusion centers differ from primary fusion centers in their designation from the State Governor and implemented procedures, but otherwise are required to maintain the same privacy protections and baseline capabilities. They also can differ in types of information collected and analyzed. For example, New York supports six different fusion centers, with its primary fusion center, the New York State Intelligence Center (NYSIC) handling information regarding terrorist and criminal intelligence.[314] New York's five other fusion centers operate according to regional directives and missions, such as the NYPD Intelligence Division's fusion center covering counter-terrorism initiatives in NYC, and the Upstate New York Regional Intelligence Center (UNYRIC) handling criminal and drug intelligence for the Upstate areas.[315]

Fusion centers as a decentralized network of intelligence sharing face several key challenges. Firstly, overlapping regional jurisdictions and authorities hinders the effectiveness of the fusion center system, as each center needs clearly defined operational parameters to better address key issues. While information sharing occurs within each center, efforts need to be made to connect the centers when addressing regional issues. Secondly, despite the efforts of the NSIS to create a unilateral policy among the fusion centers regarding handling domestic intelligence, various fusion centers have been strongly criticized for violating the civil liberties of U.S. persons. Thirdly, fusion centers have access to information through various databases that provoke legal questions regarding secondary use issues. While fusion centers are an important part of information sharing at the SLTT levels, these issues need to be addressed to move toward a better system of sharing.

[313] *Ibid*.
[314] Dana Priest and William A. Arkin, "Top Secret America: A Hidden World, Growing Beyond Control," *Washington Post*, July 19, 2012, http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/.
[315] *Ibid*.

The Impact of Technology on Information Sharing

The Evolving Technological Landscape

An ever-evolving technological landscape has dually shaped the manner in which information can be shared and the way that information-sharing models have been structured. At a fundamental level, the information sharing environment (ISE) requires a secure, interoperable network to function successfully. System encryption greatly helps to ensure the security of the information sharing environment by helping to safeguard against the potential for external threats.

In the search to create the perfect information sharing environment, several notable system features have been highlighted. Many initiatives have highlighted discoverability, tagging, auditing, "authorized use" standard and anonymization as key features in strengthening the ISE's mission to provide analysts, operators, and investigators in the law enforcement, public safety, homeland security, intelligence, defense, and foreign affairs communities with needed integrated and synthesized information on weapons of mass destruction (WMD), homeland security, and terrorism, to enhance national security.[316]

Intelligence community directives such as ICD 501, highlighted earlier in "Where We are Now – A Decade After 9/11," recognize the importance of features such as "authorized use" and have called for the implementation of discoverability.[317] The ISE has stated "to make the ISE work, we need to focus on information–discovering it, sharing it, protecting it, fusing it and reusing it."[318]

[316] "What is ISE," Information Sharing Environment, http://ise.gov/what-ise.
[317] Office of the Director of National Intelligence, *Intelligence Community Directive Number 501: Discovery and Dissemination or Retrieval of Information within the Intelligence Community.*
[318] Program Manager, Information Sharing Environment, *ISE Annual Report to the Congress,* 6.

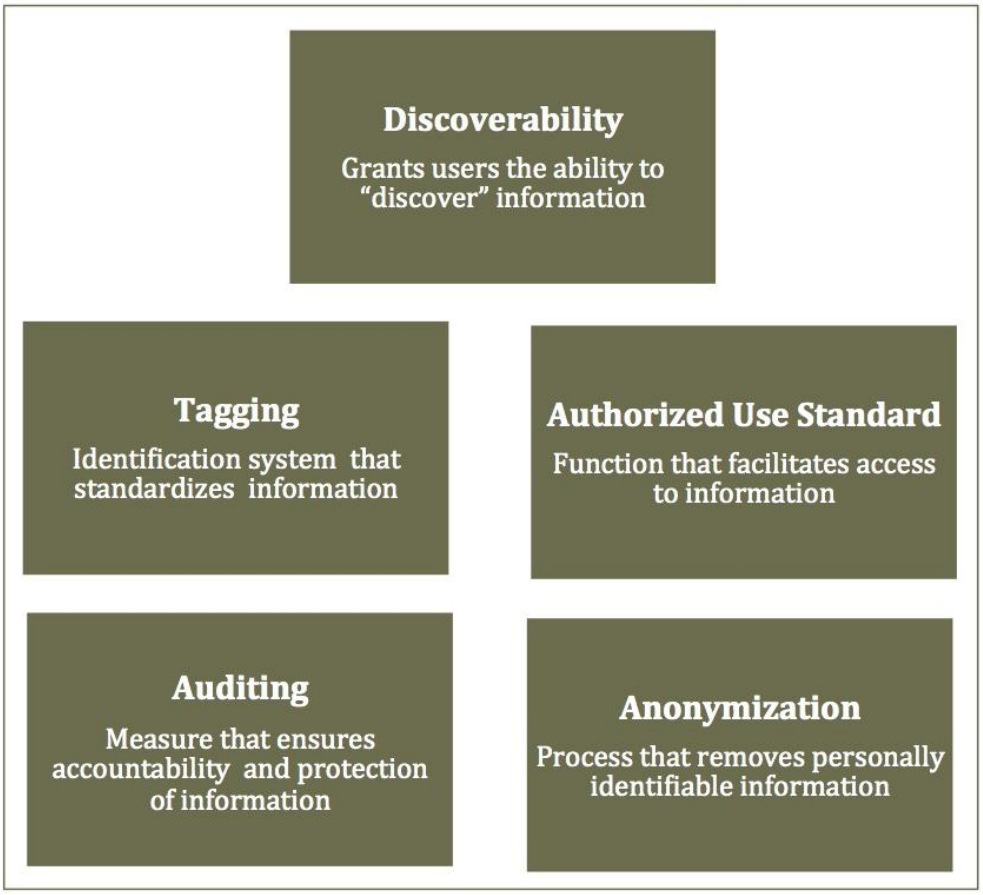

Figure 6.1: Technological Framework for Information Sharing

The Use of Discoverability

Discoverability Lets Users Uncover Information. Discoverability lets users discover information that exists in other agencies without actually providing the user the raw information, or intelligence.[319] Data would be tagged at the point of collection with standardized information (for example, a brief description answering the questions who, what, where and when) and then submitted into a central index. Users would have to make a request for access to the actual information. After receiving authorization and authentication, users would be given access to that information.

Discoverability is an essential preliminary step in strengthening collaborative efforts between agencies in hopes of increasing information sharing. While direct access to information is not immediately granted, permitting users the opportunity to learn what information other agencies possess is critical. This creates a secure foundation for effective information access and improved decision-making. It ultimately strengthens national security by providing government officials the ability to locate relevant information.[320]

[319] Office of the Director of National Intelligence, *Intelligence Community Directive Number 501: Discovery and Dissemination or Retrieval of Information within the Intelligence Community.*
[320] *Ibid.*

Discoverability would help improve cooperation and collaboration between agencies. A user's ability to discover, and potentially request access to information creates an opportunity for analysts working within different agencies on similar issues to connect with one another. As similar pieces of information are connected, related analyst and agencies that might be unaware of their connection or shared goals are similarly networked.[321]

Discoverability helps to improve privacy and security protection by ensuring that users can locate pertinent information. In turn, discoverability helps to reduce the bulk transfer of data required of traditional centralized databases.[322] This greatly improves security and minimizes privacy risks. In order to ensure its success, it is essential that agencies comply and contribute information that can be discovered.

Discoverability and Tagging

Tagging Standardizes Information. Tagging, which takes place at the point of collection, is the process of standardizing information before data is submitted to a central index. These indices point users to data holders and documents based on their search criteria. Tagging essentially provides users with basic yet crucial information, primarily an account of the individual(s) and/or group(s) involved in the reported incident and/or event (the "who"), a brief summary describing what took or will take place (the "what"), noted locations of interest (the "where") and when the incident and/or event occurred/will occur (the "when").[323]

Additionally tagging information with the date and time that it was received, informs users of the value of the information. Moreover, tagging information with a date and time helps to provide a context for which users can use the information. In addition, tagging data by date and time can greatly help to determine when information should be unclassified.

Tagging is an efficient and effective information identification system that helps to facilitate the exchange of information. It directs users to data holders and documents based on their search criteria. This is an important step in fostering greater cooperation between various agencies within the intelligence community. In order to ensure its success, it is essential that the information be tagged correctly and with pertinent information.

Regulating Use of Information Sharing Models

Auditing Ensures Accountability and Identifies Misuse. Auditing holds users accountable for their actions. To improve accountability, any attempts to access information in the system will be recorded. Regular automated compliance and behavior audits will identify all data users.[324] Any attempts to move beyond authorized access or use can be flagged, monitored

---

[321] *Ibid.*

[322] Markle Task Force on National Security in the Information Age, *Meeting the Threat of Terrorism: Improve Information Sharing, Create a Trusted System, Facilitate Access to Critical Data* (New York, NY: Markle Foundation, 2009), http://www.markle.org/sites/default/files/MTFBrief_Discoverability.pdf.

[323] David Bray, "Cross-Domain Information Sharing," *ISE Blog*, August 3, 2011, http://ise.gov/blog/david-bray/cross-domain-information-sharing.

[324] Program Manager, Information Sharing Environment, *ISE Annual Report to the Congress,* 76.

and ultimately investigated. Additionally, sharing the audit log findings with participating agencies ensures that they are knowledgeable of their users' activity while holding them accountable. The ability to monitor activity will help to reduce the potential for abuse and ensure the system's security to prevent incidents like the 2010 *WikiLeaks* scandal. Moreover, strengthening cyber security helps to better protect individual civil liberties and privacy.

An "authorized use" standard, as described at length in the "Authorized Use" section, encourages appropriate information sharing to improve national security by creating a consistent and clear standard that meets the challenges of the global communications revolution and emerging threats.[325] Authorized uses are mission or threat based permissions to access or share information for a particular, clearly identified purpose that the Government – with public scrutiny – has determined beforehand to be appropriate and lawful.[326]

This standard grants authorized users access to information based on how the information will be used rather than on where the information was collected or to whom it pertains. Access to information will ultimately be granted based upon agency mission, the role of individual officials and a predicated purpose.[327] In order to ensure its success, it is essential that the right individuals have permission to access and/or share information for a particular and appropriate mission.

Anonymization technology allows for the removal of personally identifiable information (PII).[328] The removal of personally identifiable information reduces the risk of its unintended disclosure.[329] Anonymization should prove particularly beneficial for initiatives such as the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) in which law enforcement agents at the state, local, and tribal levels (STL) observe individuals engaging in suspicious behaviors or receive reports of suspicious activity which may contain personally identifiable information.[330] In order to ensure its success, it is essential that all parties comply with policies regarding the removal of personally identifiable information in their intelligence reporting and are appropriately trained.

Effective Delivery of ISE Information

Efficiency in Utilizing New Tools. The Information Integration Sub-Committee (IISC) of the Information Sharing and Access Interagency Policy Committee (ISA IPC) coordinates high-priority interagency efforts to accelerate the delivery of the ISE information and support.

---

[325] Office of the Director of National Intelligence, *United States Intelligence Community Information Sharing Strategy* (Washington, DC, 2008), 5, http://www.dni.gov/reports/IC_Information_Sharing_Strategy.pdf. Office of the Director of National Intelligence, *Intelligence Community Directive Number 501: Discovery and Dissemination or Retrieval of Information within the Intelligence Community.*

[326] Program Manager, Information Sharing Environment, *ISE Annual Report to the Congress.*

[327] *Ibid.*

[328] Department of Justice, *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era* (Washington, DC, 2006), http://it.ojp.gov/documents/fusion_center_executive_summary.pdf.

[329] Program Manager, Information Sharing Environment, *Feasibility Report: Report for the Congress of the United States,* (Washington, DC, 2008), http://www.fas.org/irp/agency/ise/feasibility.pdf.

[330] Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI), *Nationwide SAR Initiative* (Washington, DC, 2012), http://nsi.ncirc.gov/documents/Nationwide_SAR_Initiative_Overview_2012.pdf.

One of the most important elements of their mission is to ensure that both federal and non-federal partners have the appropriate input and processes to satisfy their individual missions. Non-federal partners include all State, Local, Tribal and Private Sector (SLTPS) elements. These incorporate all 77 fusion centers and state and local law-enforcement agencies.

One of ISC's missions is the integration and interoperability of the Sensitive But Unclassified (SBU)/Controlled Unclassified Information (CUI) and Secret networks across departments in the SLTPS. Linking this information across a wide spectrum of agencies will ensure further collaboration by providing local enforcement with valuable data and help analysts to identify possible connections.

Incorporating local law enforcement into intelligence information sharing certainly has limits. State, local, tribal, and private sector entities are not subject to the same security screenings as federal agencies, and overcoming that inherent distrust is certainly a difficult task. Incorporating SLTPS into intelligence has, however, proved to be successful when examining the pre-cursor to the modern Fusion Center, EPIC (El Paso Intelligence Center).

EPIC is a true multi-agency center that remains heavily reliant upon a variety of other agencies for data, staffing and participation. No other agency in the United States provides this kind of real-time tactical support to the law enforcement community. The architecture of EPIC is based on a tiered-access system in which access to sensitive information is surveyed on a case-specific basis while maintaining immediate access to a much larger set of less sensitive information.

There has been significant satisfaction among federal, state, and local personnel with EPIC's products and services, especially in areas of timeliness, accuracy, relevance and immediate usability of its information-sharing portal. Gaining access to EPIC's least sensitive database is simple, and has proved invaluable for local law enforcement. This type of unclassified information does not jeopardize sources and methods, and can be an essential tool for non-federal entities. IISC's success in this process, however, has had varying results.

According to the 2011 ISE Annual Report, only 57% of responding ISE departments and agencies have developed (or are developing) interconnection plans for SBU/CUI networks supporting the ISE. Although this accounts for a 14% increase from 2010 there is certainly an opportunity for improvement. Notably however, only 36% of responding agencies identified that they have a plan for implementing interconnection capability for sharing terrorism and homeland security information across SBU/CUI network. Alarmingly, this accounts for a 21% decrease from 2010 and represents one of the few areas in information sharing that has declined. Any further regression in this area could have the undesired effect of minimizing intelligence collected at the non-federal level.

Further assimilation of SLTPS entities into the federal architecture will help to incorporate local and regional intelligence into the system. So long as this information is properly tagged and is discoverable in the database, it will only act to help the broader mission of securing the homeland. Federal architecture that supports an interconnection capability

for sharing terrorism and homeland security information across SBU/CUI is essential and needs expansion.

Current Concerns in Information Sharing

Debates Between Systems

Deciphering the Best Model. The 9/11 attacks have demonstrated that sharing information is essential for responding to current threats, and that having a comprehensive structure in place to facilitate cooperation is paramount. For the last ten years there has been considerable progress made on all fronts of information sharing, but the debate over how the information sharing architecture is engineered still rages. One can utilize either a centralized or a decentralized architecture, however each has its shortcomings. In several key areas, one system may be better suited to perform that task, but neither system is flawless. Both systems contain innate advantages and disadvantages.

Push/Pull

Centralized Systems Push Information. A centralized system facilitates pushing information by providing a mechanism for the redistribution of information. Any IT system used to facilitate information sharing has to address the dynamic tension between pushing and pulling information, but the advantage of the centralized system is that it allows for the redistribution of information across system partners. This is critical for the integration of data and efforts to address threats to national security.

Decentralized Systems Pull Information. A decentralized system pulls relevant information from its contributing partners on a specific issue or threat. This creates issues regarding the redistribution of information to partners as a monopoly of data holding is created. Additionally, targeting the right information within various databases and agencies is very difficult, as discoverability is hindered within the system.

Efficiency of Centralized Systems

Centralized Systems can Prove More Efficient and Effective than Decentralized Models. A centralized system almost ensures standardization of data and promotes uniform policies relating to requesting access of information. This model will allow the agency that manages the system to define the security policies, requirements and practices for information access and use. Additionally, since only one system is utilized, uniform training modules can be implemented to further awareness of policies and procedures.

Centralized systems limit the functional use of information. While agencies are allowed operational autonomy, this independence results in a cumbersome sharing system hampered without a standard policy and procedure. This critical characteristic limits the functional use of information, which is essential to information sharing.

Security of Centralized and Decentralized Systems

Centralized Models Typically Provide an Enhanced Level of Security. Standardized policies and procedures not only allow an efficient accounting of current and perishable data but also reduce the probability of malevolent individuals gaining access to the database. A centralized model facilitates a more straightforward counter-intelligence strategy by limiting the number of audit logs that need to be scrutinized. Additionally since only one central database is used, IT (which is instrumental for detecting malicious behavior) can be utilized without the need to spend a higher dollar amount on making it adaptable to multiple systems.

Although a centralized system typically is more secure than the decentralized model, if an internal or external threat breaches the system the consequences could be even worse than the *WikiLeaks* scandal. As such, a centralized system can become an attractive target for outside cyber agents. If data stewards do not trust the security of the system, then they will be unlikely to further share their information.

A Decentralized System's Security is Less Manageable. A decentralized system contains the same security concerns as a centralized system; however, it is not a prime target for cyber-terrorism and/or insider threat as is a centralized system. Additionally, agencies retain their own systems and databases, as such limiting the magnitude of any insider threat issue by removing their ability to access information across agencies. This compartmentalized system becomes much more manageable for CI departments to assess threats. The audits of entry logs become a lot less cumbersome and specific counter-intelligence IT for that agency can help to identify patterns that are agency-specific.

Discoverability/ Data Tagging

A Centralized Database Facilitates Discoverability and Tagging in a More Efficient Manner. Uniform data tagging procedures can be implemented to ensure consistency. This will assist the standardization of labels throughout the IC. As a consequence, discoverability will increase and the data can be used for its intended purpose.

A Decentralized Model Lacks the Ability to Facilitate Unproblematic Discoverability. Each system may contain its own IT for discoverability, which most likely would be incompatible with other agency or departmental systems. Decentralized systems may also have agency specific tagging, which could better coordinate that agency's information sharing. Therefore, this may prevent analysts in other agencies discovering what data is available for use.

Usefulness of Data

A Centralized System's Operating Agency has an Inordinate Amount of Influence over Authorizations and Procedure. As a large repository of information, the owner will unlikely be aware of its entirety, and thus may not be conscious of who should have authority to access what data. Additionally, they would have significantly less information about the intended use of the data than the owner would. The central agency may then become restrictive in granting access, or may grant access in instances when it is not required.

With a Decentralized Architecture, Agencies Retain Control of Their Own Database. This allows sharing of relevant pieces of information when deemed necessary and appropriate by individual agencies. As experts of their own data, they will be more knowledgeable of its intended use and what person/agency should have access to the information. Furthermore with this model, each agency is allowed to itself continue maintenance of its own data so that it can be easily updated, modified, or deleted.

Privacy

A Centralized System is Conducive to Secondary Use. This aspect is important to allow the distribution of data to other agencies, an imperative element for their mission. A centralized system, however, is not conducive to a system that provides robust protections for privacy and civil liberties. Understandably, certain personal information should not be shared with all intelligence agencies. Privacy concerns must be paramount, else third parties will no longer share with the Government and public trust in the system will be damaged.

A Decentralized System Facilitates a More Secure System. A decentralized model, although limiting in its accessibility for secondary use, is certainly a better system for protecting *privacy and civil liberties.* As data resides at the agency where it is collected, it can be shared on a case-by-case basis rather than being shared in large unspecified quantities. Additionally, each agency is then able to enact their own oversight and accountability policies, which is crucial protection against the misuse and abuse of information.

Information Sharing Initiatives

Incorporating the Two Models. Fusion Centers and the NCTC represent two distinct models, both with many advantages and some shortcomings. With both systems currently operational, the IC is able to extract the positives from each model and incorporate them into a future system. The new architecture however will attempt to be the overarching system that links all intelligence agencies and departments.

Although there is current debate over which system to implement, the system of the future will represent a hybrid model that incorporates aspects from both existing systems. It seems that “cloud computing” will hopefully help to resolve many of the shortcomings that currently plague current system.

System of the Future – Cloud Computing

Cloud Computing Delivers Services Over the Internet. There are essentially three different categories of services offered by cloud computing:

1. Infrastructure-as-a-Service (IaaS): Providers offer varying technical hardware.
2. Platform-as-a-Service (PaaS):Providers offer a computing platform, often an operating system, programming language, and a user interface.
3. Software-as-a-Service (SaaS): Providers offer software accessible to cloud users.

With cloud computing, users are no longer forced to purchase, set up, and maintain a set number of dedicated servers; the provider handles all server responsibilities, and the user only pays for what they are directly drawing from, with an automatic scalability function built-in to respond to fluctuating user needs. For this reason, the Federal Government is adopting cloud computing as a means of reducing IT costs.

Servers provide two main functions: storing data, and enabling computing power for operational platforms. A traditional network of servers provides an operational infrastructure for computers within its operating system; most agencies maintain their own servers as a means of connecting their computers to common databases and/or files. This also allows them to protect the physical security of their servers as they can control the environment of the servers and access to them. Accessing files stored on the server is limited by whether the computer in use has the physical infrastructure necessary to connect to the server.

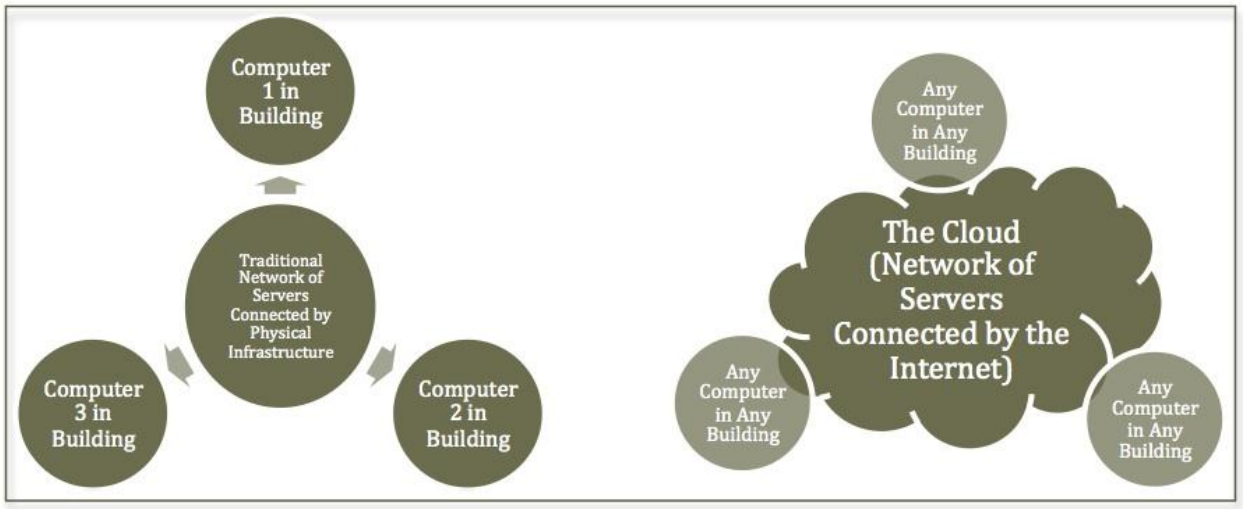

Figure 6.2: The Cloud Infrastructure

Cloud computing utilizes the Internet as a common connecting infrastructure because it stores data in "the cloud," rather than on a traditional server which has physical limitations

regarding accessibility. Therefore, any computer with a connection to the Internet can access files stored in the cloud. Examples of popular consumer programs using cloud computing include Facebook, Twitter, Gmail, Hotmail, YouTube, Skype, and Flickr.

The reason cloud computing is significant to information-sharing initiatives is because it allows agencies to maintain their own servers, while connecting servers virtually. Previously, government agencies maintained their own internal servers so that they could protect the physical security of their servers and also control access to information stored on these servers. While this was critical for security, it did not facilitate information sharing among different agencies, as access to stored information was limited to computers physically connected to the servers. Cloud computing still allows agencies to maintain the security of their servers, yet it provides a common platform for other agencies to access critical databases stored in other agencies servers.

Instead of each agency maintaining information on isolated servers incapable of sharing information, cloud computing offers a platform for connecting servers to facilitate the easier exchange of information.

Cloud Computing and the Current Administration

Cloud Computing is Central to the Government's Future Plans. In 2010, the Obama Administration unveiled the "25 Point Implementation Plan To Reform Federal Information Technology Management," which proposed a "Cloud-First" policy with the expressed goals of increasing the efficacy of IT federal systems, standardizing operational security processes, and, most emphasized, reducing the cost of maintaining data center hardware, software, and operations.[331] To implement the policy, the Federal Risk and Authorization Management Program (FedRAMP) was created through collaboration with NIST, GSA, DOD, DHS, and the CIO Council, among others, in order to provide guidance for the adoption of cloud computing among government agencies.[332] FedRAMP's first round of testing is expected to begin in June 2012, with companies specializing in providing infrastructure-as-a-service competing for future contracting opportunities; all who pass the evaluation are expected to comply with NIST's updated guidelines scheduled to be released in July 2012.[333] NSA and CIA are slated to unveil a multi-cloud system by 2013, which could facilitate easier information sharing among relevant partners. Cloud computing is neither centralized nor decentralized, and correspondingly it offers a hybrid of the features composing centralized and decentralized networks.

[331] Vivek Kundra, *25 Point Implementation Plan to Reform Federal Information Technology Management* (Washington, DC: The White House, 2010), http://www.cio.gov/documents/25-point-implementation-plan-to-reform-federal%20it.pdf.
[332] Federal Chief Information Officer Steven Van Roekel to Chief Information Officers, Security Authorization of Information Systems in Cloud Computing Environments, 8 December 2011, Executive Office of the President, Office of Management and Budget.
[333] Ross Wilkers, "FedRAMP Testing Starting in June," *ExecutiveGov*, March 21, 2012, http://www.executivegov.com/2012/03/report-fedramp-testing-starting-in-june.

Security of Cloud Computing

Cloud Computing Can be More Secure. Critics of "the cloud" cite security as one of its principle detriments, yet the cloud can be designed to address security concerns based on its defined architecture. Security features such as strong authentications for people and devices, data encryption, storage encryption and data tagging can be built into a cloud network. Already progress is being made toward authentications for personnel, predicted to be finished by the end of the year, and device implementation, slated for completion by 2013. These system features facilitate the role definition necessary for creating support for "authorized use."

Cloud computing offers autonomous security through flexible hardware/server location. The main advantage of cloud computing is that hardware can physically be stored on-site or off-site, allowing for flexibility in server location. For example, the CIA's cloud network can be maintained on servers located in the CIA's building, allowing the agency autonomy in retaining its security protocol for hardware, but not restricting access to the information stored in the cloud to computers located in the building. Rather, authorized users are able to access the server regardless of their proximity to the servers. Similarly, hardware can also be stored in an off-site location, if the CIA deems it preferable for hardware security. Either way, agencies are allowed to retain their autonomy in handling the physical security of an information system accessible by partners.

Accessibility with Cloud Computing

Cloud Computing Facilitates Accessibility. The "25 Point Plan" identified eliminating the legacy systems of each agency as a key goal in order to create an overarching, updated network capable of connecting Federal agencies. When the IC adopts the cloud network, artificial obstacles to information sharing will be eliminated, as cloud computing will offer a platform capable of connecting information and data among the agencies. Whereas in the past the agencies lacked the capability to email securely among themselves, now they would be able to access information specific to other agencies regardless of location.

Overcoming Technological Impediments

Cloud Computing Prevents Server Inadequacy. A key feature of cloud computing involves its ability to match the need for computing power with its provision. Rather than use a system with a finite amount of computing power—restricted by the number of servers—cloud computing offers infinite computing power, when it's needed. For example, if an emergency like a hurricane occurs, and more people try to access the National Weather Service's webpage, the NOAA would be automatically allotted the additional computing power necessary to maintain its site hosting a greater number of visitors. In the past, these services merely crashed under (server-surpassing) additional demand; with cloud computing, the upswing in demand would result in an upswing of power supply.

While cloud computing will offer a modern IT platform capable of removing the IT barriers for information sharing, other obstacles such as cultural aversion to sharing have to be addressed before any IT system—cloud or otherwise—is effective. The cloud will ensure

the most critical aspects of information sharing, discoverability and access, but it is incapable of ensuring an integrated IC community on its own.

NIEM and UCORE

Platforms for Interoperability. The DOJ and DHS partnered in 2005 to launch the National Information Exchange Model (NIEM), an initiative to create a platform facilitating interoperability in data sharing among government agencies and key partners.[334] It encourages the standardization of IT processes by providing "a data model, governance, methodologies, training, technical assistance, and an active community" to federal, state, local and tribal agencies, as well as some private sector partners, as an instrument to enable better data sharing among them.[335] NIEM expresses its mission as follows:

1. Enhancing the quality of governmental decision making by enabling accurate, timely, complete, and relevant information to decision makers across the broad spectrum of NIEM COIs.

2. Achieving greater efficiency, effectiveness, and return on investment (ROI) in operations by accelerating information exchange design and development.

3. Reducing risk in development efforts for practitioners and industry by having common exchange standards, tools, processes, and methodologies.

4. Improving public safety and homeland security by breaking down "stovepiping" to enable real-time, secure, enterprise-wide information sharing.[336]

NIEM pursues its vision by standardizing language and data among agencies so that they can better share data. It has 14 "domains," or fields of interest that NIEM actively engages, including biometrics, family services, emergency management, immigration, and intelligence.[337] One of NIEM's fundamental building blocks includes identifying or defining data components, the pieces of information that are universally shared and understood across partners in each domain, creating a common semantic understanding of these pieces and a consistent data format for exchange.[338]

NIEM's success stories include facilitating the implementation of Suspicious Activity Reporting (SAR) in 2008, as it provided the metadata dictionary used to define SAR's information, and also solidified key policy and processes for sharing across public and

[334] National Information Exchange Model Program Management Office, *Introduction to the National Information Exchange Model (NIEM)* (Washington, DC, 2007), https://www.niem.gov/documentsdb/Documents/Overview/NIEM_Introduction.pdf.
[335] "What is NIEM?" NIEM, https://www.niem.gov/about /what-is-niem/Pages/what-is-niem.aspx.
[336] National Information Exchange Model Program Management Office, *Introduction to the National Information Exchange Model (NIEM).*
[337] "About Domains," NIEM, https://www.niem.gov/about/domain/Pages/about-domains.aspx.
[338] Jeremy Warren, "NIEM Success Stories: LEXS, OneDOJ, and N-DEx," (presentation, NIEM Industry Day, February 17, 2009).

private partners.[339] One program manager explained, "There is now for suspicious activity reports a standard way to express and share information between agencies. You have a standardized set of data. When you look at it from an aggregate level, you start making sense of it. You can start to see patterns or similarities and anomalies."[340]

Similarly, the DHS's Domestic Nuclear Detection Office (DNDO) also implemented NIEM standardization in 2008, allowing the DNDO to create a consolidated domain for chemical, biohazard, radioactive, and nuclear information (CBRN), utilizing information from the already NIEM-standardized U.S. Customs and Border Protection (CBP) database and the Southeast Transportation Corridor Pilot (SETCP).[341] Currently, the DNDO's Joint Analysis Center monitors all CBRN data through its Joint Analysis Center Collaborative Information System (JACCIS), made possible by NIEM.[342]

UCORE originated as a joint effort between the chief information officers of the DoD and the Office of the Director of National Intelligence (ODNI) in 2007 to identify a common core of universal terms to standardize messaging among the defense and intelligence community.[343] A "universal core," or UCORE, of data was discovered among the community messaging, composed of primary data on "who, what, when, and where."[344]

After some resistance, the Universal Core 1.0 was produced, which defined common semantics and syntax for use among the community; its early adopters included the U.S. Strategic Command's (STRATCOM) Strategic Knowledge Integration Web (SKIWeb), the Joint Forces Command (JFCOM), and the National Security Agency (NSA).[345] Tasked with enveloping the DOJ and DHS into the integrated platform, the next step in UCORE development involved collaboration with NIEM to ensure the interoperability of the two systems.

The chief information officers of the DoD, ODNI, DHS, and the DoJ worked for over a year to create integration between UCORE and NIEM, resulting in enterprises such as the DHS Unified Incident Command and Decision Support (UICDS) System and the Maritime Domain Awareness initiative. Jeremy Warren, the Chief Technology Officer at DoJ, said of the success, "If I were to have an optimistic expectation for the outcome of this, it would be that UCORE and NIEM together is the triumph of interoperability over king-of-the-hill."[346]

---

[339] Program Manager, Information Sharing Environment, *From a Portfolio of NIEM Success Stories: Suspicious Activity Reporting* (Washington, DC), https://www.niem.gov/documentsdb/Documents/Success%20Stories/SuccessStory_SAR.pdf.
[340] *Ibid.*
[341] Program Manager, Information Sharing Environment, *From a Portfolio of NIEM Success Stories: The DHS Domestic Nuclear Detection Office Goes NIEM* (Washington, DC), https://www.niem.gov/documentsdb/Documents/Success%20Stories/SuccessStory_DHS.pdf.
[342] *Ibid.*
[343] Program Manager, Information Sharing Environment, *From a Portfolio of NIEM Success Stories: UCORE and NIEM, Creating Potent New Cross-Boundary Networks* (Washington, DC), https://www.niem.gov/documentsdb/Documents/Success%20Stories/SuccessStory_UCORE.pdf.
[344] *Ibid.*
[345] *Ibid.*
[346] *Ibid.*

Metrics for Information Sharing – How Well Are We Doing?

Are We Safer Today?

Assessing Information Sharing Ten Years Later. A decade has passed since 9/11 without another major terrorist of the same magnitude occurring on U.S. soil. It would be a grave misstatement, however, to declare a definitive success of U.S. efforts to secure the homeland, because of the numerous terrorist plots aimed at the U.S. Although to date all major terrorist plots have been either thwarted or otherwise failed technically, the risk of another version of 9/11 remains. More so, internationally, there have been a number of devastating attacks such as London and Madrid subway bombs, which killed more than 250 people in spite of significant counter-terrorism efforts.[347]

To some extent this can be attributed to the substantial progress made by the U.S. Government in the post 9/11 world to streamline and improve information sharing amongst the various agencies. Information sharing among Federal, State and Local intelligence agencies, and law enforcement agencies has substantially improved from the previous decades of stove piping and exclusion. Exemplifying such progress was a joint effort by the FBI, NYPD, and other agencies to survey and prevent the 2009 plot to bomb New York's major subway stations.

Although the capture of Najibullah Zazi, the suspected perpetrator of the NYC subway bomb plot, was ultimately thwarted, the investigation was rife with distrust and stove piping.[348] In the case of the NYPD, an internal decision was made to question its own informant Ahmad Wais Afzali regarding Zazi without notifying the Joint Terrorism Task Force (JTTF). Afzali subsequently warned Zazi about the investigation, forcing the FBI to execute warrants and make arrests earlier than intended, which had the major consequences of threatening the investigation and increasing the distrust between the Local and Federal agencies.

Information sharing between the varying agencies has been an important factor in the successful prevention of terrorist attacks, however, luck has been a significant contributor in the fortuitous failure of terrorist plots. A review of terrorists captured over the past decade in the U.S., Europe, and the Middle East shows that in almost all cases the terrorists took action that can be described in operational terms as either being "sloppy" or "stupid," and in many cases both.[349] The incompetence that has characterized several of the terrorist plots will, however, end as individuals become more adapt and experienced, creating an urgent need to continue enhancing the mechanisms to ensure information

[347] Mitchell Silber, *Radicalization in the West: The Homegrown Threat Assessment* (New York, NY: New York Police Department, 2007), 68.
[348] William K. Rashbaum and Al Baker, "How Using Imam in Terror Inquiry Backfired on Police," *New York Times*, September 23, 2009, http://www.nytimes.com/2009/09/23/nyregion/23terror.html?pagewanted=all.
[349] *Ibid.*

sharing. Today, information sharing to prevent future terrorist attacks by increasingly sophisticated terrorists remains insufficient.

Illustrating the pressing importance for strengthened access to information is the case of Nigerian Islamasist Umar Farouk Abdulmutallab, commonly known as the "underwear bomber." The failure to detonate explosives on Northwest flight 253, originating from Amsterdam, was the result of an inability to assemble the necessary ingredients to spark the explosion.[350] The inability of Abdulmutallab combined with a nearby passenger who rapidly took bold action to restrain Abdulmutallab reflect continued shortcomings within the realm of national security.[351] A subsequent report issued by the Senate Select Committee on Intelligence depicted 14 specific intelligence failures:

1. A revocation of Abdulmutallab's passport by the Department of State based on information available to the Department.

2. Abdulmutallab failed to be placed on the terrorist watch list due to rigid interpretations.

3. Key intelligence reports failed to be reported to appropriate CIA offices and personnel.

4. A CIA division did not perform a search of databases that included Abdulmutallab.

5. CIA failed to disseminate key intelligence until after the failed plot.

6. A simple name search through the CIA Counter Terrorism Center was limited by exact spelling and did not retrieve all critical reports.

7. CIA Counter Terrorism analysts were occupied by threats from *al-Qaeda* in the Arabian Peninsula, and were unable to extend full intelligence capacity on Abdulmutallab,

8. A wrongly configured computer prevented an FBI Counter Terrorism expert from accessing all reports on Abdulmutallab.

9. The National Counterterrorism Center (NCC) Directorate of Intelligence lacked the organizational foundation to effectively disburse intelligence on Abdulmutullab.

10. The NCC's Watch Listing Office did not perform additional research that would have placed Abdulmutallab on a watch list.

11. The NSA did not take all available actions to provide information on Abdulmutallab.

---

[350] Kevin Krolicki and Jeremy Pelofsky, "Nigerian Charged for Trying to Blow Up U.S. Airliner," *Reuters,* December 26, 2009, http://www.reuters.com/article/2009/12/26/us-security-airline-charge-idUSTRE5BP1MP20091226.

[351] *Ibid.*

12. Analysts did not connect key reports that partially identified Abdulmutallab, and did not convey intelligence.

13. The NSA did not select Abdulmutallab to be placed on a watch list based on the reports that partially identified him.

14. Intelligence analysts were focusing primarily on Yemen and the rising threat to U.S. interests of *al-Qaeda* in the Arabian Peninsula (AQAP), instead of potential threats to the U.S.[352]

Since the 9/11 terrorist attacks, the U.S. has spent upwards of 1 trillion dollars to measures and policies in the "War on Terror."[353] Quantifiable results of the massive expenditure are, however, difficult to discover, leading to an opaque conclusion on whether the U.S. is truly safer. Moreover, it remains unclear what exactly is the basis for an "effective" counter-terrorism policy, because the factors that must be examined are wide-ranging, and oftentimes consist of classified information.

The definition of terrorism, "the use of violent acts to frighten the people in an area as a way of trying to achieve a political goal," reflects the fundamental psychological element of terrorism.[354] There will always be plots to attack the U.S. no matter the changes in airport security, electronic surveillance and human intelligence; it is the curse of being a global power. Until information is released that shows the effects of U.S. counter-terrorism efforts, the question of "are we safer" remains to be answered.

Balancing the "Need-to-Share" and the "Need-to-Know"

Altering Culture Across Agencies. The Intelligence Community has made significant progress on the transformation from the long-standing security principle of "need-to-know" to the current concern for a "need-to-share." The ISE 2011 Annual Report indicates that there has been a 30% increase, encompassing 71% of all ISE departments, that have incorporated "information sharing and collaboration" as a component in performance appraisals of employees without direct ISE responsibilities.[355] Additionally, 100% of employees that directly support ISE related priorities have information sharing as a component of their performance appraisal.[356]

Possibly the best example of how effective the Government has been in promoting a culture of sharing is seen by examining the broad ramifications of *Wikileaks*. The embarrassment caused by the *Wikileaks* failure was felt throughout all realms of government, resulting in a within the IC that the exposure would hinder the information sharing culture. Without

---

[352] Senate Select Committee on Intelligence, *Report on Attempted Terrorist Attack on Northwest Airlines Flights 253, Unclassified Executive Summary, United States Senate, 111th Congress,* S. REP. NO. 111-199 (2010).
[353] John Muellerand Mark G. Stewart, "Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security" (paper presented at the annual meeting of the Midwest Political Science Association, Chicago, IL, April 1, 2011).
[354] *Merriam-Webster Dictionary*, 11th ed., s.v. "terrorism."
[355] Information Sharing Environment, *Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment,* 25.
[356] *Ibid.*

confidence in the security of the system, it was feared that data stewards would no longer share sensitive information with the rest of the IC.[357] A reversal in the positive sharing trend would act to unravel years of work to promote collaboration. However, surprisingly this was not the course of events.

Rather than a decrease in collaboration, the IC continued on the trajectory of becoming more cooperative. Security was extensively re-examined throughout agencies, protocols were changed and certain systems were either altered or removed. Confidence in the system not decline as had been originally expected following the alterations, and overall, it did not greatly affect the extent of information sharing.[358]

The *Wikileaks* failure is a testament to how far the IC has progressed in the last ten years because the public and embarrassing security breach did not significantly dampen the culture of advancing information sharing. In hindsight, it could have been worse. The release of much more sensitive information could have had much greater ramifications for National Security. The important lesson learned from *Wikileaks* is that although the current culture directs a "need-to-share," information sharing is not itself the final end point, but rather a means to better protect the country. The IC must be cautious to avoid disclosing data for the sake of sharing. Proper security and architecture are just as fundamental as the transformation of the culture.

Although technology is an important element for collaboration, it will not fix the bureaucratic issues that have plagued the IC. These bureaucratic concerns should not be underestimated and methods that continue to alter the culture should continue to be implemented. "Rewarding behaviors that foster information sharing and adoption of collaborative cross-agency work teams will improve performance throughout the Government, and improve efforts conducted with non-governmental partners. "[359] A culture that is more focused on information sharing for the federal agencies will contribute to a better integration of all stakeholders.

Structure of the Information Sharing Environment

One of the most important aspects to measure progress toward and success in information integration involves examining the interoperability between IT structures and data among the IC. Initiatives such as the National Information Exchange Model (NIEM) and Universal Core (UCORE) are integral to the success of creating a truly integrated information sharing environment, as they catalyze completion of the first step in integration: creating common syntax and semantics. Information sharing will never be fully automated without universal language and definitions for data, and a common platform for dialogue and exchange regarding implementation.

---

[357] Senate Select Committee on Intelligence, *Report on Attempted Terrorist Attack on Northwest Airlines Flights 253, Unclassified Executive Summary.*

[358] *Ibid.*

[359] Information Sharing Environment, *Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment,* 25.

Agency Holdings and Dissemination Concerns

Storing Intelligence and Releasing Intelligence. A vital metric as a means to measure of information sharing involves first, the percentage of information an agency collects and stores in an accessible database and second, the agency's progress toward implementing standardized language to enable data sharing with relevant partners.[360] Automated information sharing is only possible if information is stored on an accessible IT platform; with this understanding, agencies need to address any shortcomings in data treatment. Additionally, to continue the widespread dissemination of information, agencies need to identify realistic training measures and procedures regarding their individual protocols for treating and handling collected data.

Failure to Automate Systems

Assessing the Trilogy Program. In 2000, the FBI announced the Trilogy program, designed to update their antiquated computer system in a three-step approach. First, desktop computers would be installed throughout their offices; second, these computers would be connected using secure, high-performance networks; and third, 'virtual case file' (VCF) software would replace the Bureau's Automated Case Support (ACS) software.[361] By 2005, the FBI officially abandoned the Trilogy program after spending upwards of $170 million in Federal funding, earning an accolade for the "most highly publicized software failure in history."[362]

While the Trilogy program ultimately succeeded in its initial goal of providing office computers connected with a secure network, changing its case management software proved too difficult for the FBI. Currently, the FBI still relies on a mixture of paper records and an antiquated software system implemented in the 1970s to build case files and gather intelligence. Its continuing difficulties in automating its intelligence within its own agency promises to plague efforts toward integration with other agencies.

Appropriate Discoverability

The Ability to Discover Intelligence. In an effort to support greater information sharing throughout the law enforcement, public safety, homeland security, foreign affairs, defense and intelligence communities, the ability to discover information is crucial and becomes a necessary feature in any future architectural landscape.

The Office of Director of National Intelligence, in keeping with its Information Sharing Strategy, recognizes the importance of sharing information in an effort to bolster collaboration and facilitate analysis that is better equipped to help safeguard the nation.[363] In the new information sharing model, the ODNI stipulates that "information providers

---

[360] *Ibid.*
[361] Harry Goldstein, "Who Killed the Virtual Case File," *IEEE Spectrum,* September 2005, http://spectrum.ieee.org/computing/software/who-killed-the-virtual-case-file.
[362] *Ibid.*
[363] Office of the Director of National Intelligence, *United States Intelligence Community Information Sharing Strategy.*

must make information accessible, available and discoverable at the earliest point possible."[364]

Moreover, the ODNI suggests that all intelligence information should be discoverable and mission accessible. The ODNI supports that all information should be made discoverable to intelligence community collectors and analysts in order to establish relationships between information, and consequently analysts and operators in different agencies, and to facilitate greater information synthesis and more in depth analysis. Information, however, should be accessible only to appropriate authorized users.

While analyst and operators may be able to search for information, helping to spur collaboration between various agencies, only those with the appropriate access should be able to actually acquire that information. The ODNI maintains that all intelligence analysts and operators, regardless of their classification or their organizational affiliation, should be aware of the existence of all intelligence information, even if they are not authorized to access it. The ability to discover information has the potential to create a much needed "relationship to other data, providing a better opportunity to 'connect the dots'" and ultimately strengthen efforts to combat threats to the nation. [365]

In 2009, the ODNI issued Intelligence Community Directive Number 501 (ICD 501), to "strengthen the sharing, integration and management of information within the Intelligence Community (IC), and establishes policies for [both] discovery, and dissemination or retrieval of intelligence and intelligence-related information collected or analysis produced by the IC."[366]

This directive underscores the importance of being able to discover information. The directive mandates that "IC elements fulfill their 'responsibility to provide' by making all intelligence-related information that IC divisions are authorized to acquire, collect, hold, obtain and analyze discoverable through automated means by "authorized IC personnel."[367]

---

[364] Office of the Director of National Intelligence, *United States Intelligence Community Information Sharing Strategy,* 3.
[365] *Ibid.,* 10
[366] Office of the Director of National Intelligence, *Intelligence Community Directive Number 501: Discovery and Dissemination or Retrieval of Information within the Intelligence Community,* 1.
[367] Authorized IC personnel are individuals identified by their elements head and who have an appropriate security clearance and an assigned mission need for information collected or analysis produced. Discovery is the act of obtaining knowledge of the existence, but not necessarily the content, of information collected or analysis produced by any IC element. Office of the Director of National Intelligence, *Intelligence Community Directive Number 501: Discovery and Dissemination or Retrieval of Information within the Intelligence Community,* 2.

Long-term Viability of Information Sharing Initiatives

Information Sharing in the Future. Another specific example of progress in information sharing was the 2007 National Strategy for Information Sharing. Developed by the ISE, it has been a crucial step towards strengthening collaboration. The update to the National Strategy, scheduled to be released in 2012, will further identify key areas of focus. These crucial areas will focus on an information centric approach with particular attention to the following aspects of information: discoverability, sharing, protection, fusion, and reuse.[368] Additionally, a renewed focus will be on enhancing relationships with mission partners across the five communities: law enforcement/public safety, defense, intelligence, homeland security, and diplomacy.[369] The next major step will be development of a broad applicability to the variety of necessities for each particular CT and homeland security realms.

Currently, agencies and departments in the IC have, for the most part, taken an active role in adhering to ISE policies. Many have implemented the strategies recommended by the ISE. There are certainly areas that require improvement, but in general the ISE has been instrumental in providing a framework and metric for success. Even in areas requiring further development, there is a positive upward trend toward achieving the goals.

Agency Adherence to ISE Policies - Critical Areas where ISE Goals and Objectives Have Been Met

Important Achievements by the Information Sharing Environment. Although the Information Sharing Environment still requires improvement, it has made substantial progress in the following areas:

Personnel Appraisals

This area is a clear success story, where currently 100% of responding ISE departments and agencies have included "information sharing and collaboration" as a component in performance appraisal of employees supporting ISE-related priorities. [370] This number had a 14% increase from the previous year, demonstrating the immediate positive effect policy changes.[371] As culture is a critical area that hinders information sharing, it is a pivotal to implement and evaluate these types of policies which have had a demonstrated impact.

Governance

In order to effectively oversee and implement the ISE, the Information Sharing and Access Interagency Policy Committee (ISA IPC) was created as means of vertical leadership over the ISE. The ISA IPC formally charters Sub-Committees to provide advice and support to the IPC, as well as charging the Sub-Committees with the responsibility of quarterly

[368] Program Manager, Information Sharing Environment, *ISE Annual Report to the Congress,* 6.
[368] *Ibid.*
[369] *Ibid.*
[370] *Ibid.,* A-1
[371] *Ibid.,* 112.

progress reports since 2011.[372] Under the leadership of ISA IPC, 50% of all ISE departments have established dedicated information sharing offices, directorates, divisions or executives.[373]

ISE Awareness Training

When compared to the 2010 Annual Report, there has been a 7% increase among responding departments and agencies in the development of ISE mission-specific training.[374] This constitutes roughly 71% of responding agencies.[375] In addition to personnel appraisals, training is an important tool to combat the "turf wars" that have plagued the culture of collaboration.

Incentives for Information Sharing

Although 2010 did not experience an increase, 86% of responding agencies offer or intend to offer an award that includes information sharing and collaboration directly or indirectly as criteria.[376] Although only 43% of ISE departments and agencies identified an increase in sharing and collaboration award nominations, the number represents a 100% growth from 2010.[377] Positive reinforcement is an important element to consider when encouraging a cultural shift. The expansion of employee incentive awards for collaborative efforts will further drive the forward momentum of increasing information sharing across agencies.

Critical Areas For Current ISE Investments

Areas that Must be Improved. In spite of important successes achieved over the past decade, there are significant improvements that must be made to ensure intelligence is shared. These include:

Privacy Policies

According to the performance assessment data from the 2011 ISE Annual Report, only 64% of respondents have developed and implemented an ISE Privacy Policy and submitted it to the Privacy and Civil Liberties Sub-Committee.[378] Unfortunately, this percentage has not increased since the 2010 assessment.

Furthermore, only 57% of respondents have personnel with information sharing responsibilities that have received training on the agency's privacy and civil liberties policies. This represents a 13% increase since the 2010 report, but clearly this area has not been a key focus within the IC.[379]

---

[372] *Ibid.*
[373] *Ibid.*
[374] *Ibid.,* A-2.
[375] *Ibid.*
[376] *Ibid.*
[377] *Ibid.*
[378] *Ibid.,* A-5.
[379] *Ibid.*

The role of privacy when considering the debate over U.S. citizens is an area of considerable gravity that will require significant leadership and investment. Specific policies must address the rapidly expanding technological capabilities that the IC is able exploit in order to protect Fourth Amendment rights of citizens. Privacy concerns must be paramount, else third parties will no longer share with the Government and public trust in the system will be damaged.

Architecture – Investments

Per the 2011 ISE Annual Report, only 57% of responding ISE departments and agencies have included all major ISE IT investments in their transition plans. This constitutes only a 7% increase since the 2010 Annual Report.[380]

Surprisingly, only 36% of responding ISE departments and agencies have a plan for implementing interconnection capability in order to share terrorism and homeland security information across Special but Classified (SBU) and Controlled Unclassified Information (CUI) networks. Agencies that did not respond with a positive response include the CIA, the ODNI, and the NCTC.[381]

The 2012 Report should highlight the possible solutions to this issue as architecture is a fundamental challenge that continues to plague the IC. In the current fiscal climate, agencies and departments will no longer have the resources to independently invest in IT structures, and will be obliged to coordinate their efforts together.

Architecture-Common Information Sharing Standards (CISS)

A mere 50% of agencies approved and completed information sharing segment architecture.[382] Amongst the agencies that did not, are the CIA and the ODNI. Additionally, only 50% of agencies have incorporated Common Information Sharing Technical Standards into enterprise architecture and IT capability. The CIA, ODNI, and NCTC however, do not fall within this group.[383]

Uniform information standards and policies require focused leadership and investment from the ISE. Future inter-agency architecture will likely support a common standard, but adequate policies need to be implemented for agency specific systems. More so, policies need to specifically target departments that continue to resist CISS, such as the CIA, ODNI and the NCTC.

Networks

In order to easily facilitate information sharing amongst tribal, local, state and federal agencies, the Department of Homeland Security established the Homeland Security Information Network (HSIN). The computer-based counter-terrorism communications network is currently utilized in all 50 states, the District of Columbia, 5 territories and 50

[380] *Ibid.,* A-6.
[381] *Ibid.*
[382] *Ibid.,* A-7.
[383] *Ibid.*

outside major urban areas as a means of encouraging open two-way threat information communication.[384]

The lack of a clear mission and vision by HSIN, however, has resulted in decreasing confidence in using the system, resistance to posting sensitive and classified information, and lack of training on how to effectively utilize the new system to share critical information. As a result, the HSIN has been incapable of successfully implementing the cross-agency networks.[385]

Trust in the system poses a major obstacle in the functionality of HSIN. Although there are currently 366 members of the community, the network averages 27 logons per month representing 7% of those who currently have access.[386]

Critical Areas for Future ISE Investments

Future Goals for the ISE. Several general key future initiatives that require future investment from the ISE include:

1. Acceleration of the development and adoption of common standards through common architecture and shared training initiatives.

2. Improvement of the interoperability of inter-agency networks.

3. Implementation of an inter-agency architectural system (Cloud System).

4. Fortification of means for rapidly disseminating both classified and unclassified terrorist information between federal, state, local and tribal entities.

5. Strengthening of intelligence sharing between the IC and State, Local, Tribal and Private Sector (SLTPS).

6. Streamlining and standardization of discoverability processes.

Cost Effectiveness of Information Sharing Initiatives

Tightened Budgets Promote Information Sharing. In the current fiscal environment, budgetary constraint is a factor that must be addressed. The viability of expanding intelligence sharing under monetary restrictions is a daunting task, and decreasing budgets will prove a challenge for all federal agencies and departments for the foreseeable future. Ironically for information sharing, budget constraints may help to increase sharing by purging stovepipes and growing inter-agency cooperation.

---

[384] Information Sharing Environment, *National Strategy for Information Sharing*, 8.
[385] Department of Homeland Security Office of Inspector General, *Homeland Security Information Network Could Support Information Sharing More Effectively* (Washington, DC, 2006), 6, http://www.oig.dhs.gov /assets/Mgmt/OIG_06-38_Jun06.pdf.
[386] *Ibid.,* 24.

Intelligence agencies and departments will no longer have the resources to engineer and implement their own systems. Fiscal constraint will force the IC to aggregate funds and develop collective systems that incorporate input from multiple members of the IC. Forced integration will help to standardize the systems and make them interoperable, such as efforts by the NSA and CIA to spearhead the effort to design and implement the cloud system, estimated to be released in roughly two years.[387]

Additionally, increased integration is likely to promote the growth of coordination in areas separate from the technical and architectural aspects. Increased inter-agency cooperation will break down the intrinsic mistrust between agencies because linking agencies with a common specific goal will only help to accelerate inter-agency cooperation, in spite of agency wariness of one another.

Finally, the capacity to quicken the cultural change that has plagued the intelligence community will potentially be affected in a positive manner by reduced budgets and limited resources to implement individual technological systems. The future of IC collaboration and communication will most likely begin to reflect the economic constraints that have affected all agencies.

[387] *Ibid.*

[This page is intentionally left blank]

Conclusion

A Final Analysis of Information Sharing in the 21st Century. The Information Sharing Environment was created to facilitate the exchange of information between agencies in the hopes of increasing the effectiveness of U.S. counter-terrorism efforts. The size and scope of the U.S. Intelligence Community, along with the restrictions placed on intelligence collection and sharing by the Constitution, legislation, and Executive Orders from several Presidential Administrations, guaranteed that implementing and operating the ISE effort would be extremely difficult. The process has been further hindered by the challenge of addressing multiple issues with engrained agency culture, the protection of privacy, information security, and architectural and technological frameworks.

These challenges remain daunting, however the following recommendations attempt to further the ISE's development by addressing the primary concerns.

Culture – A Federal Vision for Information Sharing

A Federal Vision is Required to Promote Positive Reinforcement Strategies for All ISE Personnel and Agencies. Reinforcing the importance of information sharing and security is integral to changing the culture of the IC to fully accept sharing. Positive reinforcement strategies, such as increased program funding or collaboration awards, should be linked to both agency-wide and individual information sharing performance.

Joint-Duty Assignments Should be Increased to Counter Instances of Bureaucratic "Turf War." Competition over agency "turf" is extremely detrimental to mission effectiveness. To combat this, ISE partner agencies should increase their encouragement of joint-duty assignments in other agencies or departments to break down walls between agencies. Promotions to senior management positions should require at least one tour of duty at a different agency.

The President and Other Executive Branch Officials Should Express the Importance of State and Local Agencies and of the Private Sector. State, local and tribal agencies now play an extremely important role in successful counter-terrorism operations and analyses, but are not fully appreciated by their federal counterparts. The private sector also possesses large amounts of information that is of great value to federal counter-terrorism efforts. Continued Executive Branch support for the importance of state, local, tribal and private sector partnerships is needed to reinforce notions of their importance and necessity to federal agencies.

The Federal Government Should Implement a Unified, Nation-Wide Training Program for State and Local Officials. Instituting a nation-wide training program for non-federal officials will simultaneously expand the capabilities of state and local officers while increasing the levels of trust between Federal and non-Federal counter-terrorism and law enforcement officials. Training programs should include a wide range of state and tribal officials, but should be targeted at senior, management-level officials.

Privacy – Training Programs for Better Understanding

Inter- and Intra-Agency Training Programs Should Provide Solid Understanding of Key Privacy Laws and Regulations. The number of provisions within Congressional legislation that apply to information sharing through the ISE is staggering. Combined with the more than one hundred individual sets of privacy guidelines that currently exist among the ISE's various partner agencies, this amount of information can be incredibly difficult to process, understand, and properly implement. ISE partners should create training programs that provide a solid overview of these rules and regulations, so that analysts within agencies fully understand the rules that they must adhere to.

Personnel with Oversight Authority Should Also Have the Authority to Enforce Compliance . Individuals at the management level within ISE partner agencies have the responsibility to provide oversight of their agencies' compliance with relevant privacy laws and regulations. Oversight without enforcement authority, however, is not effective and is not sufficient to ensure that privacy and civil rights are protected throughout the ISE. Enforcement authority should be codified into each ISE agency's privacy guidelines.

Congressional Oversight of All ISE Participants Should be Increased. While individual agencies should be responsible for oversight and enforcement of their own privacy policies, guidelines and rules, Congressional oversight over the entirety of the ISE should be increased to ensure compliance with privacy standards on a macro level. Congressional oversight can be a very effective tool for enforcing compliance, when properly executed. Involving Congress in the protection of privacy within the ISE is a natural step.

The ISE's Privacy Guidelines Should be Unified and Centralized. As of this writing, information held by and shared through the ISE is governed by provisions in the Privacy Act of 1947, the Freedom of Information Act, the E-Government Act of 2002, the Intelligence Reform and Terrorism Prevention Act of 2004, several Executive Orders issued by several decades' worth of Presidential Administrations, and over one hundred sets of privacy guidelines written, maintained, and enforced by the individual members of the ISE.

The ISE's efforts sit at the intersection of this incredibly complicated and vast series of rules and are hampered by overlapping, contradictory, outdated and irrelevant regulations and guidelines. A singular, unified set of comprehensive and enforceable guidelines should be created that applies to all information inputted into the ISE. The current ISE guidelines are too generic and fragmented, and are not sufficient to satisfy this requirement.

Guidelines Should be Replaced with Enforceable Rules That Do Not Allow for Exceptions. The Privacy Act, Freedom of Information Act, and other major pieces of Congressional legislation have been quite effective in outlining a series of rules and regulations for protecting individual privacy while still allowing the Government to collect and analyze personal information. The number and scope of exceptions in these pieces of legislation, however, allows many of the ISE's partner agencies to avoid adherence to those regulations on various bases. These exceptions should be removed to truly ensure transparency and the protection of individual privacy.

Security – Specific Guidelines for the ISE

Information Security Guidelines Should be Created Specifically for the ISE. The frequency of data exchange necessary for operating an effective ISE creates unique challenges for the Federal Government and provides many more opportunities for security breaches. The rapid advancement of digital attacks has also, in general, greatly increased the importance of information security practices for sensitive information. These realities must be addressed by an appropriate set of information security procedures specifically designed for the ISE's unique requirements.

Personnel with Oversight Authority Should Also Have the Authority to Enforce Compliance. As with privacy guidelines, oversight authority within individual agencies should be coupled with enforcement authority for information security guidelines. Oversight without enforcement is ineffective, and the importance proper information security carries in today's world of rapidly advancing technology is too high to allow agencies to slip on compliance with proper guidelines.

A Comprehensive Risk Assessment Framework Should be Developed. Currently, information sharing decisions are made based on risk assessments undertaken by individual ISE partner agencies. These assessments consider both the privacy concerns associated with sharing a piece of information as well as the security risks associated with withholding it. Risk assessments, however, are handled individually by the ISE's agencies. In order to promote standardization in sharing, the ISE should issue a universal of criteria for conducting risk assessments.

A Risk Assessment Training Program Should be Implemented Throughout the IC. To further facilitate the standardization of risk assessment criteria, the ISE and its partner agencies need to create training programs that educate analysts about how to properly conduct a risk assessment. Standardization of risk assessment processes should be a priority of the ISE, and training programs are essential to accomplishing this goal.

Architecture – Optimizing the Centralized Model for Cost-Effective Information Sharing

Centralized Information Sharing Systems Offer Standardization Advantages. Standardizing regulations, procedures, methods, and practices through a centralized information sharing system can promote efficiency and uniformity in the ISE's efforts. Instituting a centralized system allows the ISE to ensure that all partner agencies can partake in the same set of training programs and privacy regulations, which enhances the ISE's ability to enforce compliance with necessary rules, regulations and procedures. Data is stored in a central location, which removes questions about where to access information. Centralized systems do, however, simultaneously present security advantages and risks: information stored centrally and controlled primarily by a single entity can be placed under stricter security provisions, but a breach in those provisions can facilitate a significantly larger leak of sensitive information than under a decentralized, more fragmented system.

Decentralized Information Sharing Systems Can Enhance Individual Agency Performance at the Expense of Increasing Cooperation. When a decentralized model is used, individual agencies retain their own databases and information, on their own systems, based on their own rules. This can be beneficial for legal compliance by allowing each agency to operate under its own regulatory schemes and by reducing the threat of secondary use. Security is also enhanced, as there is no central repository of information that can be breached. Decentralized models do, however, allow many of the problems currently facing the ISE to continue. By emphasizing independence among ISE agencies, issues such as "stovepiping" and lack of agency coordination and cooperation will continue. This is counter to the ISE's mission.

The ISE Should Emphasize Cloud Computing. Today's technological advancements allow the Government to retain physical media storage in a centralized location while simultaneously allowing its personnel to have extensive access to its content. The advantages offered by cloud computing can be extremely beneficial to the ISE's efforts and should be accordingly embraced. Cloud computing offers robust physical security and data access controls while maintaining quick and easy access standards for agencies. These features are scalable to enhance reliability and stability, and are very cost-effective.

Continuing, Rigorous Training Programs Should be Implemented Throughout All ISE Partner Agencies. All programs should create ongoing training programs that emphasize inter-agency cooperation, the importance of privacy protections, and an adherence to the rules and regulations associated with each agency's mission and participation in the ISE. Training programs are relatively easy to implement and come at a low cost, yet they often result in significant enhancements to performance and efficiency. Each agency should seek to streamline its own operations through training, then initiate inter-agency training programs that aim to increase the efficiency, accuracy, and security of the ISE as a whole.

It is an unfortunate truth that the U.S. Federal Government's counter-terrorism efforts will, out of necessity, continue to expand into the foreseeable future. The Information Sharing Environment will provide federal agencies with increased capabilities, notice, and information to use to combat the omnipresent threat that international terrorism represents to the nation. The system, however, will need constant oversight and attention, by Congress, individual agencies, and the American public to ensure that it is operating in ways that facilitate the useful sharing of information while protecting individual privacy, civil rights, intelligence sources and methods, and government resources. These efforts would be enhanced by the adoption of this report's recommendations.

Appendix 1: The Capstone Team

Dara Stofenberg
Project Manager

Oyindamola Adegboro

John DeNicola

Kelsey Field

Evan Howlett

Takayuki Miyagawa

Rachel Paulk

Dr. Abraham Wagner
Columbia University Faculty Advisor

Dr. Stefaan Verhulst
Director of Research, The Markle Foundation

[This page is intentionally left blank]

Appendix 2: List of Acronyms

ACLU	American Civil Liberties Union
CI	Counter-intelligence
CIA	Central Intelligence Agency
CRCL	Officer for Civil Rights and Civil Liberties
CT	Counter-terrorism
DCI	Director of Central Intelligence
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DOA	Department of Agriculture
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DOS	Department of State
DOT	Department of Transportation
DOT	Department of Treasury
EO 11905	Executive Order 11905
EO 12333	Executive Order 12333
EO 12356	Executive Order 12356
EO 12968	Executive Order 12968
EO 13284	Executive Order 13284
EO 13353	Executive Order 13353
EO 13354	Executive Order 13354
EO 13355	Executive Order 13355
EO 13356	Executive Order 13356
EO 13388	Executive Order 13388
EO 13470	Executive Order 13470
EO 13549	Executive Order 13549
EO 13556	Executive Order 13556
EO13526	Executive Order 13526
EOP	Executive Office of the President
EPIC	El Paso Intelligence Center
FBI	Federal Bureau of Investigation
FIP	Fair Information Practices
FISA	1978 Foreign Intelligence Surveillance Act

FISC	Foreign Intelligence Surveillance Court
FISMA	Federal Information Security Act of 2002
FOIA	Freedom of Information Act
FRCrP	Federal Rules of Criminal Procedure
GAO	Government Accountability Office
GPS	Global Positioning System
HHS	Department of Health and Human Services
HSA	Homeland Security Act of 2002
I&A	Intelligence and Analysis (Department of Homeland Security)
IC	Intelligence Community
ICD 501	Intelligence Community Directive 501 (2009)
IRTPA	Intelligence Reform and Terrorism Protection Act of 2004
ISACs	Information Sharing and Analysis Centers
ISE	Information Sharing Environment
IT	Information Technology
ITACG	Interagency Threat Assessment and Coordination Group
JCS	Joint Chiefs of Staff
JRICs	Joint Regional Intelligence Centers
JSC	Joint Security Commission
JTTFs	Joint Terrorism Task Forces
LEA	Law Enforcement Agency
NARA	National Archives and Records Administration
NCD	Net Centric Diplomacy
NCTC	National Counterterrorism Center
NGA	National Geospatial-Intelligence Agency
NIST	National Institute of Standards and Technology
NOBLE	National Organization of Black Law Enforcement Executives
NOL	NCTC Online
NRC	Nuclear Regulatory Commission
NRO	National Reconnaissance Office
NSA	National Security Agency
NSA	1947 National Security Act
NSC	National Security Council
NSI	Nationwide Suspicious Activity Reporting Initiative
NYPD	New York Police Department
ODNI	Office of the Director of National Intelligence
OIG	Office of the Inspector General, and

OIPR	Office of Intelligence Policy and Review
OMB	Office of Management and Budget
PCLOB	Privacy and Civil Liberties Oversight Board
PIA	Privacy Impact Assessments
PII	Personally Identifiable Information
SAR	Special Access Required
SCI	Sensitive Compartmented Information
SIPA	School of International and Public Affairs at Columbia University
SIPRNET	Secret Internet Protocol Router Network
SVTCs	Secure Video Teleconferences
TIA	Total Information Awareness
TIDE	Terrorist Identities Datamart Environment
TSC	Terrorist Screening Center
TTIC	Terrorist Threat Integration Center
USA Patriot Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001
USCP	U.S. Capitol Police
WITS	Worldwide Incidents Tracking System

[This page is intentionally left blank]

References

"Amnesty et al. v. Clapper: FISA Amendment Act Challenge." *American Civil Liberties Union.* last modified February 12, 2012. http://www.aclu.org/national-security/amnesty-et-al-v-clapper.

Andrus, D. Calvin. "The Wiki and the Blog: Toward a Complex Adaptive Intelligence

Community." *Studies in Intelligence* 49, no.3 (2005).

Babu, A. Ramesh, Y.P. Singh and R.K. Sachdeva, "Establishing a Management Information System," in *Improving Agricultural Extension (A Reference Manual)*, edited by Burton E. Swanson, Robert P. Bentz and Andrew J. Sofranko. Rome: Food and Agriculture Organization of the United Nations, 1998.

Baird, Zoe, and James Barksdale. *Mobilizing Information to Prevent Terrorism: Accelerating Development of a Trusted Information Sharing Environment*. New York: Markle Foundation, 2006.

Baker, Al and William K. Rashbaum. "Police Find Car Bomb in Times Square." *The New York Times*, May 1, 2010. http://www.nytimes.com/2010/05/02/nyregion /02timessquare.html.

Bazan, Elizabeth B. *Assassination Ban and E.O. 12333: A Brief Summary.* Washington, DC: Congressional Research Service, 2002.

Best Jr., Richard A. *Proposals for Intelligence Reform: 1949-2004.* Washington, DC: Congressional Research Service, 2004.

Best Jr., Richard A. *Sharing Law Enforcement and Intelligence Information: The Congressional Role.* Washington, D.C.: Congressional Research Service, 2007.

Bitar, Nabil, Florin Balus, Marc Lasserre, Wim Henderickx, Alcatel Lucent, Yuichi Ikejiri, and Mircea Pisica. "Cloud Networking: Framework and VPN Applicability." *IETF.org*. October 31, 2011. http://datatracker.ietf.org/doc/draft-bitar-datacenter-vpnapplicability/?include_text=1.

Borger, Julian, and David Leigh. "Siprnet: where America stores its secret cables." *The Guardian*. November 28, 2010. http://www.guardian.co.uk/world/2010/nov/ 28/siprnet-america-stores-secret-cables.

"Bradley Manning." *New York Times.* January 12, 2012. http://topics.nytimes.com/ top/reference/timestopics/people/m/bradley_e_manning/index.html.

Bray, David, "Cross-Domain Information Sharing." *Information Sharing Environment*, August 3, 2011. http://ise.gov/blog/david-bray/cross-domain-information-sharing.

Breglio, Nora K. "Leaving FISA Behind: The Need to Return To Warrantless Foreign Intelligence Surveillance." *The Yale Law Journal* (2003): 184.

"British spies help prevent al Qaeda-inspired attack on New York subway," *The Telegraph,* November 09, 2009.

Brodkin, Jon. "Private cloud networks are the future of corporate IT." *Network World*. November 12, 2008. http://www.networkworld.com/news/2008 /111208private-cloud-networks.html.

Burton, Matthew S. "How the Web Can Relieve Our Information Glut and Get Us Talking to Each Other." *Studies in Intelligence* 49 no. 3. (2007).

"Car bomb found in New York's Times Square." *BBC News*, May 2, 2010. http://news.bbc.co.uk/2/hi/8656651.stm.

Censer, Marjorie. "Agencies to look for a 'cloud option'." *Washington Post*. November 22, 2010. http://www.washingtonpost.com/wpdyn/content/article/2010/11/19 /AR2010111906449.html.

Center for Democracy and Technology. *CDT Analysis of Privacy Guidelines for the Information Sharing Environment for Terrorism Information*. February 2, 2007.

Conason, Joe. "Holder Was Right," *The New York Observer*, February 23, 2010. *Concept of Operations (CONOPS) FedRAMP*. Rep. no. 1. *GSA - DOD - DHS - NIST*. http://www.gsa.gov/graphics/staffoffices/FedRAMP_CONOPS.pdf.

Congress. House. 2010. Committee on Armed Services. Oversight and Investigations Subcommittee. National Security: Key Challenges and Solutions to Strengthen Interagency Collaboration. Statement of John H. Pendleton. 111th Cong., 2nd Sess., June 9, 2010.

Congress. House. 2012. Committee on Homeland Security. Counterterrorism and Intelligence Subcommittee. *Federal Government Intelligence Sharing with State, Local and Tribal Law Enforcement: As Assessment Ten Years After 9/11*. Testimony of Maurita J. Bryant. 112th Cong., 2nd Sess., February 28, 2012.

Congress. House. 2012. Committee on Homeland Security. Counterterrorism and Intelligence Subcommittee. *Federal Government Intelligence Sharing with State, local, and Tribal Law Enforcement: An Assessment 10 Years After 9/11*. Testimony by Scott McAllister. 112th Cong., 2nd Sess., February 28, 2012.

Congress. Senate. 2005. Committee on Appropriations. Commerce, Justice, State and the Judiciary Subcommittee. *The Federal Bureau of Investigation's Trilogy Information Technology Modernization Project*. Testimony by Glenn A. Fine. 109th Cong., 1st Sess., February 3, 2005.

Congress. Senate. 2007. Committee on Homeland Security and Governmental Affairs. *E-Government 2.0: Improving Innovation, Collaboration, and Access*. Testimony by Jimmy Wales. 110th Cong., 1st Sess., December 11, 2007.

Congress. Senate. 2008. Committee on Homeland Security and Governmental Affairs. Oversight of Government Management, the Federal Workforce, and the District of Columbia Subcommittee. *Intelligence Reform: GAO Can Assist the Congress and the Intelligence Community on Management Reform Initiatives*. Testimony by David M. Walker. 110th Cong., 2nd Sess., February 29, 2008.

Congress. Senate. 2010. Committee on Intelligence. *Senators Feinstein and Bond Release Declassified Report Detailing Intelligence Failure in the Attempted Christmas Day Bombing of Northwest Airlines Flight 253.* Press release prepared by Intelligence Committee. 111th Cong., 2nd Sess., May 18, 2010.

Congress. Senate. 2011. Committee on Homeland Security & Governmental Affairs. *Ten Years After 9/11: A Status Report on Information Sharing*. Report prepared by Zoe Baird and Jeffrey H. Smith. 112th Cong., 1st sess., October 12, 2011.

Congress. Senate. 2011. Committee on Homeland Security & Governmental Affairs. *Information Sharing in the Era of WikiLeaks: Balancing Security and Collaboration.* Statement on behalf of the Markle Task Force on National Security in the Information Age. 112th Cong., 1st sess., 2011.

Crump, George. "Big Data Changes Storage Needs." *InformationWeek*. January 13, 2012. http://www.informationweek.com/news/storage/systems/232400330.

Crump, George. "How To Manage The Collaborative Cloud." *InformationWeek*. June 17, 2011. http://www.informationweek.com/news/storage/systems/230800139.

Cummings, Julian. "Najibullah Zazi pleads guilty in New York terrorism plot." *CNN Justice.* February 22, 2010. http://articles.cnn.com/2010-02-22/justice/najibullah.zazi.plea_1_mohammed-wali-zazi-najibullah-zazi-terrorism-plot?_s=PM:CRIME.

"Data Mining: What is Data Mining?" *UCLA Anderson School of Management*. http://www.anderson.ucla.edu/faculty/jason.frand/teacher/technologies/palace/datamining.htm.

Department of Commerce. National Institute of Standards and Technology. "FISMA: Background." August 17, 2010. http://csrc.nist.gov/groups/SMA /fisma/ overview.html.

Department of Commerce. National Institute of Standards and Technology. "FISMA: Detailed Overview." August 17, 2010, http://csrc.nist.gov/groups/SMA/fisma /overview.html.

Department of Commerce. National Institute of Standards and Technology. *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII): Recommendations of the National Institute of Standards and Technology.* Washington, D.C.: Government Printing Office, 2010.

Department of Homeland Security. *Critical Infrastructure Sector Partnerships*. last modified September 12, 2011, http://www.dhs.gov/files/partnerships /editorial_0206.shtm.

Department of Homeland Security. Data Privacy and Integrity Committee. *Report No. 2011-01: Privacy Policy and Technology Recommendations for a Federated Information-Sharing System.* Washington, D.C.: Government Printing Office, 2011.

Department of Homeland Security. Data Privacy and Integrity Advisory Committee. *The Use of Commercial Data to Reduce False Positives in Screening Programs*. Washington, D.C.: Government Printing Office, 2005.

Department of Homeland Security. *Hometown Security*. Last modified March 30, 2012. http://www.dhs.gov/files/programs/hometown.shtm.

Department of Homeland Security. Information Sharing Governance Board. *Department of Homeland Security Information Sharing Strategy*. Washington, DC: Government Printing Office, 2008.

Department of Homeland Security. Publications. *Classified National Security Information Program for State, Local, Tribal and Private Sector Entities Implementing Directive.* Washington, DC: Government Printing Office, 2012.

Department of Homeland Security. *Next Steps: Supporting Community-Based Efforts to Reduce Violent Crime.* Washington, DC: Government Printing Office, 2010.

Department of Justice. Bureau of Justice Assistance. *Guidance for Building Communities of Trust.* By Robert Wasserman. Washington, DC: Government Printing Office, 2010.

Department of Justice. Bureau of Justice Assistance. Program Management Office. *Nationwide SAR Initiative*. Washington, DC: Government Printing Office, 2012.

Department of Justice. Federal Bureau of Investigation. *Fact Sheet: National Criminal Intelligence Sharing Plan*. Washington, DC: Government Printing Office, 2004.

Department of Justice. Federal Bureau of Investigation. *National Information Sharing Strategy 2011.* Washington, DC: Federal Bureau of Investigation, 2011.

Department of Justice. Office of Justice Programs. *Applying Security Practices to Justice Information Sharing.* Washington, DC: Bureau of Justice Assistance, 2004.

Department of Justice. Office of Justice Programs. *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era.* Washington, DC: Bureau of Justice Assistance, 2006.

Department of Justice. Office of the Inspector General Evaluation and Inspections Division. *Review of the Drug Enforcement Administration's El Paso Intelligence Center.* Washington, DC: Government Printing Office, 2010.

Eggen, Dan, and Griff Witte. "The FBI's Upgrade That Wasn't." *The Washington Post*. August 18, 2006. http://www.washingtonpost.com/wp-dyn/content/article/2006/08/17/AR2006081701485_2.html.

Executive Office of the President. Office of Management and Budget. *Memorandum for Chief Intelligence Officers: Security Authorization of Information Systems in Cloud Computing Environments.* By Steven VanRoekel. Washington, DC: Government Printing Office, 2011.

Executive Office of the President. Office of Management and Budget. *Memorandum M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.* Washington, DC: Government Printing Office, 2003.

Executive Order No. 13,388. 70 Fed. Reg. 62023 (October 25th, 2005).

Federal Bureau of Investigation. Reports and Publications. *National Information Sharing Strategy*. Washington, DC: Government Printing Office, 2011.

Foley, John. "FBI's Beleaguered Sentinel Project Delayed Again." *InformationWeek*. January 4, 2012. http://www.informationweek.com/news/government/enterprise-apps/232301261.

"Fusion Center Locations and Contact Information." Department of Homeland Security. March 12, 2012. http://www.dhs.gov/files/programs /gc_1301685827335.shtm.

"'Fusion centers' at a glance." *Los Angeles Times*. November 15, 2010. http://articles.latimes.com/2010/nov/15/nation/la-na-fusion-centers-box-20101115.

General Accounting Office. *Defense Acquisitions: Steps Needed to Ensure Interoperability of Systems That Process Intelligence Data*. GAO-03-329. Washington, DC: General Accounting Office, 2003.

General Accounting Office. *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information*. GAO-06-385. Washington, DC: General Accounting Office, 2006.

General Accounting Office. *Results-Oriented Cultures: Creating a Clear Linkage between Individual Performance and Organizational Success*. GAO-03-488. Washington, DC: General Accounting Office, 2003.

General Accounting Office. *Security Clearances: FBI has Enhanced Its Process for State and Local Law Enforcement Officials.* GAO-04-596. Washington, DC: General Accounting Office, 2004.

German, Mike, and Jay Stanley. "Fusion Center Update." *American Civil Liberties Union,* July 2008. http://www.aclu.org/pdfs/privacy/fusion_update_20080729.pdf.

Goldman, Adam and Matt Apuzzo. "Consequences for security as NYPD-FBI rift widens," *Associated Press*, March 20, 2012.

Goldstein, Harry. "Who Killed the Virtual Case File?" *IEEE Spectrum*. September 2005. http://spectrum.ieee.org/computing/software/who-killed-the-virtual-case-file/0.

Gould, Jeffrey and Larry Ponemon. "Federal IT Managers Embrace Cloud, But Not Cloud-First Mandate," *AOL Government*, January 30, 2012.

Government Accountability Office. *Data Mining: Agencies Have Taken Key Steps to Protect Privacy in Selected Efforts, but Significant Compliance Issues Remain*. GAO-05-866. Washington, DC: Government Printing Office, 2005.

Government Accountability Office. *Data Mining: DHS Needs to Improve Executive Oversight of Systems Supporting Counterterrorism*. GAO-11-742. Washington, DC: Government Printing Office, 2011.

Government Accountability Office. *Data Mining: Early Attention to Privacy in Developing a Key DHS Program Could Reduce Risks*. GAO-07-293. Washington, DC: Government Printing Office, 2007.

Government Accountability Office. *Information Sharing: Federal Agencies Are Helping Fusion Centers Build and Sustain Capabilities and Protect Privacy, but Could Better Measure Results*. GAO-10-972. Washington, DC: Government Printing Office, 2010.

Government Accountability Office. *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information.* GAO-06-385. Washington, DC: Government Printing Office, 2006.

Government Accountability Office. *Key Challenges and Solutions to Strengthen Interagency Collaboration.* GAO-10-822T. Washington, DC: Government Printing Office, 2010.

Grewe, Barbara A. *Legal Barriers to Information Sharing: The Erection of a Wall Between Intelligence and Law Enforcement Investigations.* Washington, DC: Commission on Terrorist Attacks Upon the United States, 2004.

Grimmet, Richard F. *9/11 Commission Recommendations: Implementation Status.* Washington, DC: Congressional Research Service, 2006.

Healey, Michael. "Leap of Cloud Faith." *InformationWeek.* February 6, 2012. http://i.cmpnet.com/infoweek/green/020612/InformationWeek_2012_02_6.pdf.

Hedley, John H. "The Evolution of Intelligence Analysis." *Analyzing Intelligence: Origins, Obstacles.* ed Z. Roger et al. (Washington DC: Georgetown University Press, 2008): 21.

Henry, Samantha. "NJ FBI: NYPD monitoring damaged public trust," *Associated Press*, March 7, 2012.

Hersh, Seymour. "Huge C.I.A. Operation Reported in U.S. Against Antiwar Forces, Other Dissidents in Nixon Years." *The New York Times.* December 22, 1974.

Hickey, Kathleen. "FBI at last ready to go live with Sentinel case management system." *Government Computer News*. March 18, 2011. http://gcn.com/articles/2011/03/18/fbi-sentinel-set-to-go-live.aspx.

Hoover, J. Nicholas. "Cloud Security, Costs Concern Federal IT Pros." *InformationWeek*. January 31, 2012. http://www.informationweek.com/news /government/cloud-saas/232500801.

Hoover, J. Nicholas. "Federal Standards Body Focuses On Big Data." *InformationWeek*. February 7, 2012. http://www.informationweek.com/news /government/policy/232600419.

Hoover, J. Nicholas. "GSA Details Federal Cloud Security Program." *InformationWeek*. February 8, 2012. http://www.informationweek.com/news/government/cloud-saas/232600484.

"How and Why We Do It." National Counterterrorism Center. *About Us.* http://nctc.gov/about_us/how_we_do.html

Howard, Newton, and Sergey Kanareykin. "Analysis of Federated and Centralized Information Sharing Architectures." *Center for Advanced Defense Studies,* 2007. http://www.c4ads.org/sites/default/files/Federated%20vs%20Centralized.pdf.

"Inside the Zazi Takedown." *Newsweek*. September 25, 2009. http://www.thedailybeast.com/newsweek/2009/09/26/inside-the-zazi-takedown.html.

Jackson, Brian A., ed. *The Challenge of Domestic Intelligence in a Free Society*. Santa Monica: RAND Corporation, 2009.

Johnson, Nicole. "FBI's Sentinel project $100 Million over budget, 2 Years behind schedule." *Federal Times.* October 20, 2010. http://www.federaltimes.com/article/20101020/IT04/10200302/1001.

Jones, Calvert. "Intelligence Reform: The Logic of Information Sharing." *Intelligence and National Security* (2007): 392.

Jones, Jason B. "The Necessity of Federal Intelligence Sharing with Sub-Federal Agencies." *Texas Review of Law and Politics* (2011): 192.

Kaplan, Eben. "Fusion Centers." *Council on Foreign Relations.* February 27, 2007. http://www.cfr.org/intelligence/fusion-centers/p12689.

Kean, Thomas H. et al. *The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States.* Washington, DC: U.S. Government Printing Office, 2004.

"Key Partners." National Counterterrorism Center. *About Us*. http://nctc.gov/about_us/key_partners.html.

Knorr, Eric, and Galen Gruman. "What Cloud Computing Really Means." *InfoWorld*. April 7, 2008. http://www.infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031.

Kris, David S. "The Rise and Fall of the FISA Wall." *Stanford Law and Policy Review* 17 (2006): 487-529.

Krolicki, Kelvin and Jeremy Pelofsky. "Nigerian charged for trying to blow up U.S. airliner." *Reuters*, December 26, 2009.

Landau, Susan. "National Security on the Line." *Journal of Telecommunication and High Technology Law* vol. 4, no. 2 (2006): 416. http://ssrn.com/abstract=1166155.

Lewis, James A. "Significant Cyber Incidents Since 2006." *Center for Strategic and International Studies*, April 10, 2012. http://csis.org/files/publication/120316_Significant_Cyber_Incidents.pdf.

Library of Congress. Congressional Research Service. *Privacy and Civil Liberties Oversight Board: New Independent Agency Status*, by Garret Hatch. CRS Report RL34385. Washington, DC: Office of Congressional Information and Publishing, November 14, 2011.

Library of Congress. Congressional Research Service. *Sharing Law Enforcement and Intelligence Information: The Congressional Role,* by Richard A. Best Jr. CRS Report RL33873. Washington, DC: Office of Congressional Information and Publishing, February 13, 2007.

Library of Congress. Congressional Research Service. *Terrorism Information Sharing and the Nationwide Suspicious Activity Report Initiative: Background and Issues for Congress*, by Jerome P. Bjelopera. CRS Report R40901. Washington, DC: Office of Congressional Information and Publishing, June 10, 2011.

Library of Congress. Congressional Research Service. *The Federal Bureau of Investigation and Terrorism Investigations*, by Jerome P. Bjelopera. CRS Report R41780. Washington, DC: Office of Congressional Information and Publishing, December 28, 2011.

Library of Congress. Congressional Research Service. *The National Counterterrorism Center (NCTC) – Responsibilities and Potential Congressional Concerns*, by Richard A. Best Jr. CRS Report R41022. Washington, DC: Office of Congressional Information and Publishing, December 19, 2011.

Linthicum, David. "How to Revive the Feds' Lifeless 'cloud First' Policy " *InfoWorld*. October 27, 2011. http://www.infoworld.com/d/cloud-computing/how-revive-the-feds-lifeless-cloud-first policy-177056.

Madsen, Paul. "Understanding OAuth and Securing Cloud APIs." *FBI.* CSI Webinars, February 24, 2011. http://gocsi.com/Webinars.

"Meeting the Threat of Terrorism: Culture Change: New Thinking on Information Sharing Critical to Strengthening National Security." *Markle Foundation*, September 1, 2009.

"Meeting the Threat of Terrorism: Improve Information Sharing, Create a Trusted System, Facilitate Access to Critical Data." *Markle Foundation,* September 1, 2009.

"Meeting the Threat of Terrorism: Protecting Privacy and Civil Liberties in a Networked Information Sharing Environment." *Markle Foundation*, July 1, 2009.

"Mission." National Security Agency Central Security Service. last modified April 15, 2011. http://www.nsa.gov/about/mission/index.shtml.

Montalbano, Elizabeth. "Feds Refine Cloud Security Standards." *InformationWeek*. January 10, 2012. http://www.informationweek.com/news/government/security /232400086.

Montalbano, Elizabeth. "State, Local Governments Face Cloud Imperative." *InformationWeek*. February 16, 2012. http://www.informationweek.com/news/ government/cloud-saas/232601033.

Naamani-Goldman, Dalia. "Anti-terrorism program mines IRS' records," *The Los Angeles Times*, January 15, 2007.

National Archives and Research Administration. *2011 Report to the President: Controlled Unclassified Information.* Washington, DC: Government Printing Office, 2011.

National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. Washington, DC: Government Printing Office, 2004.

"National Council of ISACS." *ISACCouncil.org.* Last modified March 30, 2012. http://www.isaccouncil.org/index.php?option=com_content&view=article&id=83&Itemid=195.

New York Police Department. Domain Awareness System. *Public Security Privacy Guidelines.* NYC, NY: New York Police Department, 2009.

New York Police Department. *Counterterrorism Units.* NYC, NY: New York Police Department, 2012.

"NSA Multi-District Litigation." *Electronic Frontier Foundation*, last modified July 1, 2010. https://www.eff.org/cases/nsa-multi-district-litigation.

Office of the Director of National Intelligence. *Intelligence Community Directive Number 206: Sourcing Requirements for Disseminated Analytic Products.* Washington, DC: Government Printing Office, 2006.

Office of the Director of National Intelligence. *Intelligence Community Directive Number 501: Discovery and Dissemination or Retrieval of Information within the Intelligence Community.* Washington, DC: Government Printing Office, 2009.

Office of the Director of National Intelligence. *Intelligence Community Directive Number 651: Performance Management System Requirements for the Intelligence Community Civilian Workforce.* Washington, DC: Government Printing Office, 2008.

Office of the Director of National Intelligence. National Counterterrorism Center. *Guidelines for Access, Retention, Use and Dissemination by the National Counterterrorism Center and Other Agencies of Information in Datasets Containing Non-Terrorism Information*. Washington, DC: Government Printing Office, 2012.

Office of the Director of National Intelligence. National Counterterrorism Center. *NCTC and Information Sharing: Five Years Since 9/11: A Progress Report*. Washington, DC: Government Printing Office, 2006.

Office of the Director of National Intelligence. *United States Intelligence Community Information Sharing Strategy.* Washington, DC: Government Printing Office, 2008.

Paige Jr., Emmet. "The Rapid Expansion of Intelink." *Federation of American Scientists*. June 11, 1996. ttp://www.fas.org/irp/program/disseminate/di1166.htm.

"Police examining video from Times Square." *CNN Justice,* May 2, 2010. http://articles.cnn.com/2010-05-02/justice/times.square.closure_1_detonated-times-square-area-bomb-making?_s=PM:CRIME.

"Principles for Government Data Mining: Preserving Civil Liberties in the Information Age." *The Constitution Project.* 2010.

"Privacy and Civil Liberties Oversight Board Seats Remain Vacant." *The Markle Foundation.* last modified April 15, 2011. http://www.markle.org/news-events/connected-world-blog/privacy-and-civil-liberties-oversight-board-seats-remain-vacant.

Rahavy, Shana K. "The Federal Wiretap Act: the Permissible Scope of Eavesdropping in the Family Home." *Journal of High Technology Law* (2003): 88.

Rashbaum, William K. and Al Baker. "How Using Imam in Terror Inquiry Backfired on Police," *The New York Times*, September 23, 2009.

Rashbaum, William K. "Interagency Rift Cited in New York Terror Case," *The New York Times*, December 14, 2009.

"Re: Creation of a Federated Information-Sharing System." *American Civil Liberties Union.* November 16, 2011.

Rittgers, David. "We're All Terrorists Now." *Cato Institute.* February 2, 2011. http://www.cato-at-liberty.org/we%E2%80%99re-all-terrorists-now/.

Sales, Nathan Alexander. "Share and Share Alike: Intelligence Agencies and Information Sharing." *The George Washington Law Review* (2010): 281.

Savage, Charlie. "U.S. Relaxes Limits on Use of Data in Terror Analysis," *The New York Times*, March 22, 2012.

Schmitt, Eric. "Director of National Counterterrorism Center is Resigning." *New York Times*. June 09, 2011. http://www.nytimes.com/2011/06/10/us/politics/ 10leiter.html.

Steiner, Barry H. "Policy Organization in American Security Affairs: An Assessment." *Public Administration Review* (1977): 359.

Stevenson, Charles A. "Underlying Assumptions of the National Security Act of 1947." *Joint Force Quarterly*, no. 48 (2008): 129-33. http://www.ndu.edu/press /lib/pdf/jfq-48/JFQ-48.pdf.

Shumacher, Scott. "How to Preserve Security and Autonomy While Meeting Information-Sharing Directives." *ISACA Journal* 6 (2009): 1-2.

Sulzberger, A. G. "Imam Snared in Terror Plot Admits He Lied to the F.B.I." *The New York Times.* March 4, 2010. http://www.nytimes.com/2010/03/05/nyregion/ 05terror.html.

Task Force on Controlled Unclassified Information. *Report and Recommendations of the Presidential Task Force on Controlled Unclassified Information.* Washington, DC: Government Printing Office, 2009.

"The Cloud Imperative: Better Collaboration Better Service Better Cost." *TechAmerica.org*. February 2012. http://www.techamerica.org/Docs/ fileManager.cfm?f=taf_slg_cc.pdf.

Travers, Russell. "Information Sharing, Dot Connecting and Intelligence Failures: Revisiting Conventional Wisdom." submitted to the Director of National Intelligence 2009 Galileo Awards Program. Washington, DC: August 2009.

Treverton, Gregory F. "Reorganizing U.S. Domestic Intelligence: Assessing the Options." (Santa Monica: RAND Corporation, 2008): 8. http://www.rand.org/pubs /monographs/MG767.

"Top Secret America: New York." *The Washington Post*. 2012. http://projects.washingtonpost.com/top-secret-america/states/new-york/.

Warner, Michael. "Legal Echoes: The National Security Act of 1947 and the Intelligence Reform and Terrorism Prevention Act of 2004." *Stanford Law and Policy Review* 17, no. 2 (2006): 303.

"What is ISE?" Information Sharing Environment. *About ISE.* http://ise.gov/what-ise.

"What We Do." National Counterterrorism Center. *About Us.* http://www.nctc.gov/ about_us/what_we_do.html.

White House. *25 Point Implementation Plan to Reform Federal Information Technology Management,* by Vivek Kundra. Washington, DC: Government Printing Office, December 9, 2010.

White House. *Federal Cloud Computing Strategy*, by Vivek Kundra. Washington, DC: Government Printing Office, February 8, 2011.

White House. Information Sharing Environment. *2011 ISE Annual Report to the Congress.* Washington, DC: Government Printing Office, June 30, 2011.

White House. Information Sharing Environment. *Civil Rights and Civil Liberties Protections.* Washington, DC: Government Printing Office, 2008.

White House. Information Sharing Environment. *Feasibility Report: Report for the Congress of the United States.* Washington, DC: Government Printing Office, March 2008.

White House. Information Sharing Environment. *Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment*. Washington, DC: Government Printing Office, 2006.

White House. Information Sharing Environment. *Information Sharing Environment Guidance (ISE-G): Federal Resource Allocation Criteria (RAC)*. ISE-G-112. Washington, DC: Government Printing Office, 2011.

White House. National Security Council. *National Strategy for Information Sharing*. Washington, DC: Government Printing Office, October 2007.

White House. Office of the Press Secretary. *Classified Information and Controlled Unclassified Information.* Washington, DC: Government Printing Office, 2009.

Wilkers, Ross. "Report: FedRAMP Testing Starting in June." *ExecutiveGov.* March 21, 2012. http://www.executivegov.com/2012/03/report-fedramp-testing-starting-in-june/.

Wilson, Michael. "From Smiling Coffee Vendor to Terror Suspect," *The New York Times,* September 25, 2009.