UNITED STATES INTELLIGENCE COMMUNITY

INFORMATION SHARING STRATEGY

FEBRUARY 22, 2008

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
E PLURIBUS
UNUM
UNITED STATES OF AMERICA

TABLE OF CONTENTS

Message from the Director of National Intelligence.....2

Message from the Associate Director of National Intelligence.....2

Introduction.....3

Challenging New Environment.....5

Information Sharing Strategy.....9

Implementing Our Strategy.....15

Appendix - List of Acronyms.....20

Policy Law Enforcement Joint Intelligence Analysis
Military Defense Military Defense Military Defense Military
Intelligence Community
Congress Collaboration Information Sharing Steering Committee

MESSAGE FROM THE DIRECTOR OF NATIONAL INTELLIGENCE

This is an extremely dynamic time for the Intelligence Community and we have the privilege to lead its transformation. With this responsibility, we made information sharing a top priority in our strategic agenda for change. Information sharing must improve since it is central to our ability to anticipate and deter the ill intentions of our Nation's adversaries. Improving information sharing will bring about true all-source analysis and deliver timely, objective, and actionable intelligence to our senior decision makers, war fighters, and defenders of the homeland. This strategy—by detailing information sharing strategic keystones, goals, and objectives—provides vital direction to our efforts to effect these changes. Together, we must challenge the status quo of a "need-to-know" culture and move to one of a "responsibility to provide" mindset. Implementing this strategy will enable intelligence entities to act as stewards of intelligence data and take advantage of every opportunity to share information that can improve the security of our Nation.

J. M. McConnell
Director of National Intelligence

MESSAGE FROM THE INTELLIGENCE COMMUNITY INFORMATION SHARING EXECUTIVE

Information sharing is a principal component of the DNI's strategy for improving the Intelligence Community's ability to overcome the new challenging threat environment that we face as a Nation. This document outlines a forward-leaning information sharing strategy to enhance our capability to operate as a unified, integrated intelligence enterprise. The information sharing strategy is focused on developing a "responsibility to provide" culture in which we unlock intelligence data from a fragmented information technology infrastructure spanning multiple intelligence agencies and make it readily discoverable and accessible from the earliest point at which an analyst can add value. This new information sharing model will rely on attribute-based access and tagged data with security built-in to create a trusted environment for collaboration among intelligence professionals to share their expertise and knowledge. Moreover, we should reiterate our commitment to develop a risk management approach where we carefully contemplate anticipated benefits and potential costs, ensuring mission success and protection of privacy, civil liberties, and sources and methods. As we embark on this challenging endeavor, we look forward to working collaboratively with you to implement this strategy's information sharing strategic goals and objectives in a manner that benefits the Intelligence Community as one enterprise.

Dale Meyerrose
Associate Director of National Intelligence and Chief Information Officer
Intelligence Community Information Sharing Executive

INTRODUCTION

The need to share information became an imperative to protect our Nation in the aftermath of the 9/11 attacks on our homeland. The Intelligence Community's "need-to-know" culture, a necessity during the Cold War, is now a handicap that threatens our ability to uncover, respond, and protect against terrorism and other asymmetric threats. Each intelligence agency has its own networks and data repositories that make it very difficult to piece together facts and suppositions that, in the aggregate, could provide warning of the intentions of our adversaries. The inability or unwillingness to share information was recognized as an Intelligence Community weakness by both the 9/11 Commission and the Weapons of Mass Destruction (WMD) Commission. The President and the Congress have mandated that the Intelligence Community create a more integrated enterprise where information is routinely shared. Since these mandates were issued, progress has been made in information sharing, realized through the stand up of the National Counterterrorism Center (NCTC), the Information Sharing Environment (ISE), and related partnership efforts. These endeavors, though proving to be excellent in facilitating greater information sharing, are the "tip of the iceberg" and continued focus on "accelerating information sharing" is needed. Simultaneously, consumers must protect the information made available to them.

> "I've asked [Director McConnell] to improve information sharing within the intelligence community and with officials at all levels of our government, so everyone responsible for the security of our communities has the intelligence they need to do their jobs."
> – President George W. Bush

Recognizing the very real and profound necessity to improve information sharing, the Director of National Intelligence (DNI) has made accelerating and improving Intelligence Community information sharing one of his top priorities. The DNI has called on the Intelligence Community to transform its culture to one where the "responsibility to provide" information is a core tenet.

A central principle is the recognition that information sharing is a behavior and not a technology. In the Intelligence Community, information sharing behavior is the act of exchanging intelligence information between collectors, analysts, and end users in order to improve national and homeland security. Information providers must make information accessible, available, and discoverable at the earliest point possible.

Policy Law Enforcement Joint Intelligence Analysis
Military Defense Military Defense Military Defense Military
Intelligence Community
Congress Collaboration Information Sharing Steering Committee

While technical improvements can enable information sharing, technical solutions alone are not enough. The goal is to transform the Community in a way that results in much greater and more effective communication between the participants in the national security community – communication that improves the quality, applicability, and usage of the results of the intelligence process.

This document lays out a strategy to establish this new culture and to share information better, both among those whose job it is to provide intelligence and with those who need intelligence to perform their missions—i.e., policy makers, war fighters, defenders of the homeland, and the officials who enforce our laws. Time is of the essence. Improvements must be made rapidly to build on recent progress and improve our ability to thwart the plans of our enemies and protect our values, people, institutions, and assets. This document outlines:

- ***Challenging New Environment.*** This section shows that a profound mandate for change exists: (1) Externally, new and evolving threats must be addressed to ensure the Nation's security; (2) Internally, the President intends for the DNI to create a more integrated and collaborative enterprise. Here we also examine the need to manage risk, considering both the need to satisfy national security and mission requirements and the need to protect against unauthorized disclosure of sensitive information that could jeopardize sources and methods, endanger privacy and civil liberties, or reveal our intentions to adversaries.
- ***Information Sharing Strategy.*** This section communicates our information sharing vision and outlines its key elements, describes the envisioned outcomes, and communicates our strategic intent in a clear and succinct manner. The strategic keystones describe the principles around which we have designed our strategy and are those that will be adhered to as the information sharing model evolves in the Intelligence Community. Finally, the strategic goals and objectives are defined to guide information sharing efforts moving forward. The goals articulate the outcomes to be achieved over the long term and the objectives are the discrete actions to be taken to attain their respective goals.
- ***Implementing Our Strategy.*** This section discusses challenges to overcome in order to improve information sharing and how the use of five building blocks— governance, policy, technology, culture, and economics—can guide efforts to overcome those challenges. It then describes our forthcoming implementation roadmap and outlines the immediate tactical plan mapped to the 500 Day Plan. Also, we discuss the role of the Intelligence Community Information Sharing Steering Committee. Finally, alignment to key information sharing initiatives is identified and we reiterate our commitment to continue our collaboration with them.

CHALLENGING NEW ENVIRONMENT

MANDATE FOR CHANGE

Information sharing is a key element in the Intelligence Community's transformation to provide better support for our Nation's protection. The major factors driving the need for change are the changing threat environment, new national and homeland security customers, and emerging threats that require synthesizing intelligence from a greater variety of sources. These key factors influence the future direction of information sharing in the Intelligence Community and will affect the modus operandi of the intelligence apparatus in the United States.

THE NEW AND EVOLVING THREAT

The tragic events of September 11, 2001, demonstrated that the United States needed greater integration across the Intelligence Community and improved information sharing to respond to evolving threats and to support new homeland security customers. The new threat environment we face is dynamic: The players and their motivations and methods emerge and evolve rapidly. Advances in technology are accelerating and are spreading through globalization. Commercial products featuring state-of-the-art technology are available globally at favorable prices. Our adversaries achieve technological advantage through the rapid assimilation and adaptation of commercial information and telecommunication products. They freely communicate, obtain training, share information on tactics, gather intelligence on potential targets, spread propaganda, and proselytize. In this post-9/11 world, intelligence must move faster and leverage all sources of intelligence information.

IMPERATIVES TO TRANSFORM THE INTELLIGENCE COMMUNITY

Since September 11, 2001, the President, the Congress, independent commissions, and think tanks have placed greater emphasis on transforming the Intelligence Community to address the new threat environment. Paramount to that effort is the need for greater information sharing within the Intelligence Community in support of national policy makers, the military, state and local law enforcement, homeland security, and our allies.

- Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA): Requires the Director of National Intelligence (DNI) to ensure maximum availability of and access to intelligence information within the Intelligence Community consistent with national security requirements. The statute also calls for protecting sources and methods in the context of maximizing the dissemination of intelligence information following DNI-established guidelines for classification, retrieval (in the form when initially gathered through finished products), and writing products at the lowest classification possible to support customers.
- The 9/11 Commission Report: Emphasizes the need to change the mindset from "need-to-know" to "need to share." Moreover, it places the DNI as the principal change agent in creating a culture within the Intelligence Community focused on data "stewardship" rather than data "ownership." The 9/11 Commission challenges the concepts of "originator controlled" (ORCON) adopted by collectors, which inhibits information dissemination and sharing and creates diffused information ownership and inconsistent access standards.
- Executive Orders (13311, 13356, 13388, and others): Direct that agencies be held accountable for sharing information and promptly grant access to their terrorism information to other agencies with counterterrorism functions, and in conducting these activities, protect the freedom, information privacy, and other legal rights of Americans.
- Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (WMD Report): Provides multiple recommendations endorsed by the President to improve information sharing beyond those outlined in the IRTPA. The WMD Report calls for the establishment of a Chief Information Management Officer responsible for information sharing, information security, and information technology. The Report asserts that the risk of not sharing should be balanced with the need to protect classified sources and methods. The Commissioners also recommend improvements related to a networked environment, including identity management with attribute-based access, user authorization and audits, encryption of stored data, and universal discovery. Further, they recommend uniform information sharing policy, practices, procedures, and rules for accessing "U.S. persons" information. Finally, the Commissioners recommend simplified classification rules and tagging data for security and content to ease discovery and retrieval.

AN INTEGRATED INTELLIGENCE ENTERPRISE

In today's dynamic environment, it is imperative that all participants exchange information expeditiously and precisely. Intelligence Community personnel need to understand where and why information is needed. Analysts and collectors need to be able to piece fragments of information together from all intelligence sources. Intelligence consumers need to interact with the Intelligence Community to focus intelligence on the specific problems at hand. Moreover, in today's environment the traditional lines between foreign and domestic, strategic and tactical, intelligence and operations, and customer and producer are blurring, creating an imperative to improve integration between National and Departmental intelligence programs. Meeting these needs requires development of a culture that values sharing information with those who need it, and providing them with the training, policies, laws, processes, and information technologies necessary to distribute their knowledge.

An integrated intelligence enterprise promises an environment to counter the threats we currently face, to adapt rapidly to these threats as they change over time, and to address new threats as they emerge. The information component of an integrated enterprise promises development of better and more timely intelligence. Intelligence Community participants shall have access to all appropriate information that they are authorized to see—no matter where it is in the intelligence information life cycle—as well as the tools that they need to make use of the information. Automation will enhance human performance, scouring information streams and repositories to uncover information more efficiently than humans can and discovering, filtering, and delivering the knowledge that users need while guarding against information overload. The members of the Intelligence Community and its customers will be able to find and meaningfully engage each other. A risk management approach will protect (1) sources and methods as well as sensitive information from unauthorized disclosure; (2) information and infrastructure from being compromised, damaged, destroyed, or lost whether it be by attack, error, or negligence; and (3) privacy and civil liberties of U.S. persons. The President also has called for the creation of an integrated intelligence enterprise.

MANAGING RISK – MISSION EFFECTIVENESS AND INFORMATION SECURITY

One of the key challenges moving forward with improved information sharing will be managing risk – appropriately considering the importance of both mission effectiveness and information protection. There exists a "dynamic tension" in our culture between the benefits of making information available and the risk that unauthorized disclosure of sensitive information could jeopardize sources and methods, endanger privacy and civil liberties, or reveal our intentions to adversaries.

A new culture of collaboration and risk management will require that people and organizations understand and trust how their partners manage risk. We will need a uniform trust model across the Intelligence Community.

Since the National Security Act was signed in 1947, the U.S. Intelligence Community has worked under a "need-to-know" mindset where protection of sources and methods was foremost. This protective mindset was based primarily on two factors: (1) the need to minimize the risk of inadvertent disclosure of sensitive information to the "wrong hands," and (2) to protect the sources and methods to minimize any compromises in clandestine or sensitive technical collection capabilities or analytic techniques.

In today's environment, the risks associated with not sharing can lead to missing clues of an attack, cost lives, and endanger our Nation's security. This new environment requires the Intelligence Community to move to a "responsibility to provide" culture to ensure all members of the Community can retrieve the information they need and effectively support intelligence customers. The "responsibility to provide" culture is predicated on managing risks associated with mission effectiveness and unauthorized disclosure of sensitive information.

Information Sharing Strategy

INFORMATION SHARING STRATEGY

There is an urgent need to transform intelligence information sharing in the Intelligence Community. The information sharing strategy must overcome the systemic issues that have accumulated over more than half a century. The information sharing strategy outlined below will evaluate where we are and outline how we achieve information sharing across all missions.

INFORMATION SHARING VISION

Intelligence Community Information Sharing Vision

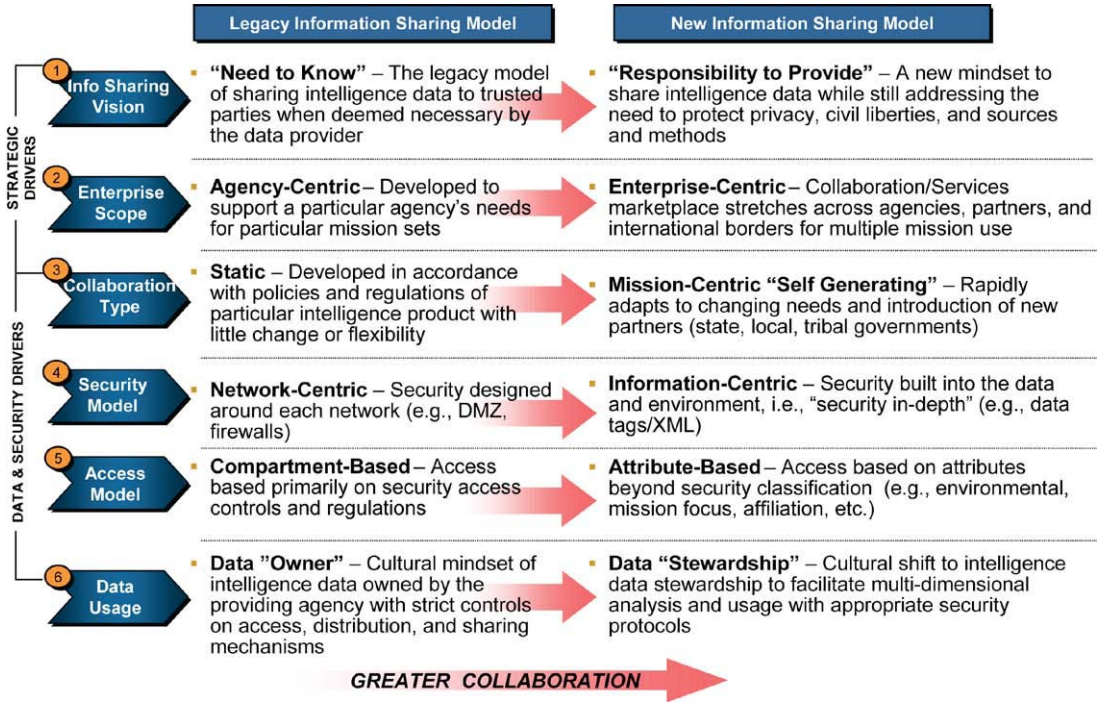
Shared Information • Deeper Knowledge • Improved Security

An integrated intelligence enterprise that anticipates mission needs for information by making the complete spectrum of intelligence information seamlessly available to support all stages of the intelligence process.

The Intelligence Community information sharing end-state is a common trust and information environment, wherein all intelligence information is discoverable and mission accessible. In this new environment, the same information is available to all appropriately authorized parties allowing them to perform truly competitive and collaborative analyses.

To achieve our information sharing vision, we adopted a new information sharing model, which is depicted in Figure 1.

Figure 1. New Information Sharing Model



The new information sharing model will emphasize a "responsibility to provide" culture and an Intelligence Community-wide enterprise perspective. Inherent in moving towards greater sharing will be the establishment of a trust environment with attribute-based access and security built into the data and the environment. Intelligence Community stakeholders will be able to share intelligence information with greater confidence for multiple mission objectives while managing the risks associated with inadvertent disclosure of intelligence information. Ultimately, the new information sharing model will foster greater collaboration among Intelligence Community stakeholders and partners.

STRATEGIC KEYSTONES

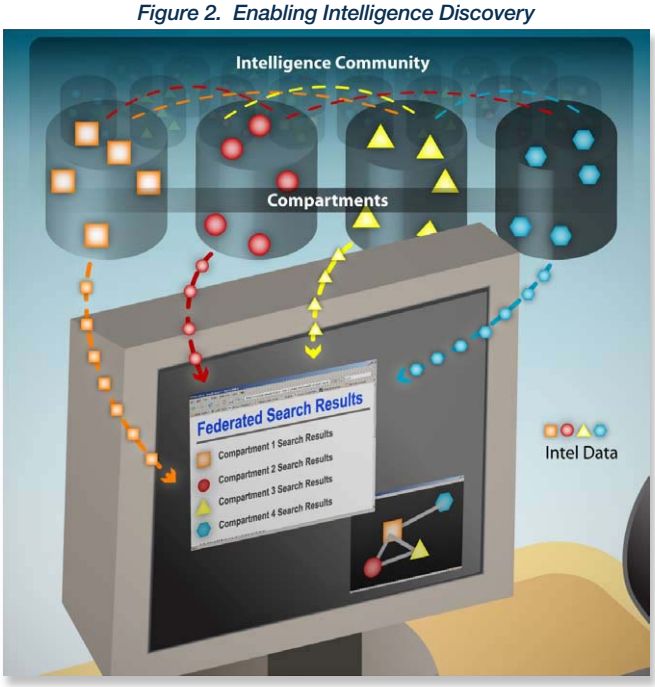
True information sharing ensures that all participants in the intelligence cycle supporting collection, analysis, dissemination, and feedback have the information they need when they need it. Members of the Intelligence Community must be able to discover the existence of information and retrieve relevant information when needed. Analytic organizations supporting senior decision makers must have the means to understand the implications of the most sensitive information when creating a product. The information itself must be available through an accessible Intelligence Community infrastructure that supports information discovery, retrieval, and collaboration. The following strategic keystones are necessary underpinnings to meet these objectives:

Keystone #1: Intelligence Information Retrieval and Dissemination Moves Toward Maximizing Availability

The Intelligence Community must "ensure the maximum availability of and access to intelligence information within the Intelligence Community consistent with national security requirements." Our strategy must support retrieval and dissemination from the point of initial collection through the resulting product. Maximizing access and dissemination must occur using a managed risk approach, managing the risk of not satisfying mission needs against the risk of unauthorized disclosure of intelligence information, including sources and methods, and the protection of privacy and civil liberties.

Keystone #2: All Intelligence is Discoverable, and All Intelligence is Accessible by Mission

Figure 2. Enabling Intelligence Discovery



The Intelligence Community collects a vast amount of intelligence information from many sources, information that is difficult to discover or access outside of collection stovepipes. Analysts "don't know what they don't know." They are often unaware that information has been collected. We need to move to a collaborative information environment, where all information is discoverable by Intelligence Community collectors and analysts, relationships between information can be easily discerned, and the people and organizations of an integrated enterprise readily engage one another to synthesize knowledge. The key concept is that regardless of classification or compartment, intelligence analysts and collectors can be aware of the existence of all intelligence information. Analysts and collectors could access and retrieve relevant information based upon mission need. The information could be directly retrievable, provided to an authorized user within the analyst's organization, provided to the analyst as a sanitized product, or made available after further authorization. Discovery of all information allows the uncovering of information having a relationship to other data, providing a better opportunity to "connect the dots."

Keystone #3: Sharing Requires Greater Trust and Understanding of Mission Imperatives

The "need-to-know" culture led to practices that inhibit information sharing today. Multiple organizations establish their own classification rules and procedures, resulting in inconsistent use and understanding of security markings. Differing requirements for access and certification and accreditation inhibit trust across the Intelligence Community agencies. The key concepts are the need for consistent certification and accreditation practices, uniform information security standards, and uniformity across the Intelligence Community for accessing data to enable information sharing. Information users' confidence in the information itself and, conversely, information providers' confidence in who has access to the information, how the information will be protected, and how the information will be used are all essential elements of the trust model. The information sharing strategy must address these issues, as well as attribute-based access, automated user authorization and auditing, and security at the data-level to enable a trust-based model for the free-flow of information among participants.

Keystone #4: Developing a Culture that Rewards Information Sharing is Central to Changing Behaviors

Changing the culture to one that naturally encourages the responsible sharing of information is fundamental to success. Training must increase the emphasis on the "responsibility to provide" while understanding the implications of the protection of sources and methods, privacy, and civil liberties within that responsibility. If Intelligence Community personnel perceive that their professional success is based in part on how well they share information, sharing will improve. The Write for Release Policy (WFR) is a critical technique to encourage the sharing of information with Intelligence Community customers. By promoting award mechanisms for sharing information, analysts and collectors will demand that obstacles be removed and they will welcome better tools that help them succeed.

Keystone #5: Creating a Single Information Environment (SIE) Will Enable Improved Information Sharing

The SIE will improve how the Intelligence Community manages transactions, information, and knowledge and will open the door for new collaboration opportunities and improved analytic practices. The fragmentation of the Intelligence Community information infrastructure has led to additional costs, inefficient operations, and stovepiped solutions that limit mission effectiveness. Common information standards and core services will enable search and discovery across disciplines.

STRATEGIC GOALS AND OBJECTIVES

In December 2006, the Associate Director of National Intelligence and Chief Information Officer (ADNI CIO) issued his Strategic Intent highlighting information sharing as a strategic goal for the next two years. This information sharing strategy continues that original direction by evolving and solidifying the key strategic goals for information sharing on which the Intelligence Community must focus in the years ahead. These strategic goals should be viewed as long-term with their attainment as an indicator of successfully meeting our information sharing objective.

Table 1. Information Sharing Strategic Goals

Strategic Goal	Description
Goal #1: Institute Uniform Information Sharing Policy and Governance	Enable the transformation of culture necessary for information sharing: policies, governance models, standards, personnel evaluation and awards, and compliance mechanisms.
Goal #2: Advance Universal Information Discovery and Retrieval	Advance information search, discovery, retrieval, dissemination, and pervasive connectivity through common metadata tagging, security markings, and networks throughout the Intelligence Community.
Goal #3: Establish a Common Trust Environment	Put in place uniform identity attributes, identity management, information security standards, information access rules, user authorization, auditing, and access control to promote common trust.
Goal #4: Enhance Collaboration Across the Community	Develop the tools and incentives necessary at the institutional, leadership, and workforce levels to collaborate and share knowledge and expertise and information.

Each information-sharing goal is designed to be specific enough to achieve, attainable to avoid overreaching, targeted on our desired outcomes, and measurable so that we can determine progress. We realize that success requires collaboration with Intelligence Community collection, analysis, and personnel security authorities on policies, procedures, and standards to support these information sharing goals and objectives.

For each Strategic Goal, we have defined Strategic Objectives, which are clear descriptions of the main actions that we must take to achieve each goal. They are designed to be the “bridges” that take us from where we are today to where we want to be. In the following sections, we provide the information sharing strategic goals and their associated strategic objectives.

Strategic Goal #1: Institute Uniform Information Sharing Policy and Governance

This goal focuses on bringing to bear a new rule set for information sharing in the Intelligence Community via official policy, guidance, and oversight to create standardization and uniformity. We will implement the following Strategic Objectives to achieve Uniform Information Sharing Policy and Governance:

- Develop a policy framework to increase information sharing across the Intelligence Community and with external partners and customers.
- Establish governance mechanisms to instill common practices for intelligence classification, clearance processing, and policy and standards compliance.
- Reduce risks to civil liberty and privacy infractions from greater information sharing.
- Ensure policy implementation through institutionalized training programs and standards for information sharing policies and procedures.
- Resolve information sharing disputes.

Strategic Goal #2: Advance Universal Information Discovery and Retrieval

This goal focuses on improving intelligence information discoverability, accessibility, and availability based on common tagging, retrieval, and dissemination standards applied across the Intelligence Community. We will implement the following Strategic Objectives to Advance Universal Information Discovery and Retrieval:

- Define common metadata tagging standards for intelligence information to achieve discovery, search, and retrieval objectives.
- Establish “universal discovery” processes, procedures, standards, and tools to support intelligence information transparency.
- Develop retrieval protocols to intelligence information repositories based on analytical focus, mission needs, and identity attributes.
- Integrate Intelligence Community information networks at each security level.

Strategic Goal #3: Establish a Common Trust Environment

This goal focuses on establishing a common trust environment to engender the free-flow of intelligence information among Intelligence Community participants based on their identity attributes, mission area focus, and affiliations. We will implement the following Strategic Objectives to Establish a Common Trust Environment:

- Define a uniform identity structure and uniform attributes to enable identity management, develop uniform standards and guidance for identity management, and support decentralized, agency-specific implementation.
- Establish identity management standards for authentication, authorization, auditing, and cross-domain services.
- Develop information security policies to support logical and physical data protection efforts.
- Create a common classification guide for the Intelligence Community.
- Establish a risk management approach that supports the common trust and information environment while still protecting sources and methods as well as sensitive information from disclosure.

Strategic Goal #4: Enhance Collaboration Across the Community

This goal focuses on developing incentives (e.g., at the institutional, leadership, and workforce levels) for collaboration among Intelligence Community stakeholders to instill the “responsibility to provide” culture across the Community and to share knowledge and expertise. We will implement the following Strategic Objectives to Enhance Collaboration Across the Community:

- Develop information sharing communication programs to create awareness of a “responsibility to provide” culture.
- Create award and assessment programs to transform the culture from a “need-to-know” to a “responsibility to provide” mindset.
- Serve as an integration point for establishing a virtual collaboration environment to facilitate collaboration and information sharing among intelligence professionals (e.g., analysts and collectors).
- Enable the Intelligence Community stakeholders and partners to connect on a time-imperative basis to fulfill their mission requirements.

Implementing Our Strategy

IMPLEMENTING OUR STRATEGY

Executing the information sharing strategy will be an ongoing endeavor with a long-term implementation roadmap and a near-term plan that is continually refreshed in 100-day increments.

There are many challenges that must be overcome to improve information sharing and collaboration. The key will be addressing the root causes of these challenges rather than making cosmetic changes to improve information sharing. For instance, additional liaison officers could improve interagency information sharing but would leave most causes of limited sharing between agencies unaddressed. Solving this problem will require a fundamental rethinking of how to build a trust model for information sharing in which intelligence information users can transparently discover, retrieve, and disseminate intelligence information wherever they sit. We describe the five building blocks that must be touchstones for effective information sharing.

IMPLEMENTATION BUILDING BLOCKS OF INFORMATION SHARING

Information sharing is a wide-ranging, multi-layered issue that spans governance, policy, technology, culture, and economic facets. For information sharing to improve, we must identify and address critical questions about how the Intelligence Community operates in each of these facets. The goal is an evolved information sharing regime that rewards collaboration, promotes uniformity in sharing practices, and increases availability of intelligence data.

INFORMATION SHARING– BUILDING BLOCKS AND KEY QUESTIONS

Figure 3 provides a snapshot of the key questions that were examined while developing the information sharing strategy. As we move forward, these questions must continually be reassessed across the Intelligence Community. Ultimately, to improve information sharing practices in the Intelligence Community, we have to address systemic issues across the enterprise, evolve the Intelligence Community's culture by promoting and recognizing information sharing behaviors, and adopt a risk management approach to information sharing.

Figure 3. Information Sharing– Building Blocks and Key Questions

	Description	Key Questions
Governance The "environment" influencing sharing	Oversight and leadership that help govern information sharing. How managers drive initiatives within organization and across agencies. Standards and guidelines to ensure a consistent approach.	▪ Is there a clear value proposition for sharing among partners, i.e., quid pro quo or negotiated trade-offs? Are MOUs or service-level agreements required? ▪ Do people understand how to abide by the law and policies? ▪ How are information sharing disputes resolved? ▪ Who are the key stakeholders?
Policy The "rules" for sharing	National policies, internal policies, rules of engagement, standards, and role of players internal and external to the organization.	▪ Are laws, regulations, policies, and procedures in place that authorize, mandate and/or enable the organization to share? Is the organization complying with these mandates? ▪ Do laws/regulations/policies/procedures impede or constrain the organization/people from sharing? ▪ Are privacy and civil liberties sufficiently protected?
Technology The "capability" to enable sharing	The technology, systems, and protocols that provide the platform for enabling the sharing of information and that address security and privacy issues.	▪ Are there common data standards and systems for organizing, identifying, and searching? ▪ Can participants push and pull data across networks? ▪ How is information protected; is the system auditable? ▪ Are tools/mechanisms available to manage identities; authorize, authenticate, and audit users; and ensure confidentiality?
Culture The "will" to share	The organizational approach and philosophy around sharing information and its ability to realign and adapt as circumstances change.	▪ How do we motivate people and create incentives to collaborate and share information across organizations? ▪ Does the organization communicate across all levels? ▪ How does the organization adapt to change, and how responsive is it to stresses and opportunities? ▪ How are decisions and conclusions reached?
Economics The "value" of sharing	Ability to obtain and provide resources for information sharing initiatives, and external pressures (e.g., budget) that influence how resources are allocated and managed.	▪ Has sufficient funding been appropriated to support the initiative? ▪ Have incentive structures been developed? ▪ Is the funding reaching the appropriate level within the enterprise to fully implement the sharing program? ▪ How do we measure performance?

IMPLEMENTATION ROADMAP

The forthcoming implementation roadmap will be a long-term plan with a five year time horizon that will guide and synchronize implementation efforts. The implementation roadmap will: (1) include long-term milestones for each strategic goal and objective, (2) define detailed performance measures and metrics at the strategic goal level, (3) assign ownership of information sharing activities among the Intelligence Community members, and (4) outline periodic checkpoints for refreshing the information sharing strategy. This implementation roadmap will provide the overarching framework in which 100-day increments can be developed to ensure tactical efforts are focused and put into action.

NEAR-TERM PLAN: 500 DAY PLAN TO IMPROVE INFORMATION SHARING

The current 500 Day Plan highlights the initiatives and tasks that the Office of the DNI (ODNI) and the Intelligence Community will pursue to transform information sharing. The current 500 Day Plan initiatives for information sharing are closely aligned to our information sharing strategy and will serve as our short-term tactical execution plan to increase information sharing in the Intelligence Community and with our customers. The pertinent areas of the current 500 Day Plan are Focus Area 2: Accelerate Information Sharing, Focus Area 3: Foster Collection and Analytic Transformation, and Focus Area 5: Modernize Business Practices. These and others are mapped to the Strategic Goals outlined in this strategy in the table below.

Table 2. 500 Day Plan Mapping to Information Sharing Strategy

STRATEGIC GOAL	500 DAY PLAN
Goal #1: Institute Uniform Information Sharing Policy and Governance	• Core Initiative: Update Policy Documents Clarifying and Aligning Intelligence Community Authorities • Initiative 5B: Collaborate to Protect Privacy and Civil Liberties • Initiative 6E: Harmonize Intelligence Community Policy on “US Person” Information
Goal #2: Advance Universal Information Discovery and Retrieval	• Initiative 2A: Create a Single Information Environment • Initiative 2B: Implement Attribute-Based Access and Discovery
Goal #3: Establish a Common Trust Environment	• Initiative 2B: Implement Attribute-Based Access and Discovery • Initiative 2D: Establish a Single Community Classification Guide • Initiative 5D: Improve the Information Technology Certification & Accreditation Process
Goal #4: Enhance Collaboration Across the Community	• Core Initiative: Create Collaborative Environment for All Analysts • Initiative 2C: Provide Collaborative Information Technology to Federal Executive Department Agencies and Organizations • Initiative 2D: Establish a Single Community Classification Guide

INTELLIGENCE COMMUNITY COORDINATION

Immediately after his confirmation, Director McConnell established the Intelligence Community Information Sharing Steering Committee to serve as the conduit on information sharing issues within the Intelligence Community. As we implement the Information Sharing Strategy, the Intelligence Community Information Sharing Steering Committee will consider and address information sharing challenges and opportunities and provide a balanced forum to find the best solutions that will benefit the Intelligence Community and stakeholders at-large rather than focused improvements for one agency or department. The Intelligence Community Information Sharing Steering Committee, chaired by the Intelligence Community Information Sharing Executive, has broad representation of members, including each Intelligence Community element, the Under Secretary of Defense for Intelligence, the Joint Chiefs of Staff, and the Assistant Director of National Intelligence for Security.

ALIGNMENT WITH OTHER INFORMATION SHARING EFFORTS

The ODNI recognizes that there are several key government intelligence initiatives focused on improving information sharing and increasing collaboration in the Intelligence Community. Through the Intelligence Community Information Sharing Steering Committee, the ODNI will integrate with these and other information sharing initiatives by leveraging the Information Sharing Environment to take into consideration efforts such as the DOJ Law Enforcement Information Sharing Program (LEISP) and the DHS Information Sharing Strategy, to ensure alignment to the overarching community-wide goals and objectives for information sharing. Several critical efforts are highlighted below:

- ***National Strategy for Information Sharing (NSIS): Successes and Challenges in Improving Terrorism-Related Information Sharing (October 2007):*** Recently released from the White House, the NSIS focuses the plan to build upon progress and establish a more integrated information sharing capability to ensure that those who need information to protect our Nation from terrorism will receive it and those who have that information will share it. The NSIS will improve interagency information sharing at the Federal level, while building information sharing bridges between the Federal Government and our non-Federal partners. Though NSIS is focused on improving the sharing of homeland security, terrorism, and law enforcement information related to terrorism within and among all levels of governments and the private sector, the foundational principles presented in this strategy are in alignment with the NSIS.
- ***Department of Defense Information Sharing Strategy (DoD ISS):*** Provides the strategy for the Department of Defense (DoD) to build a collaborative culture and DoD Information Sharing Environment. Through this strategy and its vision to "deliver the power of Information to ensure mission success," the DoD will: (1) Achieve unity of effort across missions and operations, (2) Improve the speed and execution of decisions, (3) Achieve rapid adaptability across mission and coalition operations, (4) Improve the ability to anticipate events and resource needs, and (5) Achieve greater precision in mission planning and execution. The DoD also defines information sharing as, "[m]aking information available to participants (people, process, or systems)." This information availability is to be brought about by a 4-tiered set of goals, envisioned to be quick wins: (1) Promote, encourage, and incentivize sharing, (2) Achieve an extended enterprise, (3) Strengthen agility, in order to accommodate unanticipated partners and events, and (4) Ensure trust across organizations. The DoD ISS establishes five touchstones of information sharing to guide implementation planning and establish key areas for improvement by all stakeholders.

- ***Program Manager, Information Sharing Environment (PM-ISE), Information Sharing Environment Implementation Plan:*** A multi-volume work that serves as a blueprint for information sharing efforts within the intelligence, law enforcement, homeland security, defense and foreign affairs communities of Federal Government as well with State, local and tribal governments, the private sector, and foreign partners. The PM-ISE notes that further integration "…requires a vision based on national policies, priorities, and partnerships, and clear understanding of the operative framework, roles, and responsibilities for effective information sharing." The ISE has a 6-point overall goal structure including: (1) Facilitate the establishment of trusted partnerships outside of government, (2) Promote information sharing by providing timely, validated, protected, and actionable information, (3) Encourage ISE members to function in a decentralized, distributed, and coordinated manner, (4) Leverage existing capabilities while at the same time collaborating to build new ones, (5) Enable the Federal Government to speak with one voice regarding terrorism, and (6) Ensure that sharing procedures protect privacy and civil liberties. A significant challenge to realizing these goals is that the ISE exists in a dynamic, unpredictable, shifting threat environment. In order to provide an integrated service in an unpredictable environment, the ISE must offer a suite of collaborative tools that exist side by side with policies and processes that allow for robust information sharing. Culture is not to be overlooked in this effort as each arm of the Federal Government has its own culture and heritage, as do State and local governments. ISE emphasizes the imperative need of moving beyond considering State and local government to be only 'first responders,' preferring instead to thinking of them as the first line of defense in a very deep line of information assets. Additionally, consistent with the IRTPA section 1016(g), the mission of the Information Sharing Council (ISC) is to provide advice and information concerning the establishment, implementation, and maintenance of the ISE to facilitate the sharing of terrorism information among appropriate agencies. The Intelligence Community Information Sharing Executive will represent the views of the Intelligence Community on this Council and bring to bear its input, resources, and support for information sharing activities pertaining to terrorism, weapons of mass destruction, and homeland security.
- ***Executive Office of the President (EOP), Office of Management and Budget (OMB), Federal Enterprise Architecture (FEA):*** In the spirit of OMB's intent to use FEA to identify opportunities to simplify processes and unify efforts across the agencies of the Federal government, information sharing has been a critical component embedded into the reference models. For the Business Reference Model, the PM-ISE has submitted a proposal to add sub-function 262 - Information Sharing that will provide a category to allocate Federal agency ISE-related planning elements. For the Services Reference Model, under the Digital Asset Services Domain, several sub-functions pertain to information sharing, specifically, 571 - Information Retrieval, 572 – Information Mapping/Taxonomy, 573 - Information Sharing, and 560 - Tagging and Aggregation.
- ***National Counterterrorism Center (NCTC):*** Prior to September 11, 2001, no single organization in the U.S. Government had access to the full range of terrorist intelligence information that was available. With the creation of NCTC, the Center is responsible for integrating all intelligence possessed or acquired by the U.S. government pertaining to terrorism and counterterrorism (except for exclusively domestic terrorism and counterterrorism) and for ensuring that agencies have access to and receive intelligence needed to accomplish their activities. NCTC has adopted a 'role-based access' mindset that parallels this strategy's intent to develop a uniform identity structure with attribute-based access to confidently share intelligence information. NCTC has developed innovative solutions, including NCTC Online and Terrorist Identities Datamart Environment, to increase information sharing and collaboration in support of the counterterrorism mission.

- ***National Counterintelligence Executive (NCIX):*** In the wake of the attacks of September 11, 2001, the NCIX was established in statute by the Counterintelligence Enhancement Act of 2002, as amended, to serve as the head of national counterintelligence (CI) for the U.S. Government, subject to the direction and control of the Director of National Intelligence. To evolve the counterintelligence community from a confederation toward a unified enterprise, the NCIX produced The National Counterintelligence Strategy, which was published in 2007. The Strategy outlines both mission and enterprise objectives in order to integrate and unify the counterintelligence community to support information sharing. To increase information sharing and collaboration, NCIX developed Mission Objective 3, which states: "Provide incisive, actionable intelligence to decision makers at all levels." The Office of the National Counterintelligence Executive will work with the Intelligence Community to balance the responsibility to provide information and the need to protect sources and methods.
- ***National Intelligence Strategy (NIS), Enterprise Objective 5 (EO5):*** Published in October 2005, the NIS outlines both mission and enterprise objectives in order to create a unified Intelligence Community that is better integrated and innovative. Of particular interest to this information sharing strategy is the need to fulfill the intent of Enterprise Objective 5, which states: "Ensure that Intelligence Community members and customers can access the intelligence they need when they need it." The strategic goals outlined in this information sharing strategy support EO5 and, namely, Goal #2 that pertains to the need for better discovery, access, and retrieval of intelligence information.

These documents have been included to depict Director McConnell's focus on partnering and alignment efforts both internal and external to the Intelligence Community.

Appendix

APPENDIX

LIST OF ACRONYMS

ADNI CIO	Associate Director of National Intelligence and Chief Information Officer
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DoD	Department of Defense
DoD ISS	Department of Defense Information Sharing Strategy
DOJ	Department of Justice
EO	Enterprise Objective
FEA	Federal Enterprise Architecture
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
ISC	Information Sharing Council
ISE	Information Sharing Environment
NCIX	National Counterintelligence Executive
NCTC	National Counterterrorism Center
NIS	National Intelligence Strategy
NSIS	National Strategy for Information Sharing
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
ORCON	Originator Controlled
PM-ISE	Program Manager – Information Sharing Environment
SIE	Single Information Environment
WFR	Write for Release
WMD	Weapons of Mass Destruction

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
E PLURIBUS
UNUM
UNITED STATES OF AMERICA

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511