

*Defense Science Board
2003 Summer Study*

on

**DoD Roles and Missions in
Homeland Security**



VOLUME II – PART B: SUPPORTING REPORTS

September 2004

**Office of the Under Secretary of Defense
For Acquisition, Technology, and Logistics
Washington, D.C. 20301-3140**

This report is a product of the Defense Science Board (DSB).

The DSB is a Federal Advisory Committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions and recommendations in this report do not necessarily represent the official position of the Department of Defense.

This report is unclassified.



OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301-3140

DEFENSE SCIENCE
BOARD

MEMORANDUM FOR THE ACTING UNDER SECRETARY OF DEFENSE
(ACQUISITION, TECHNOLOGY & LOGISTICS)

SUBJECT: Report of the Defense Science Board 2003 Summer Study on DoD
Roles and Missions in Homeland Security

I am pleased to forward the final report of the DSB 2003 Summer Study on DoD Roles and Missions in Homeland Security. The report consists of two volumes. Volume I evaluates DoD's role in homeland security and makes recommendations on how best to accomplish this mission. Volume II is a compilation of four sub-panel reports.

The conceptual thinking and the capabilities required to address the homeland security challenge are still immature. The study concludes that maturing the conceptual framework and capabilities related to homeland protection will require a holistic approach. Thus, fostering a holistic approach to protecting the homeland is a guiding theme for this study. The report's recommendations, which fall into the following six areas, reflect this theme.

- Global situation awareness
- Protect DoD mission-critical infrastructure
- Deter and prevent attack
- Emergency preparedness and incident response
- Exporting DoD core competencies
- Empowering U.S. Northern Command

I endorse all of the recommendations of the Task Force and encourage you to review their report.

A handwritten signature in black ink that reads "William Schneider, Jr." with a stylized flourish at the end.

William Schneider, Jr.
Chairman

This page intentionally left blank



OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301-3140

DEFENSE SCIENCE
BOARD

MEMORANDUM FOR THE CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Report of the Defense Science Board 2003 Summer Study on DoD
Roles and Missions in Homeland Security

Developing an effective capability to protect the homeland is a top national priority. It is also a complex undertaking filled with many challenges. There are so many assets to protect, so many modes of attack available to adversaries, and so many organizations involved, that, understandably, both the conceptual thinking and the capabilities required are still immature. Maturing the conceptual framework and capabilities related to homeland security, the DSB believes, requires a holistic approach—a guiding theme for this study.

The final report of this study consists of two volumes. Volume I identifies capabilities and initiatives needed by DoD to fulfill its responsibilities to project force when directed and to protect the homeland. It focuses on those capabilities that depend upon DoD working closely with other agencies. In addition, opportunities are identified for DoD to “export” some of its core competencies to help accelerate the maturation of the many agencies involved in homeland security tasks. Volume II is a compilation of four sub-panel reports.

The principal findings and recommendations fall in six key areas:

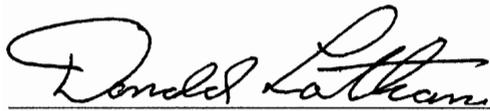
- Information is vital to homeland security. *Yet improvements are needed in many areas of information sharing, assurance, and collection.* First, incentives are needed to enhance information sharing. Second, tools and capabilities for information assurance need to be developed and implemented. Third, collection capabilities, importantly in the area of human intelligence, must be enhanced. In general, foreign intelligence collection must be more proactive and better integrated with domestically derived intelligence.
- DoD’s ability to fulfill its missions—most notably force projection—is dependent on an intricate infrastructure in the

United States. *DoD is not doing enough to address the vulnerabilities of mission critical infrastructure and services, particularly in areas outside its direct control. A systematic approach – that focuses both “inside and outside the fence” – must be taken to identify and redress vulnerabilities. Moreover, cyber security and cyber-based aspects of critical infrastructure need to be better integrated into DoD mission-critical infrastructure protection efforts.*

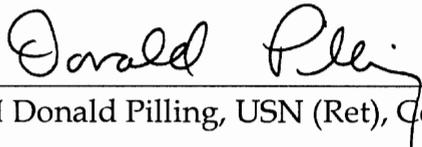
- *Ocean vessels, cruise missiles, and low-flying aircraft are credible delivery systems available to adversaries. DoD needs to take steps to counter these threats as a complement to ongoing initiatives to defend against ballistic missiles. First, much more can and should be done to improve maritime security and to integrate maritime-security capabilities across the federal government. Second, because these delivery systems could threaten the continental United States with biological and other weapons of mass destruction, DoD should create a master plan for defense against the low-altitude air threat.*
- *Should the U.S. homeland be attacked, DoD could be called on to assist with incident response. Execution of this mission could require capabilities in areas where the Department is deficient: 1) mitigation and remediation of the effects of attacks from weapons of mass destruction, 2) the ability to surge medical capabilities, 3) communication operability between first responders and federal, state, and local agencies. The report offers detailed recommendations for improving capabilities in each of these areas as well as enhancing Reserve Component capabilities that can support the homeland security mission.*
- *DoD can enhance homeland security by “exporting” relevant core competencies that match the needs of other organizations that have homeland security responsibilities. The study identifies three core competencies in particular: training, experimentation, and operational-level planning and execution. Responsibility to develop, and oversee execution of, plans to export core competencies to other agencies should be assigned to U.S. Northern Command.*

- *U.S. Northern Command must be empowered for the nation to achieve its homeland security and homeland defense goals.* The study recommends more than a dozen new tasks for NORTHCOM, with four identified as priorities: develop a roadmap for maritime surveillance; develop a roadmap for defense against the low-altitude air threat; assume operational lead for DoD mission-critical infrastructure protection in CONUS; and assume the lead for exercises, training, experiments, and standards related to homeland defense and military assistance to civil authorities.

The specific recommendations provided in the pages that follow reflect the holistic approach to protecting the homeland that the DSB envisions for the Department of Defense. By taking this approach, and developing the capabilities described in the six areas above, the security of our nation will be improved.



Donald Latham, Co-Chair



ADM Donald Pilling, USN (Ret), Co-Chair

This page intentionally left blank

TABLE OF CONTENTS*

INFORMATION, SHARING AND ANALYSIS PANEL REPORT

* VOLUME I OF THIS REPORT REPRESENTS THE CONSENSUS VIEW OF THIS TASK FORCE. VOLUME II OF THIS REPORT CONTAINS MATERIAL THAT WAS PROVIDED AS INPUTS TO THE TASK FORCE, BUT WHOSE FINDINGS AND RECOMMENDATIONS MAY NOT REPRESENT THE CONSENSUS VIEW OF THIS TASK FORCE

This page intentionally left blank

INFORMATION SHARING AND ANALYSIS PANEL REPORT

This page intentionally left blank

1.0 INTRODUCTION

During the Cold War, the United States developed and refined intelligence capabilities based upon a number of key factors:

- Known adversaries, the Soviet Union and the Communist Bloc, including China and North Korea;
- Known geographic boundaries: that of the communist nation states (We knew where to look);
- Known conflict of ideology: communism vs. capitalism;
- Observable (with some degree of confidence over time) military capabilities of adversaries; and
- Indications (and in some cases, warning – developed over the years) of activity potentially hazardous to the United States and NATO.

The defense and intelligence communities were able, through prolonged observation of the Soviet Union, to understand that the appearance of a single data point could be indicative of a much broader context because prior observations had created a mosaic of discrete events and classes of events. Thus, communications intercept of refueling activities at a strategic bomber base might be indicative of increased readiness of Soviet strategic forces, or a satellite image of a single section of a submarine hull at a Soviet shipyard could indicate that a new submarine class was in year seven of a probable ten year construction program; and numerous other examples from which a single piece of data would be fairly clearly indicative of a much broader range of activities or intent.

These capabilities resulted from what has most recently been characterized as intelligence, surveillance and reconnaissance (ISR) capabilities. ISR capabilities have been remarkably effective in recent conflicts. In Afghanistan, U.S. forces found and hit moving targets in near real time by sharing information quickly and effectively. In Iraq, information from national technical means moved in near real time to a U.S. aircraft that was involved in attacking the meeting place of senior

Iraqis. The military proved adept at developing tactical knowledge in time and information-constrained operations. In the case of Afghanistan and Iraq, the U.S. military's networked operations permitted fundamentally new capabilities for intelligence preparation of the battlefield.

Homeland defense and homeland security must function in a vastly changed world. Consider the differences. In contrast to the situation during the Cold War:

- Adversaries are not well known, and focusing efforts and intelligence collection and analysis capabilities is more difficult.
- The familiar geographic boundaries are gone and monitoring and searching must now be done globally.
- The ideology is different and there are different goals, objectives and motivation on the part of potential adversaries. For fundamentalists and Islamists (estimated to be on the order of 10% of all Muslims), Islam is both a religion and an ideology. This means that the Muslim Brotherhood and Al Qaeda, inter alia, challenge the fundamental existence of the United States.
- Weapons (destructive) capabilities of adversaries are not well known and thus it is appropriate to plan for "worst case" scenarios.
- The familiar "indications and warning" are not very useful and effective new ones have not been developed.

While the roles, missions, responsibilities and authorities of the Department of Defense (DoD) with regard to securing and defending the homeland are not yet fully defined, it seems clear that DoD's intelligence capabilities must be employed in defending the nation, securing the homeland, countering terrorism and combating terrorists.

One of the most important issues for DoD and HLD/HLS in general is the sharing of intelligence and information required to deter and prevent terrorist attacks. Some intelligence needed to fight terrorism may not reside primarily in places amenable to foreign intelligence

collection. Much of the information required resides in law enforcement databases, in ongoing investigations, and in the daily information gathered from persons and cargo entering or bound to or from the United States. And terrorists have demonstrated their ability to “work the seams” between U.S. intelligence and law enforcement communities to plan and conduct operations just as petty criminals have learned to target their crimes at the intersection of jurisdictions. Note that every successful medium to large scale terror attack in the United States has the following characteristics:

- They have been well planned
- They have been, to a significant degree, based on intelligence collected over time and put into useable form.
- All but one has been the work of a group of two or more persons, and in most cases a much larger group. A presumed exception is the east coast anthrax attack.
- Most have been directed against facilities as well as people or the institution as well as the person of the President of the United States.
- They have depended on the elements of secrecy and surprise for their success and have thwarted the efforts of the U.S. intelligence community (IC).

New approaches are required for information gathering and information sharing. One of the biggest challenges in this new approach is the sheer number of stakeholder communities engaged in homeland defense (HLD) and homeland security (HLS). As illustrated in Figure 1, the information-sharing environment for HLD/HLS encompasses the defense, foreign intelligence, and law enforcement communities and includes public information such as real-time news broadcasts. The environment also includes state and local government organizations such as emergency operations centers, first responders, private sector owners and operators of critical infrastructure that may be targeted by terrorists. Each of these stakeholder communities has its own methodologies for gathering, processing, and sharing information.

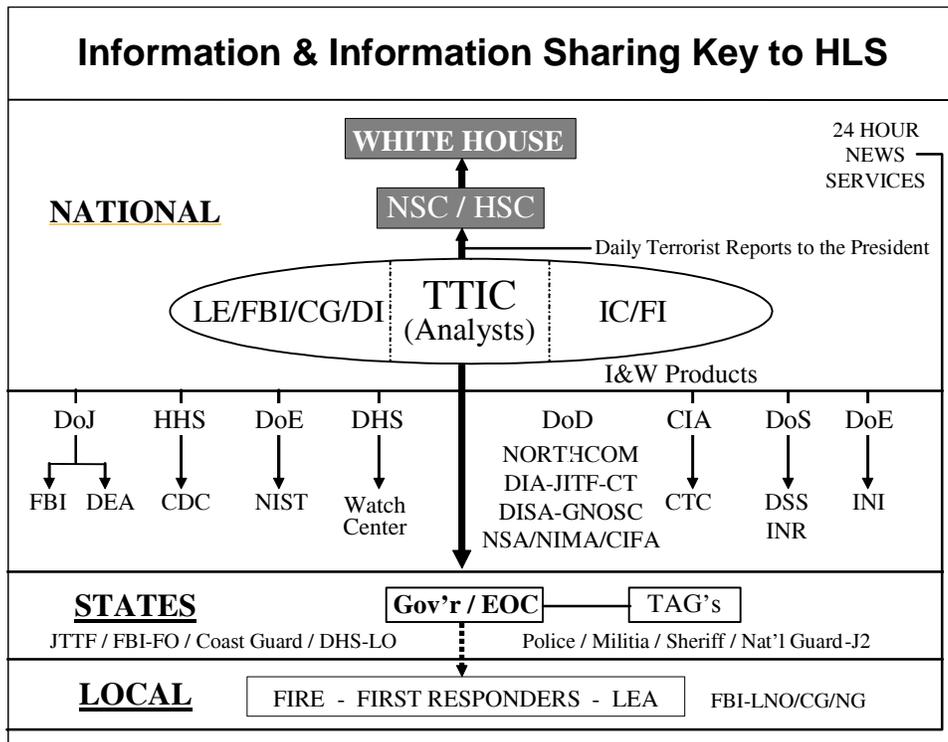


Figure 1. The Information Sharing Environment for Homeland Security

Lessons learned from 9/11 have been translated into tremendous energy and expenditure of resources at the federal, state, and local levels. The Department of Homeland Security was created in recognition of the need to bring together many of the agencies, organizations, and activities whose work is central to the overall homeland security mission. The President established the Terrorist Threat Integration Center (TTIC) to provide greater focus on the anti-terrorism problem. NORTHCOM was established to improve the defense of North America and to focus on terrorist threats to critical U.S. infrastructures required to support the U.S. military and Department of Defense. Many states, metropolitan areas, and localities have initiated homeland security actions of varying descriptions, from improved emergency communications to detailed planning for defense against a bio-terrorism attack. Yet the potential value of all this activity cannot be realized unless and until effective means of information

sharing are instituted at all levels and among all participants in the war on terrorism.

Rapid conversion of information to knowledge requires reuniting homeland defense and security users with the raw material of their trade...and with the tools, techniques and capability to mine, manipulate, integrate and display all potentially relevant data. Users across the spectrum of homeland security need to have access to both analytical results and data. Too often today, there is excessive filtering, fondling and information packaging, which cause inefficiencies and time delays. These are all valuable services, but not in all cases. There are no monopolies on interpretive functions. It is clear that there is a need to provide wider access to substantive content.

DoD has much more to offer than simply the sensitive intelligence and other information available to it. DoD has important information, information strategies, and information architectures (as well as data fusion, visualization and integration tools) that are vital to the national homeland security effort. Equally valuable are the conceptual and architectural approaches DoD has taken to many problems (e.g. information operations, secure communications), many of which are applicable to the national, state, and local players. To ensure national success in the prevention of terrorist attacks on the United States, DoD must share some of these concepts, architectures and information-sharing and analysis approaches with DHS and other homeland security stakeholders. While DoD resource constraints must always be considered, DoD will play a vital role in the overall Homeland Security mission.

Many of the legal and policy constraints have been removed since 11 September 2001, but the differences in culture and incompatible technologies remain. This part of Volume II addresses the issues associated with both information sharing and information analysis in the context of homeland security and then provides recommendations for improvement.

2.0 SHARING WHILE PROTECTING INFORMATION

2.1 *WHY SHARE?*

The General Accounting Office (GAO) addressed the range of issues concerning information sharing for homeland security in a 2002 report:

“To protect the nation from terrorist attacks, homeland security stakeholders must more effectively work together to strengthen the process by which critical information can be shared, analyzed, integrated and disseminated to help prevent or minimize terrorist activities. Activities that are hampered by organizational fragmentation, technological impediments, or ineffective collaboration blunt the nation’s collective efforts to prevent or minimize terrorist attacks.”

There are compelling reasons for sharing information in support of homeland defense and homeland security. First, homeland defense and security involves a broad and complex set of organizational relationships. Department of Homeland Security/Information Analysis and Information Protection (DHS/IAIP), TTIC, and NORTHCOM are still taking shape. At the same time, a new dialogue between federal, state, and local authorities on threats to the homeland is evolving. Yet even before the organizational dust settles, it is clear that the range of stakeholders is so broad and the issues so complex that no one entity, department, or agency can be expected to know everything about terrorist threats to the United States. To assure success in the long-term war on terrorism, an environment characterized by effective information sharing must be shaped now. Mechanisms, policies, and procedures must be established to ensure the continuing dialogue among the new institutional actors as well as existing law enforcement and intelligence communities.

Second, information required for homeland defense and homeland security in many cases will be the same information. DoD,

by itself, cannot solve the homeland defense problem, nor can DHS handle homeland security by itself. Extensive and continuing collaboration will be vital to the national effort. In many situations (September 11, 2001, for example), the security and defense aspects of the homeland mission quickly blend into one activity; the transition from defense to security may occur in a matter of seconds. As the DoD and DHS missions overlap in some respects, so too does the data to support the information needs of each department.

Third, data owners cannot know or predict the value of their data to all potential users. Data requires context to become information. One person's data is another person's information. What is vital information to one is just data to another. The point of this logical thread is to underscore that--with few exceptions--data can no longer be "owned" but needs to be shared among all homeland security stakeholders to ensure that critical information is not discarded or remains dormant because its existence or significance is unknown. In this new paradigm, data "owners" become data "stewards" obligated to make their data and information available to all homeland security stakeholders, albeit with appropriate safeguards as required to protect sources and methods, provide for information assurance, etc. During Panel deliberations, a compelling argument for this change from data ownership to data stewardship was discussed.

The most basic reason for sharing information among stakeholders in the U.S. fight against terrorism is because it is the "right thing to do" and it is now required by law, executive order, and inter-departmental agreement. The background and rationale for changes to the law are fully described in the Congressional "Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of 2001."

Based on the legal principles established in the National Security Act of 1947, clear lines of authority evolved which restricted the Central Intelligence Agency and, by extension, other members of the Intelligence Community, from participation in domestic intelligence and law enforcement functions. The Foreign Intelligence Surveillance Act of 1978 (FISA) defined a strict boundary between the use of electronic surveillance for foreign intelligence purposes and that

required for law enforcement investigations, allowing sharing of law-enforcement information with appropriate intelligence authorities only when the original purpose of the surveillance had been foreign intelligence. Policies that grew around these laws enforced the continuing separation of foreign intelligence and law enforcement information.

The Administration and Congress recognized the need to improve information sharing between foreign intelligence and law enforcement well before the Joint Inquiry was published. The USA Patriot Act of 2001 authorized the sharing of grand jury information with “any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official” when such information involved foreign intelligence or counter-intelligence that could be used to thwart terrorism. The Patriot Act also modified the requirement for FISA surveillance, allowing such surveillance if foreign intelligence was “one” of its purposes and not “the” purpose. These changes were meant to eliminate the restrictions that evolved around FISA operations, which had effectively shut down information exchange between law enforcement and intelligence on matters relevant to anti-terrorism. However, the courts have yet to adopt this more fulsome interpretation.

The Homeland Security Act of 2002 (Act) goes beyond the USA Patriot Act to broaden the requirement for information sharing between federal, state, and local personnel. Federal entities explicitly called out in this Act include the Department of Homeland Security and the Intelligence Community and they are to share relevant homeland security information with state and local personnel. All involved departments, agencies, and activities are to have access to information sharing systems containing all homeland security information. Appropriate safeguards are to be applied to limit unauthorized dissemination and to protect individual privacy. The Act was supplemented by an Executive Order on 29 July 2003, the effect of which was to designate the Secretary of Homeland Security as the responsible official for implementing information sharing policies and procedures called for in the Act.

Information sharing is also the subject of a comprehensive Memorandum of Understanding (MOU) signed in March 2003 by the Director of Central Intelligence, (DCI) the Attorney General, and the Secretary of Homeland Security.¹ The MOU is binding on all entities under the purview of the signatories and is “intended to mandate minimum requirements for information sharing, use, and handling, and for coordination and deconfliction of analytic judgments” to protect against terrorist threats to the United States. Although not signed by the Secretary of Defense, this MOU should be binding on Defense agencies that are members of the Intelligence Community. To remove any confusion among DoD members of the Intelligence Community, the Secretary of Defense should formally direct that all DoD agencies and elements comply with this MOU. The fundamental principle of this MOU is that: “The parties recognize and agree that, in some cases, this priority shall dictate information sharing even where doing so may affect criminal prosecutions or ongoing law enforcement or intelligence operations.” Consequently, all entities subject to the MOU are cautioned to protect “to the greatest extent possible” sensitive sources and methods, other classified information, and operational and prosecutorial information.

Sharing information in isolation is not adequate. Information sharing initiatives must be integrated and coordinated to be most effective. An August 2003 GAO report points out that many states and cities participate in information-sharing activities today, but that the lack of coordination at the national level limits the effectiveness of these initiatives. The GAO concludes that:

“While these initiatives may increase the sharing of information to fight terrorism, they are not well coordinated and consequently risk creating partnerships that may actually limit some participants’ access to information and duplicating efforts in some key agencies in each level of government. Moreover, while beneficial to these participants, the initiatives do not necessarily integrate others into a truly national system

¹ Inexplicably, in the Panel’s view, the Department of Defense was not a signatory.

and may inadvertently hamper information sharing for this reason. A lack of effective integration could increase the risk that officials will overlook, or never even receive, information needed to prevent a terrorist attack.”

2.2 WHAT NEEDS TO BE SHARED?

The Information Sharing MOU signed in March 2003 categorizes the types of information that must be shared among homeland security stakeholders and provides guidelines for the sharing of this information. The taxonomy used in the MOU provides a good framework for discussion by the Defense Science Board (DSB).

The MOU places information on terrorism, vulnerabilities, and weapons of mass destruction (WMD) information into a category as “covered” information subject to the rules and restrictions of the MOU. These types are further defined as follows.

Terrorism Information – “All information relating to the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, domestic groups or individuals involved in terrorism, to threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations, or to communications between such groups or individuals, and to information relating to groups or individuals reasonably believed to be assisting or associating with them.”

Vulnerabilities Information – “All information relating to the susceptibility – actual, perceived, or conceptual – of the United States, including any portion, sector, population, geographic area, or industry, to terrorist attack.”

WMD Information – “Terrorism information or vulnerabilities information relating to conventional explosive weapons and non-conventional weapons capable of causing mass casualties and damage, including chemical or biological agents, radioactive or nuclear materials, and the means to deliver them.”

The MOU outlines the processes and procedures for sharing these types of information with DHS, TTIC, private infrastructure owners, state and local officials and the public. Information in the three covered categories is to be provided to DHS “without request,” subject to certain restrictions involving the protection of intelligence sources and methods and law enforcement operations. A distinction is made between “analytic conclusions,” which are to be shared, and other formats (e.g. report of an interview with a source) that are not to be shared. The MOU also includes procedures for sanitizing classified information, for the use of tear-line reports, and other topics that are covered elsewhere in this paper.

While the MOU does not spell out specific formats for sharing terrorist threat information, the focus on “analytic conclusions” suggests that the primary format should be textual reports, conveyed to all homeland security stakeholder organizations via electronic networks, facsimile or hard-copy. Common practice in the intelligence community is to convey documented analytic conclusions in a variety of media depending on the technologies available to the consumers of the information provided, and the MOU seems to assume no new or different techniques for providing covered information to homeland security stakeholders.

The Panel spent a considerable amount of time discussing the need to share not just “analytic conclusions,” but the underlying “data.” Several presentations to the Panel focused on the need to get to the basic information that feeds the analytic process and results in analytic conclusions and finished intelligence reports. Two basic concerns were identified. First, since “data owners” do not always understand the value of their data to all potential homeland security stakeholders, there may be a delay in conveying vital information from the point of collection to delivery to the consumer who actually needs it. In some cases, the information may not be delivered at all. The second concern is that analysts may omit certain pieces of information from the final report without understanding that what ends up on the “cutting room floor” may be valuable to an analyst or consumer in another agency.

Current thinking within DoD and elsewhere (e.g., the finance and pharmaceutical sectors) is focused on addressing these problems by “tagging” data before it is analyzed and placing it in a data base that can be accessed by analysts in other organizations. The DoD concept of “TPPU” – Task, Post, Process, Use – focuses on making data available to all potential stakeholders as soon as physically possible, – *i.e.*, at its earliest point of “consumability” – allowing more than one organization to perform analysis on the same data simultaneously. This approach is enabled by the “network centric architecture” published by the DoD Chief Information Officer (CIO) in May 2003 and briefed to the Panel. The use of XML tagging of data is gaining acceptance as a common technique for facilitating the sharing of data before it is fully processed and finally reported.

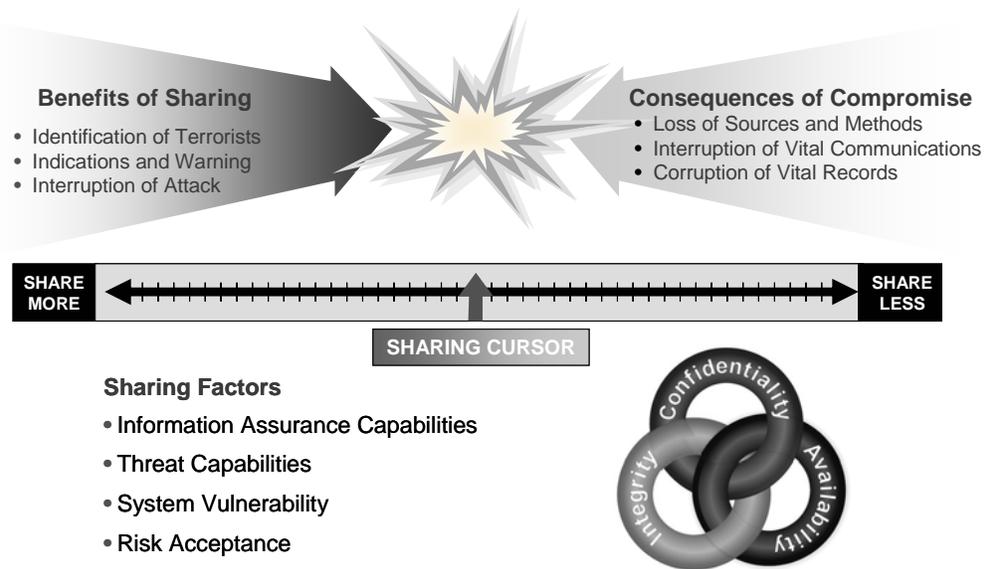
Adopting an approach to the analysis of terrorist threat information that includes sharing data (sometimes referred to as “raw data”) in addition to completed reports is easier said than done. Legal, policy, stovepiped IT architectures (networks and data bases), and cultural factors quickly come to the fore in any discussion of sharing at the data level. As the Panel discovered, most analogies do not work. For example, even though Electronic Intelligence (ELINT) data is shared among many organizations with effective results does not mean that all other types of signals intelligence intercepts can be shared with equal facility. Different policies, procedures, and aspects of institutional culture come into play and must be addressed. Nonetheless, the Panel believes that data exchange has a high potential for improving overall information sharing among homeland security stakeholders.

2.3 THREATS FROM INFORMATION SHARING

While there are nationally significant reasons for sharing information across government organizations, it is less obvious that sharing can become a “double-edged sword”. Although greater connectivity will allow increased sharing, the increased aggregation of data and applications, globally dispersed nodes, and technically complex systems, components and architectures provides both the motivation and operational opportunity for an adversary to breach

the confidentiality of this information as well as attack its integrity and availability. Implementing sharing architectures without taking into account the adversarial perspective and consequently improving the information assurance of networked systems could result in disproportionate benefit to adversaries. (See figure 2 below)

Figure 2: Information Sharing is a Double-Edged Sword.



Today more than ever, sharing information is essential to U.S. national security. Cultural differences, technical shortcomings, policy roadblocks, legal restrictions and lack of personal and institutional resolve were, in part, the enemy of information sharing. Motivated by the tragic events of September 11, 2001, much progress has been made in softening the cultural differences, developing technical applications to enable sharing, removing policy roadblocks, reviewing and addressing legal restrictions, and strengthening national resolve to never let this happen again.

But there remain potential consequences to information sharing. The advances in information technology over the past few decades, and the availability of such technology in the hands of potential adversaries, mean the probability of successful targeting and

exploitation of critical information systems is on the rise. Technical advances and the dramatic increased dependence on technology for conducting business, projecting military force, and sharing intelligence and law enforcement information have created new and very attractive targets for adversaries. The successful targeting and exploitation of these systems will have increasing benefit to the enemy and reduce the U.S. ability to detect, deter, and respond to their operations.

To achieve the delicate balance between collaboration and security, it is critical to understand the nature and capability of the current foreign threat to U.S. information systems. Senior decision makers must take into account the challenges technological advances and complexities pose in protecting vital systems as well as the impact of their failure. There must be an understanding on how these changes create new operational opportunities for the adversary in exploiting U.S. critical systems. Deeper understanding must be acquired of both the inherent and operationally introduced vulnerabilities in these systems.

Techniques for discovering these weaknesses must be developed, effective defenses must be designed and metrics must be developed and used for assessing the operational impact of the compromise of systems. Depending on the system, the compromise of confidentiality, corruption of integrity, or the loss of availability can have extreme impact. While great attention has been given to confidentiality issues, in many instances the failures of either integrity or availability in even unclassified systems can have greater impact than the loss of a secret – indeed, sometimes critical information may not be secret. Only through gaining clearer insight into these issues, developing more effective defensive technology and placing greater emphasis on integrity and availability can the benefits of sharing be put into proper balance with the probability of compromise and its associated consequences.

With a growing percentage of software being designed, coded, distributed, and maintained overseas, U.S. adversaries enjoy unprecedented direct and indirect operational access to many vital U.S. systems. Coupling this advantage with the United States

transitioning much of its microelectronic fabrication offshore, the clever adversary has the opportunity to penetrate key U.S. systems in a deeply concealed manner. Our ability to evaluate, detect anomalies, control configuration, and assure the trustworthiness of these systems markedly diminishes as capability, complexity and size increase. U.S. evaluation capability has failed to keep pace with this escalating complexity. Therefore, systems architectures, designs, and operations must be able to provide crucial services even under assault or in degraded modes.

There is a growing body of evidence that many U.S. adversaries have adopted asymmetric approaches to attacking U.S. systems. FBI Director Mueller reportedly estimated that China has established more than 3,000 “front” companies in the United States to conduct espionage and will become the United States’ greatest intelligence threat in the next decade.

As software and hardware development moves offshore and becomes operationally vulnerable to implant; as complexity rises to levels that are impossible to evaluate; and as U.S. dependence on these technologies for future systems escalates, the potential exists for an adversary to gain a foothold and bury himself in this complexity. Then at a time and place of his choosing, the adversary exercises an asymmetric weapon to compromise the confidentiality, integrity, or availability of U.S. information or services. At that point, U.S. dependence on the strategy of information dominance becomes an Achilles heel.

Without this understanding, the defensive players are likely to invest resources, develop defensive barriers, promote strategies, and establish policy that has little impact on the adversary’s ability to compromise U.S. systems. However, current information assurance efforts focuses predominately on tools and techniques for protecting data while in electronic transit as well as external accesses to U.S. systems. It is increasingly apparent that equal efforts must be devoted to protecting information systems from malicious activity by those who successfully penetrate our defensive measures, and from “insiders” with malicious intent.

Today, there are too few tools to detect unauthorized activities within U.S. systems and inadequate tools to detect the insertion, or presence, of malicious code. Effective homeland defense and homeland security require thousands of new participants in our information systems, thus raising the probability of successful assaults on key nodes. The Panel believes that substantially increased emphasis must be placed on capabilities to build systems that can withstand such attacks. Therefore, this Panel suggests that DARPA expand its R&D on developing systems that degrade gracefully while preserving crucial capabilities.

The bottom line is that the United States is both vulnerable and a target and is probably being exploited in an undetected fashion by sophisticated adversaries. The dichotomy is that information sharing systems must be expanded in order to stay at the leading edge and be effective in combating terrorism, recognizing that this will increase the risk of exploitation by these adversaries. This drives us to a risk management strategy. Regrettably, this is easier said than done. In order to have an effective risk management program, one must: know what needs to be secret and thus require added protection; know the adversaries, their capabilities, limitations, constraints, resources, partners and risk model; identify vulnerabilities; and understand defensive options. Without understanding these issues, risk management is simply a quote from the latest book on management.

3.0 IMPROVE INFORMATION SHARING

3.1 A NATIONAL VISION FOR INFORMATION SHARING FOR HOMELAND DEFENSE AND HOMELAND SECURITY

In meeting the information sharing needs of both homeland security and homeland defense, a national vision must be evolved that encompasses several realities.

Homeland defense and homeland security share many of the same information needs. In some scenarios the transition from one to another needs to be quick and seamless. Those engaged in homeland defense will have to maintain cognizance of what is occurring throughout the homeland security sector and vice versa.

The technologies and overall approach in most ongoing efforts to improve information sharing are the same. Extending network connectivity to homeland security stakeholders and applying analytic and collaboration tools to the common network are needs for all stakeholders.

Even under the heightened state of awareness since September 11, 2001 (and the resulting improvements in information sharing), the situation today is still characterized by individual or organizational data “owners” who don’t know the value of their data to all potential users, operating under a culture that requires those seeking information to ask the “perfect question” before gaining access to the information they need, and by security rules and procedures that inhibit the necessary *sharing* of essential information by applying a one-size-fits-all approach based on the *source* of the information.

The most important requirement is to provide access for all HLD/HLS stakeholder communities of interest to the information they need to perform their mission regardless of the source of that information. While sensitive intelligence sources and methods, law enforcement equities, and the like, must be protected, there is a

compelling need to get timely, actionable information to those on the front lines of the homeland defense and security missions. Providing a common operational picture that can be tailored to specific user needs would be a vital contribution.

In consideration of these realities, the Panel endorses the following vision for HLD/HLS information sharing:

The vision for the national information-sharing architecture is to achieve a common situational awareness for all stakeholders, tailored to specific user needs – the federal, state, local, and private sectors – for those who have a role in providing the nation’s security and preventing or disrupting terrorist attacks on the United States.

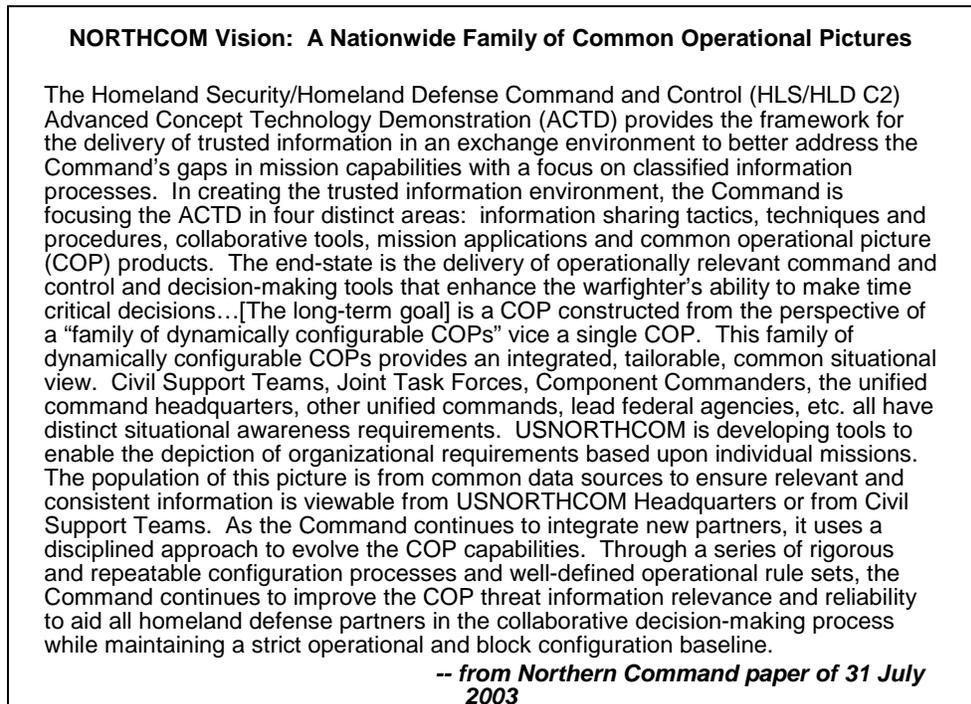
Achieving this vision does not require invention of new technology. Today’s internet- and web-based technologies will support the development of highly effective information-sharing among HLD/HLS stakeholder communities. In a national network-centric architecture, users themselves will define strategies for successful information sharing. They will find ways to bridge the gaps inevitable in any organizational structure at any level. They will also build a culture based on information sharing that will create synergies in threat detection and prevention.

To be successful, however, leadership is required to bring focus to implementing new laws and regulations that have been promulgated since 9/11. These new laws and regulations allow for much greater sharing among various communities, particularly between law enforcement and foreign intelligence entities. Leadership is also required in enabling the interconnections of networks containing intelligence, law enforcement, and private sector information that enables effective sharing while simultaneously protecting sensitive sources, methods, and ongoing investigations.

Effective national information sharing to support HLD/HLS is well within the realm of the possible. Already, NORTHCOM has developed an overall approach that would enhance HLD/HLS capabilities for DoD and for the Nation as whole. NORTHCOM’s

vision addresses the goal of developing common operational pictures for stakeholder communities of interest. (See Figure 3.)

Figure 3. NORTHCOM Vision for Information Sharing.



New structures have been established to implement Administration homeland security policies and make real the concepts of HLD/HLS information sharing.

DHS/IAIP Directorate - IAIP integrates foreign intelligence, law enforcement, and private sector information to identify and evaluate current threats to the Nation's critical infrastructure. IAIP works with federal, state, local, and private sector organizations to shield that infrastructure and to ensure that measures are in place in the event that protective measures fail.

Joint Intelligence Task Force for Counterterrorism (JITF-CT) - The Director, Defense Intelligence Agency (DIA), established the JITF-CT to integrate all available information that impacts DoD activities in CONUS and overseas. JITF-CT exchanges intelligence

and other information with Intelligence Community agencies, the Department of Homeland Security, and the law enforcement community.

U.S. Northern Command (NORTHCOM) - Established by the Secretary of Defense in 2002, NORTHCOM is responsible for integrating HLD/HLS information relating to the protection of North America and littoral areas and for working with federal, state, and local law enforcement authorities to provide force protection for U.S. military forces based in the United States.

Terrorist Threat Integration Center (TTIC) - Under DCI leadership, TTIC brings together personnel from the IC and law enforcement as well as DHS. TTIC integrates foreign intelligence and law enforcement information into a coherent product and shares that information with DHS. This process closes a critical gap, of integrating foreign- and domestic-sourced terrorist threat-related information.

These new organizations are sharing information for HLD/HLS through electronic means and via the exchange of personnel to perform assignments in counterpart organizations. The current system for homeland security intelligence information sharing is depicted in Figure 4. Not depicted are the cultural and institutional barriers that preclude information sharing in a manner consistent with the Panel's vision. These issues are described more fully in Sections 3.2 and 3.3 below.

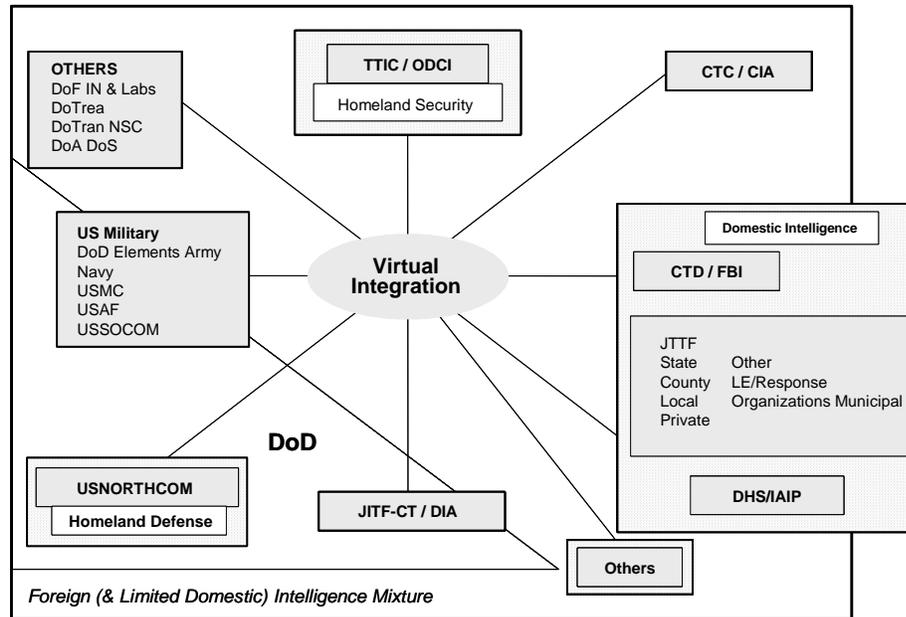


Figure 4. Homeland Security Intelligence System²

Achieving the Panel’s vision will impact organizational cultures, ways of doing business, and traditional prerogatives. Establishing a national information-sharing network for homeland security information will require new ways of doing business that focus on the “need to share” all relevant HLD/HLS information. Overcoming organizational resistance based on years of not sharing information with other communities (or sometimes internally within their own organizations) will require a concerted effort on the part of DoD elements and external agencies and departments. There are compelling national needs for changing traditional paradigms.

² Figure 4 does not include the details of intelligence organizations, some organizations are not shown and other units and elements are not mentioned. This is necessary to keep this viewgraph UNCLASSIFIED.

3.2 INFORMATION SHARING TODAY

The Panel sought to identify unclassified examples of the complexity and challenges of information sharing, in the context of the attacks on 11 September 2001, by studying data from public sources. Analysis of public source data demonstrated two aspects of this complex problem.

- Important information was discovered (and in some cases not recognized for its significance) by the U.S. or foreign entities prior to 9/11; and
- Important data was either not shared between agencies, or filtered in a way that hindered more adequate warning.

Analysis of classified data provides similar results.

DoD entities, especially those within the Intelligence Community, do not have a clear or uniform understanding of the homeland security responsibilities. While the need for better information sharing is generally accepted, this need is not fully integrated and leveraged in a systematic way across all HLD/HLS-mission areas and DoD entities. Some DoD managers believe their information, while vital to the Department, is not relevant to the war on terrorism or have not considered its application to homeland security. Others know they have useful data to share, but are thwarted by policies and cultures that discourage sharing outside their own institutions. Still others are unaware that vital information that could help them perform their mission resides elsewhere, in an organization they may not know exists. For example:

- The DoD Information Assurance Strategic Plan (2003) provides an excellent roadmap for information sharing and protection within the Department; however, it does not adequately address interoperability requirements such as data element standards or encryption compatibility for sharing sensitive information with HLD/HLS communities of interest.

- There is a widespread perception that senior DoD and NORTHCOM officials are not allowed to interact with DHS or other members of the HLS community.
- A senior officer with infrastructure protection capabilities at a major U.S. military facility was unaware of critical infrastructure protection activities underway elsewhere in the Department or his own service.

One source of confusion has to do with new customers and new types of necessary information resulting from the national homeland security mission. Information sharing in DoD has evolved primarily in functional stovepipes. Traditional information flows and data networks have been established to satisfy traditional missions and may not adapt well to homeland security requirements. Moreover, the number of major players in the homeland security communities has increased significantly with the inclusion of other federal agencies as well as state, local, and private sector entities involved in homeland security. Clarification is required in terms of what types of information can be shared with whom. When that information is classified, clear guidelines and procedures are needed for sharing that information with those not in the traditional information flow for classified data.

During the period March – June 2003, over fifty onsite and telephonic interviews were conducted with DoD employees and a representative sample of interested external DoD parties from both the public and private sector in order to expand understanding of current information sharing issues. The objective of the interviews, and the subsequent analysis was to: a) identify relevant stakeholders; b) map how HLS-related information is flowing – and how it should flow – within the DoD and between the DoD and external organizations; c) provide insights into stakeholder expectations of key issues; d) highlight key issues and obstacles to data sharing; and e) provide possible recommendations for DSB consideration.

The results of this study are contained in Appendix D. The central recommendation emerging from the interviews is that the Secretary of Defense should charter a study to fundamentally rethink

how HLS-related information should be shared within the Department of Defense and with key partners, to identify *what* information must be shared, and to determine *which* high impact actions and programs are needed to thoroughly improve information sharing for homeland security, in order to enable the DoD's longstanding mission to protect its own forces and critical infrastructures, as well as to support lead civil agencies implementing the *National Homeland Security Strategy*. Figure 5 depicts the summary of key issues and general findings from the interviews.

Due to the magnitude of potential threats to the homeland, the difficulty of assigning attribution to attackers, and the resources necessary to address the challenge, the DoD may be called upon to play a supporting role in homeland security. Within the context of the new environment, neither the DoD nor civilian agencies have fully explored the potential homeland security-related information sharing implications.

Figure 5. Summary of the key issues and general findings

Key Issues	General Findings
<ul style="list-style-type: none"> ▶ Changing communities of shared mission. New players in homeland security with new missions and existing entities with different priorities leave roles, responsibilities, and interfaces between agencies unresolved and/or immature. ▶ DoD and Interagency misunderstanding of roles and supporting mission in homeland security. DoD is generally unclear on information sharing needed internally for its own core missions, and some Defense entities are unaware of DoD-held information needed by other agencies for HLS. DoD and interagency lack of understanding of the potential support DoD may be asked to provide for HLS has created a false perception by some in DoD that they face <u>no</u> major information sharing challenges. ▶ Significant information sharing breakdowns. Anecdotal, yet potentially significant, information sharing breakdowns exist in key HLS fields (e.g., threat reporting, CIP, intelligence sharing, and support to NORTHCOM). ▶ Current sharing methods and processes are not scaleable and are inadequate for new security environment. Linear, hierarchical information flows and legacy databases contribute to an increasingly outmoded “push” system of information sharing. Complex networks of relationships encouraging horizontal information flow may be a better model (e.g., current information-centric warfighting operating concepts). 	<ul style="list-style-type: none"> ▶ Significant cultural barriers to sharing, largely the result of a mentality that emphasizes data ownership; “push,-”-based information sharing requiring DoD to know the needs of other agencies, a limited view of the “need to know,” and institutional disincentives to openness. ▶ Perceived lack of leadership commitment and focus conveys low priority on HLS-related requirements. ▶ Limited interagency interface or understanding as to what information is needed from DoD by other agencies, from other agencies by DoD, and among DoD agencies. ▶ Policy and doctrinal guidance shortfalls inhibit mature information sharing relationships and processes. ▶ Legal misinterpretations of laws regulating information sharing, and often times undue caution result in greater risk-aversion to sharing than is merited by the laws themselves. ▶ Classification procedures encourage over-classification and inhibit efficient, standardized processes such as tear sheets for declassifying and sharing information. ▶ Technology is necessary to enable improved information sharing and analysis—HOWEVER, without leadership, cultural, and organizational change, improved HLS-related DoD info sharing will not occur even if technology exists.

Effective approaches are evident in specific and specialized areas, such as the exchange of scientific and technical information within the Department as well as with external entities. In some cases, especially in the intelligence agencies, information exchange is highly formalized and conducted within well-defined and clearly understood boundaries. Policies and procedures have grown up around existing information exchange mechanisms, reinforcing the stovepiped nature of sharing and making significant change hard to achieve. Although innovative ideas for new approaches to information sharing abound, they quickly bump up against strictures of existing policies and procedures. This phenomenon is mostly apparent in dialogue between DoD and other departments, where implementation of cross-organizational initiatives can be easily delayed or stymied.

Leadership and cultural issues are seen as presenting the greatest impediments to improved information sharing in DoD. Among the issues identified are long-held cultural beliefs, poor coordination of analysis and lack of analytic capability, inability to downgrade or declassify information for sharing, and failure of DoD to catalogue its own assets systematically and dynamically. Policy issues loom large in the context of existing impediments.

Security and classification issues are important impediments. The current trend is based on application of the traditional, national-security model to classified information-sharing needs for homeland security. However, the traditional model is not well-suited for the information-sharing environment for HLD/HLS for several reasons:

1. Vetting individuals for security clearances is a slow and costly process, with no real assurance that the suitability factors investigated ensure trustworthiness.
2. The widespread belief in state, local, and private sector stakeholder communities that the Federal Government has “silver bullet” information that, if only released to the proper authorities, would “solve” all homeland security challenges is (however untrue) further validated by the continued use of national-security clearances and has the unintended consequence of inhibiting more collaboration among state, local, and private sector authorities that could make an important difference.
3. The current national-security model is based on “need-to-know” established by the collectors or producers of the data and then classified accordingly, precluding any sharing of that information that may be of use to homeland security officials whose “need-to-know” for that information has not been established because they are not part of the traditional clearance system.
4. The technology for securely providing HLD/HLS information is not widely available to those outside the national-security community, does not scale well, and is cost-prohibitive for most state governments.

Despite these complexities and recognizing that granting security clearances to all state, local, and private sector officials with security responsibilities is not possible, the basic trend is nevertheless moving towards increasing the number of people with security clearances. DHS has authorized security clearances up to TOP SECRET for a limited number of state officials and SECRET clearances for more state, local, and private sector representatives. The FBI has granted SECRET clearances to state and local law enforcement officials to support expanded cooperation on anti-terrorism since 9/11. And the National Guard, in pursuing its new goal of establishing a “joint forces command” type structure for the fifty states will surely pursue clearances for more state and local officials.

In addition, plans are already well underway to provide secure communications (e.g., Secure Telephone Instrument – STEs) to governors, mayors, and law enforcement officials. Some private sector owners/operators of critical infrastructure also have clearances and DoD entities share with them classified threat information on a need-to-know basis. For example, USTRANSCOM shares information concerning specific threats to U.S. airlines with cleared representatives of the affected airline. USTRANSCOM has also established a web-based information sharing capability for Sensitive-But-Unclassified information sharing with public and private-sector participants in the Defense Transportation System. At the same time, DHS is leading an effort to define a new category of sensitive information, “SHSI” or “Sensitive Homeland Security Information,” that will allow a fuller exchange of sensitive information between the government and private sector. SHSI will provide another conduit for the flow of sensitive information outside the traditional classification system.

Directly related to security policy is the issue of handling of data related to U.S. persons. The intelligence community is bound by the policies set forth in Executive Order 12333 and substantial case law derived from the Foreign Intelligence Surveillance Act of 1978 (FISA). The law enforcement community is also subject to FISA but not to Executive Order 12333 and has different standards for treating U.S. person information. These policies and their continued interpretation in pre-9/11 terms inhibits effective information sharing for homeland

security, as pointed out in the Congressional “Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001.” A new category of person-specific data that would bridge the law enforcement and intelligence communities and enable a more substantive dialogue on terrorist-threat information is required.

Cultural barriers to exchanging information exist universally today and are another fruitful area for policy discussions. These barriers exist in part because of the collision of traditional communities of interest (e.g., intelligence and law enforcement) in the context of HLD/HLS. The establishment of DHS has complicated the situation by adding another stakeholder community to the mix. All stakeholder communities have similar information needs, but have not yet established the working relationships necessary for consistent and effective interaction. The figure below depicts the current situation.

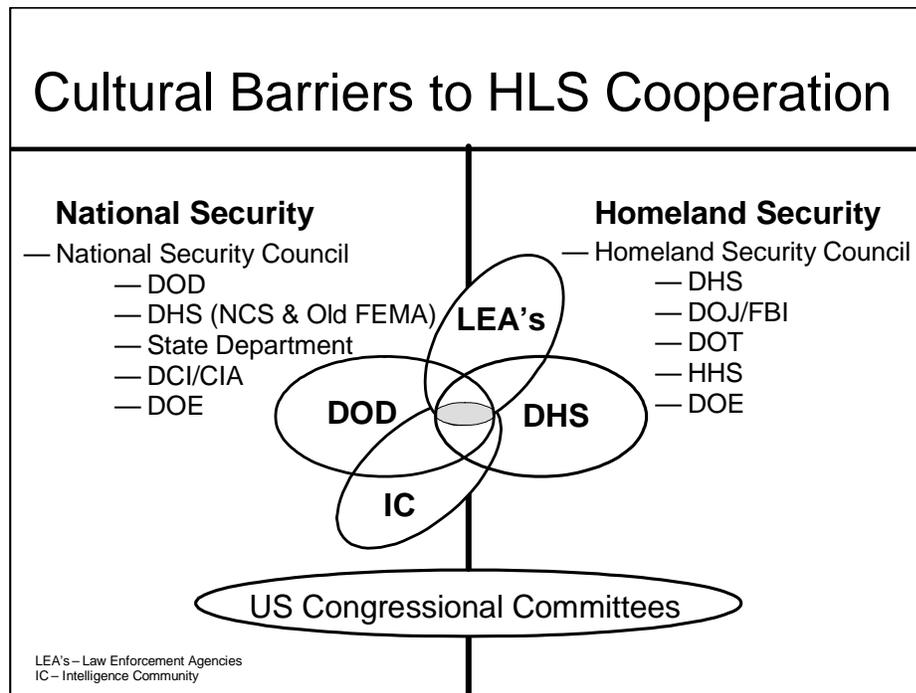


Figure 6. Cultural Barriers to HLS Cooperation

Other cultural problems run deeper. For example, current promotion and rewards policies reward the “knowledge is power” syndrome, reinforcing traditional practice and exacerbating the lack of information sharing across organizational boundaries. While senior officials are being briefed that information sharing is being expanded, the process is in many cases ad hoc and there is a danger that those steeped in DoD’s traditional culture will out-wait an administration that is not in alignment with traditional beliefs and practices. Most information sharing in DoD today is based on partnerships and relationships that pre-existed 9/11 and (with the exception of the National Guard and NORTHCOM) does not include non-traditional communities such as state governments. The GAO noted in its August 2003 report on information sharing that the DoD and Intelligence Community culture, “perceives the fight against terrorism as a federal responsibility and consequently does not

integrate state and city governments into the information-sharing process.”

3.3 *EFFECTIVE INFORMATION SHARING MECHANISMS*

Building effective information sharing mechanisms involves policy and cultural changes as well as some new technologies. Because information sharing is central to so many activities in DoD and elsewhere, useful models and best practices (such as those used by the Defense Technical Information Center (DTIC) and Web-based systems such as Intelink) already exist that can be brought to bear on the homeland security problem. There are important, cross-cutting technological issues that must be addressed, such as multi-level security and information assurance in general, but the major barriers to achieving effective information sharing tend to be in the areas of policy and culture. The highest potential for “breakthroughs” in HLD/HLS information sharing lies in reshaping organizational culture and interactions among and between stakeholder communities through innovative approaches to sharing information using existing technologies.

Those who collect and produce information in the intelligence community are “graded” on the quantity and (hopefully) quality of their material. Their fortunes are not, however, directly tied to *uses* of their materials. The intelligence community and the law enforcement community should arrange their respective incentive structures in such a way that collectors and producers are encouraged to ensure that their materials are widely received, digested and used. In fact, both the collectors of the future and the analyst/reporter/data warehouse information managers are going to have to be schooled and given tools, as well as such incentives for how to live in the world of the future where, at one end they have a statutory responsibility to protect sources and methods and, at the other, get the data to the widely diverse user set associated with homeland defense and security. Entrepreneurial processes should be enabled so that individuals held so accountable can affect the final disposition of their products. The consumers, themselves, should parcel out these incentives.

The figure below depicts a reward system for successful information sharing.

Figure 7. Rewards for Information Sharing

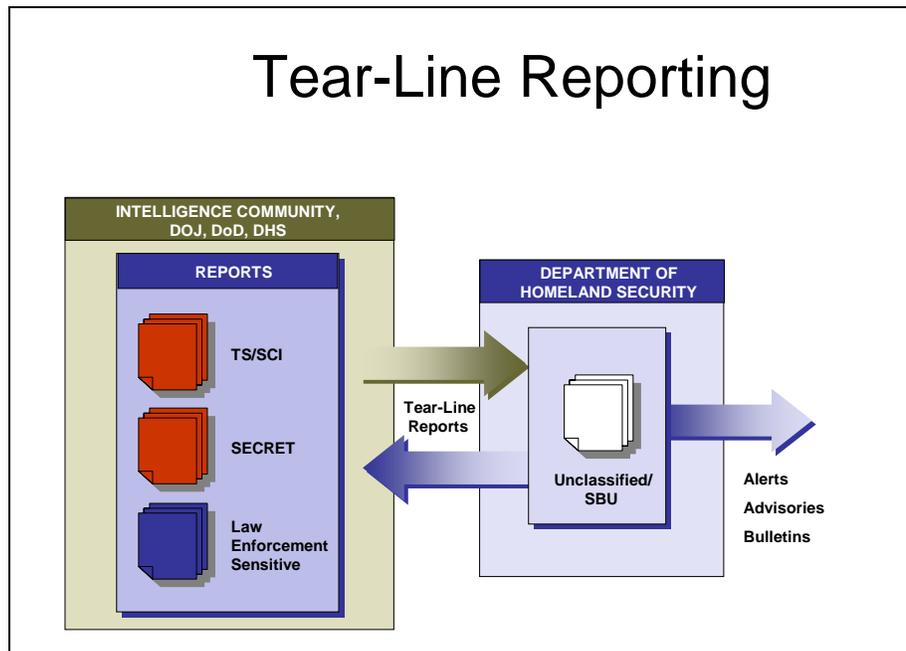


The Panel has reviewed many approaches to information sharing inside as well as external to the Department and has debated at length the advantages and drawbacks of each. The most promising approaches are discussed below.

Tear-Line Reporting – For several years, intelligence elements have provided a second version of highly classified information at a lower classification level. The lower classified information comes at the end of a report, separated by a “tear line.” Typically, a SECRET version of information is provided under a tear line on a TOP SECRET report, although UNCLASSIFIED/FOR OFFICIAL USE ONLY tear-lines are also provided on SECRET reports. Since most homeland security stakeholders do not have security clearances above SECRET, the use of tear-line reports is laudable and should be expanded, as called for in the Information Sharing MOU signed by the DCI, Attorney General, and Secretary of Homeland Security for information being shared with DHS. A more useful approach would

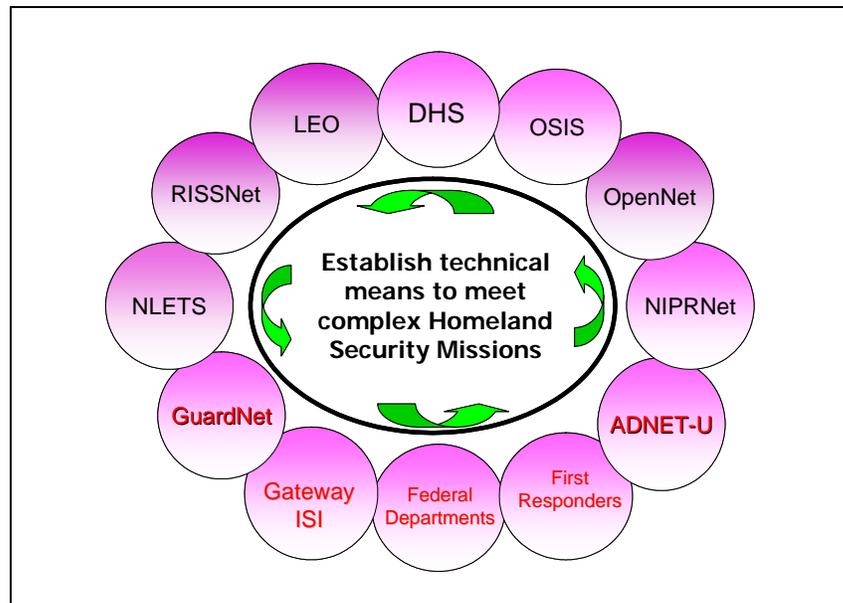
be to first produce the tear-line information and then add the more compartmented details as “meta-data.”

Figure 8. Tear-Line Reporting



Federated Sensitive-But-Unclassified Network – DoD and the intelligence and law enforcement communities have provided analysts with protected access to the Internet and other unclassified networks. Examples include the NIPRNet, supporting DoD, OSIS (Open Source Information System), supporting the Intelligence Community, and RISSNet (Regional Information Sharing Support Net), supporting DoJ. Authorized (but not necessarily cleared) users are provided access to these networks to research open-source material available via the Internet and to facilitate information exchange across organizations. DHS, with a boost from DIA, is considering the concept of “fusing” these networks into a homeland security network for Sensitive-But-Unclassified information.

Figure 9. Conceptual model for a federated SBU Network



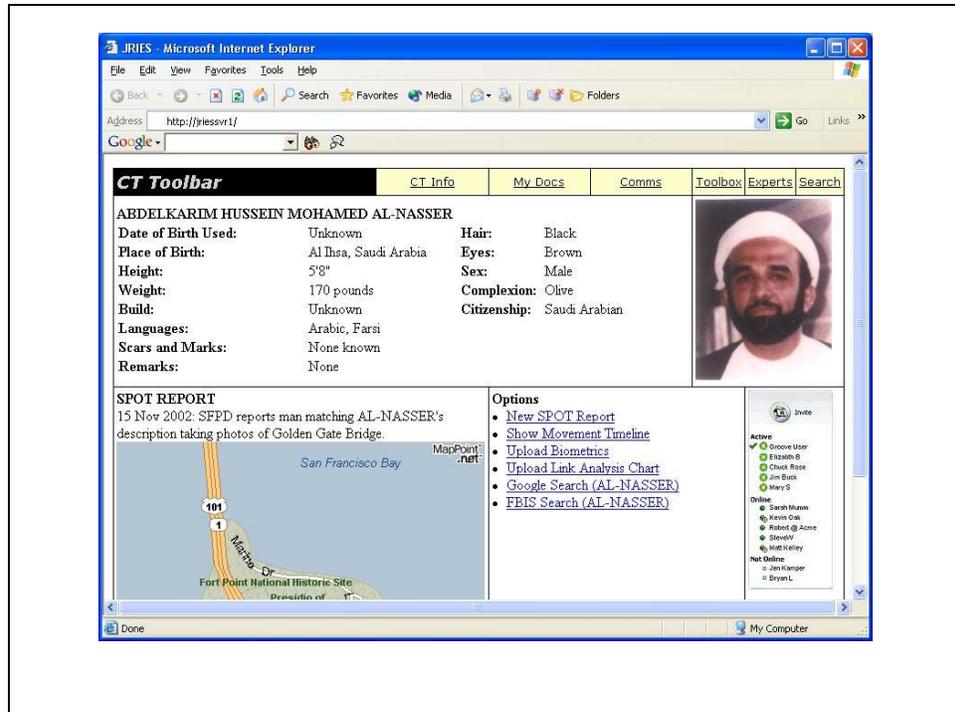
IACs – DTIC has established “Information Analysis Centers” (IAC) in 13 areas of interest to the S&T community. These IACs have web-based interfaces, backed by appropriate security protocols that allow users to gain information, submit queries, and gain access to subject matter experts. In just one example of many, the Chemical & Biological Defense IAC supports the Naval Air Warfare Center with information concerning agent testing on individual protection suit materials for the Joint Protective Aircrew Ensemble, JPACE. Some IACs already support HLD/HLS information sharing.

TRANSCOM DTS Initiative – TRANSCOM has an important information sharing initiative with its Defense Transportation System (DTS) partners. TRANSCOM has developed a prototype information-sharing portal to convey threat information on U.S. ports, the civilian transportation industry, military logistics, and CONUS forces to its commercial transportation partners. Working through its component commands, TRANSCOM is developing a two-way approach in which the command will receive threat information from the commercial transportation industry and will provide SBU threat information to airlines, ports, and other partners who provide services in support of TRANSCOM’s mission. TRANSCOM also

disseminates classified information to appropriately cleared personnel at U.S. airlines, airports, and ports.

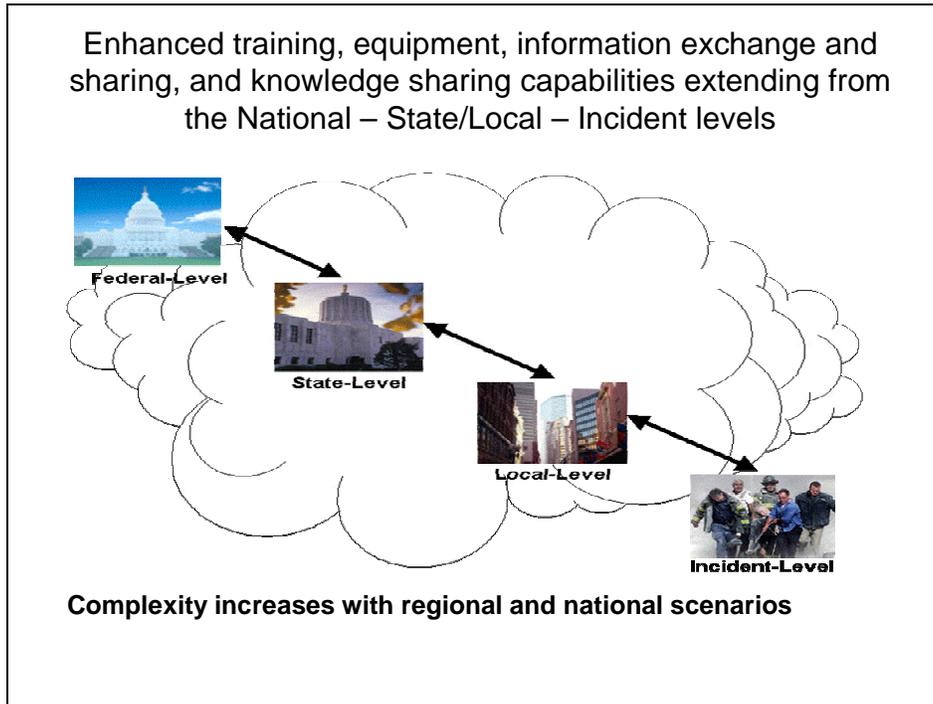
JRIES – The “Joint Regional JTF-CT RISSNet Information Exchange System” began as a DIA initiative to improve the exchange of counterterrorism information among federal, state, and local organizations. Begun as a pilot in late 2002 and subsequently adopted by DHS as the standard for sharing information between DHS and state and local homeland security officials, JRIES provides for the collection, analysis, collaboration and warning of terrorist threats. Using existing networks and cost-effective collaboration technology, JRIES provides for the real-time exchange of information and collaboration of federal and local officials in response to potential terrorist threat information. The goal of JRIES is to provide a consistent user interface to leverage existing investments in analytic tools made by federal and local agencies. See Figure below.

Figure 10. Sample JRIES Web Page



National Guard – In its Title 32 USC role (support to governors), the National Guard has taken a lead role in homeland security. Adjutant Generals in many states serve as the head of their state's emergency management effort, homeland security adviser, or both. The National Guard also has homeland defense combatant responsibilities in its Title 10 USC (support to the Federal Government) role. In both its state and federal roles, the National Guard is promoting information sharing between federal, state, and local authorities in support of homeland security. Some of these initiatives involve using "GuardNet" for the dissemination and exchange of information. (See Figure below.)

Figure 11. National Guard Concept for Homeland Security Support



NIMA NGA – The newly designated National Geospatial Intelligence Agency (formerly NIMA) has designated responsibilities for homeland defense, for example support to the U.S. Coast Guard in maritime border protection. They have participated in several exercises focused on homeland security, such as SOUTHCOM Blue Advance 02 (Sep 02), with a scenario postulating weapons of mass destruction in Puerto Rico, and the DOJ/DoD (JFCOM) TOPOFF Exercise in May 2003, focused on the national response to simultaneous bioterrorism, chemical and radiation event in two different CONUS cities. In addition, NGA has conducted several demonstration projects for providing support to homeland security, for example in providing support for critical infrastructure protection. NGA has the tools and ability to provide more information sharing for homeland support, but lacks the policy authorization to do so (i.e. NGA support to non-federal agencies must be provided via FEMA).

4.0 IMPROVE INFORMATION ANALYSIS

4.1 *KEY FACTORS FOR IMPROVED ANALYSIS*

The DSB Task Force Report on “Improving Intelligence in Support to the Global War on Terrorism” was published in 2003. This report contains a framework and recommendations for improving the posture of the foreign intelligence community to more deeply penetrate terrorism threats. This Panel used this report as a starting off point for its consideration of how to improve information analysis in support of homeland security. Critical to its conclusions are concepts such as:

- Making intelligence more proactive and provocative
- Instilling better research skills in intelligence
- Institutionalizing abilities to do continuous and iterative target development involving collectors, technologists, operators, etc.
- Improving the depth and quality of analysis through, e.g., working smarter by hiring experts with strong language and country cultural expertise
- Maximizing the relationships and programs defined around terrorism, including focused specialized forces and capabilities (which includes Special Operations Forces, and IC Covert Action forces and other elite IC capabilities)
- Dramatically reinventing HUMINT in DoD and improving HUMINT in IC

This section addresses three aspects associated with improving information analysis: growing and improving the analyst corps, analytic tools and techniques, and new sources of data and information.

A key first step to improving analysis is to acknowledge the need to collect and evaluate intelligence on a wide variety of factors. These include understanding new adversaries' views and operating patterns in the following areas.

Operational Secrecy: To succeed, terrorists must achieve and maintain secrecy, relying on several forms of vetting of persons, long term relationships, commitment validated by acts, and other similar kinds of measures. They follow rules that might be referred to as operational tradecraft, including approved communications and interpersonal interaction methods, hiding their true identities, and not engaging in activities that appear to be excessively risky to their discovery.

Philosophical Motivation: Terrorists are usually motivated by deeply held philosophical beliefs and there must be a more robust understanding of this. Root causes underlying terrorist motivation need to be derived. Similarly, the cultural anthropological issues need identification and insights must be derived regarding how to manage the information, public diplomacy, operational and intelligence aspects.

Committed Persons: This is not a modern phenomena – history is filled with accounts of zealots and fanatics who gave up their lives for a cause or a belief, but the “suicide combatants” of recent years are especially difficult for U.S. analysts to study and understand.

Money and Other Support: Terrorists and the groups and organizations they belong to need money and other kinds of support (equipment, capability, facilities, transportation and communications support, identity modification, and numerous other expensive needs) and tracking these sources of support is critical.

Insightful Leadership: Terrorist leaders often are very shrewd at calculated risk taking, careful planning, timing appropriate to conditions, the orchestration of numerous features of the plan, and successful execution of operations. In the past U.S. law enforcement and intelligence analysts have underestimated some terrorist leadership.

Organizational Identity: Many terrorists have a multi-faceted approach to organizational identity. By definition, they belong to a secret group, often one that should not have (does not have) a recognizable form or identity. Meanwhile they may belong, at least philosophically, to a larger organization that they are willing to identify with. This has become a feature of the “hide in plain sight,” phenomena. A person, who is publicly identified as a member of Hamas or Hezbollah, may also be a secret member of an interior group or effort, carrying out acts of terror or supporting terrorism.

Operational Capability: Terrorists and the organizations and groups they belong to, need a ready operational capability to facilitate their acts. This means that they need all of the resources, tools and options that they require, ranging from the common and mundane, like spending money, to the sophisticated and complex, like an at-hand WMD capability that they can and will employ on order. This implies a logistics and support structure in parallel with or concurrent with the operational terrorist action element.

Intelligence Support: This requirement is fundamental to all terrorist activity. It is a precursor to targeting, a necessity to ensure operational secrecy and security, and a vital tool in operational success from beginning to end of any terrorist operation, and indications of such activity needs to be identified and categorized.

The Concepts of Terror: U.S. intelligence and law enforcement analysts must be able to think more like terrorists in order to properly evaluate fragments of information in a timely fashion.

4.2 GROW AND IMPROVE THE ANALYST CORPS

During the 1990’s, reductions in the intelligence community budgets forced reductions in the numbers of intelligence analysts. At the same time, the breadth and scope of intelligence requirements grew as the United States responded to global forces of unrest, including terrorism. While a Counterterrorism Center was established at CIA, events of September 2001 dramatically illustrated both the vulnerabilities of the United States and the lack of

capabilities to identify, track and respond to terrorist threats--- particularly in the continental United States.

A spate of activity in the past year has focused energy, and in some cases, resources on improving intelligence capabilities; e.g., creation of the TTIC and Department of Homeland Security with its Information Analysis Division. The DHS is gaining additional billets to hire new analysts (as has the FBI), but many more new analysts are needed in the Intelligence Community, specifically including the intelligence community resources in the Department of Defense such as DIA, JTF-CT, and selected military department intelligence analytic and HUMINT resources. Additionally the panel's discussions with JTF-CT highlighted the importance and potential power of improved information sharing to U.S. counterterrorism activities.

Becoming an expert analyst requires time and focus, in addition to the obvious needs for intellect and education. This nation's premier analysts have spent years in their profession and years focusing on particular topics or areas of study. The reductions in intelligence budgets over the decade of the nineties caused a commensurate reduction in the analytic communities. During this same period, the United States felt compelled to track more and more events globally rather than focus on the communist bloc/Soviet Union. The natural consequence over time of this dichotomy was fewer analysts tracking much larger geographic areas and the increasingly complex problems associated with them. As a result, we have fewer experts, and lack expertise in some significant areas including:

- Counter-terrorism,
- Weapons of mass destruction and effect,
- Knowledge of how potential adversaries "think,"
- Understanding Islam and the islamist or fundamentalist groups of Islam,
- Relevant language skills,
- And numerous others.

The Panel concludes that, if we are to find “more needles”, more analysts are required as well as substantial improvements in their education, training and the tools and techniques that support them. An analyst’s expertise can vary depending on the relative degree of regional knowledge, familiarity with disciplinary theory, and with intelligence methods in general.

Regional and domain expertise is essentially area studies: a combination of the geography, history, sociology, and political structures of a defined geographic region. The Intelligence Community regional offices are responsible for an analyst’s regional expertise and develop it by providing access to language training, regional familiarization through university courses, or in-house seminars.

Disciplinary expertise relates to the theory and practice that underlies the individual analytic occupations. For example, economic, military, political and leadership analysis are built on a bed of theory derived from the academic disciplines of economics, military science, political science, and political psychology, respectively. This same expertise is required in the area of terrorism and counter-terrorism. Disciplinary expertise can be acquired through previous academic coursework, on-the-job experience, or supplementary training.

Choosing Analysts - Analysts that are either deliberately selected for counterterrorism (CT) intelligence work or who migrate to that work by a variety of pathways are not specifically or distinctly made into CT analysts until they have performed on the job, have been mentored or “trained,” in some way, and have produced over some period of time in which senior analysts and leaders have assessed them and designated them as bonafide CT analysts. Finding analysts will likely be a big issue for the Nation. New approaches to using cultural and language-capable people will need to be developed and pursued by the intelligence community. The community must come to grips with accessing talent that does not have to be cleared into highly sensitive channels in order to be effective.

Training Analysts - While structured training programs exist to help analysts understand intelligence community roles and missions and resources and develop proficiency with automated tools, training of analysts remains largely an On-The-Job (OJT) process for regional and domain expertise. Training requirements include, for example: how to use specific databases and what inter-community terms mean. There are specific communities of interest, for example the CT-Link community of interest that can be used by anyone with a normal knowledge of browsers on web sites, but cannot be used optimally without some form of training. As the CT knowledge base has evolved over time, there are certainly training opportunities for new analysts to be informed and empowered, and for longer term analysts to be refreshed in their knowledge base. Cross training between and among agencies and CT groups would be very valuable. The Information Sharing and Analysis Panel recommends that this subject be explored by the CIA University (CIAU) and the Joint Military Intelligence College (JMIC), and by the counterpart training and educational elements of the IC.

Sustaining Analysts Over A Career. Sustaining an analyst in CT work over a long period of time seems both professionally right to do and necessary in order to maintain continuity against the terrorism / terrorist target. Since we are many years into CT work, but only a couple of years in to what now seems to be a long term effort by the Intelligence Community to combat what we assess now to be a continuing and lasting phenomenon, some form of specific and distinct career track for CT analysts is desirable. The Intelligence Community has begun this work. DoD CT leadership should investigate what they have done and adapt it to the DoD CT analytic workforce. Other parts of the nation's homeland security structure should join in this effort.

4.3 IMPROVE AND EXPAND ANALYTIC TOOLS AND TECHNIQUES

A primary concept in analysis is the fusion or the bringing together of data in order to form a coherent and complete account of the topic...whatever that topic is. That data is textual, visual, audible,

mathematical, graphical, and multi-featured. It is composed of many gradations of quality and quantity and it is tied to time, area, space, speed, tempo, and human cognition among other things. Relationship and pattern, linkages and nodal centers, and numerous other facets of the data exist. It is complex in many ways. Data in the modern context is, if nothing else, voluminous. There is so much of it and it is in so many different forms that dealing with it is a challenge. In fact, in many ways human analysts cannot comprehend what it means without assistance. That assistance is often found in some form of synthesis and in finding the critical essence of meaning and import out of the larger data set.

During the course of the Panel's deliberations, stakeholders discussed their choices with regard to analytic tools. Some analysts employ the "best of breed" commercial off the shelf (COTS) tools and approaches. Others take government off the shelf approaches (GOTS). Some are directly involved in commercial or governmental research and developments activities related to analysis and data mining, such as the Defense Intelligence Agency (DIA) program known as Joint Intelligence Virtual Architecture (JIVA). There are many others.

The Panel is not recommending specific programs, processes or capabilities, but proposes that the Intelligence Community empower a group of seniors to evaluate options and make choices for the community as a whole because the United States cannot continue indefinitely to allow multiple diverse and dissimilar capabilities to be purchased and used in the IC without regard to interoperability, synergy and seemingly redundant costs.

To support both Homeland Defense and Homeland Security, a cogent need exists for computational, software, hardware and procedural tools that will assist in the following analytic functions. In order to optimize the effect of these tools some form of standard and interoperability must be applied. The following capabilities are essential:

- Pattern Analysis: One way to determine what a terrorist or a terrorist group might do in the future is

called pattern analysis – the discerning of some repeated or repeatable activity over time against context.

- Link Analysis – The analytic establishment of the fact of or the possibility of linkages of various kinds (relationships, associations, communications mechanisms, etc.), between nodes, and perhaps penetrating those links in order to gain access to intent or to some other useful information.
- Node Analysis – The identification of persons or groups (organizations, supporting elements, sympathizers, State sponsors, etc.), and facilities, locations, and other spatially defined information, and their inter-relationships through the link analysis effort.
- Individual Identity & Relationships – The specific identification in as much detail as possible of terrorists and persons of interest who are involved in some way with terrorist activities. This particular form of information is fraught with legal and procedural issues, especially when U.S. persons are involved.
- Group/Organization Identity and Relationships – Group/Organization (G/O) identification and information adequate to know what the G/O is, engages in and is capable of, is critical to developing a useful knowledge base.
- Communications Linkages – The fact of a link and its technical characterization (interpersonal, electronic, conventional mail, clandestine, etc.) is also critical to understanding how a terrorist or a G/O works and also presents one potential for penetration. There are many forms of linkage but those listed below, without further explanation here, show the breadth and depth of this intelligence focus. There are many variations on each of these themes.

1. Telephony

2. Computer / Modem
 3. Facsimile
 4. Radio
 5. Mail
 6. Hand Delivered Messages
 7. Cargo & Commercial Delivery
 8. Other Communications Mechanisms
- Data Base Development and Management – This functional need is perhaps the most complex. The volumes and different nature of data have been noted. The need is to develop fully relational and autonomously interactive databases, at least up to some point at which human intervention is required in order to validate an action or to allow the transfer of data or the posting of data.
 - Automated Production Systems – the need to greatly improve the accuracy, clarity and timeliness of intelligence products in as much of an autonomous way as possible. Tools to do this exist and are in use in commercial enterprise and in the government. The CT analytic community and the larger IC should focus on and acquire the best capability to meet the many needs of the customer set. There are great differences between what you can put on a laptop screen and what you can communicate in a substantial printed document. Images shown in inadequate form are less effective than they might be. Mapping, charting and geodesy products require an entirely different production approach than textual documents.
 - Metadata Tagging, Extensible Markup Language Applications, and Other Digital Interaction Tools – The idea of maximizing the digital forms we work with so that data can be separated, associated, parsed, sifted, mined and otherwise made to have analytic and

synthesized meaning, compels us to apply the best tools we can get to enable those applications.

- Display and Presentation Capabilities – Similar to automated production systems, the best capabilities are needed to display and present intelligence and other information forms. Visualization tools offer dramatic leverage to intelligence and law enforcement analysts attempting to integrate available data in the context of their roles and responsibilities.

4.4 IMPROVED SOURCES OF DATA

The 2003 DSB report on Improving Intelligence in Support of the Global War on Terrorism also suggests a number of initiatives aimed at improving data and information sources:

- Major new initiatives in improving overall battlefield ISR in areas such as improved dwell/ persistence, pervasiveness/ definition and penetrability/ survivability/ stealth (This is achieved by a revolution in space, air, ground, underground, and maritime sensing and netting.);
- Putting substantial effort into dramatically improving its overall clandestine human-technical capabilities for new sources, methods, concepts and capabilities for penetrating hard targets; and
- Working more with industry.

The continued development of collection and target access capabilities is important in order to expose and define terrorism threats, both foreign and domestic. One of the highest leverage areas for improving the ability to collect against terrorism threats is a rigorous, disciplined, doctrinal process of continuous target development. This means that the TTIC and others involved in analysis must first start their day dealing with what is known, (and more importantly) what is not known, and how to get the critical threat information required. If for example, the question is “where is Bin Ladin, and what is he doing,” then it is the implied job of TTIC to

properly frame that question on a continuing basis, and to work relentlessly in a circumscribed process with the collectors, operation personnel, leadership, resource and collection managers to define how the answers to those questions are being pursued. In this process, there is a need to focus equally on what it is that is not known. Likewise, the domestic intelligence activities must develop analog methods to focus on priorities linked to leads provided by foreign intelligence and enhanced collection means. It is only these tight couplings between collection and analysis, and between foreign and domestic intelligence processes that will define and differentiate the improved potential to be broadly successful in pre-accessing and blunting threats to this Nation.

A major collection priority is assigned to HUMINT, but a reinvented HUMINT which is at once human -derived and at the same time, fully augmented with technical extensions. These technical extensions must be on the shelf, available, and protected from compromise. This is an area that is substantially under-invested and not optimally focused, and where a major partnership with industry and national labs should be pursued. This requires an elite force of specialized people and capabilities (who are not in large supply and are difficult to grow), and the nature and character of their operations and technical access means must be improved and kept secure.

A special relationship must exist between HUMINT and Special Operations Forces (SOF), as well as a special relationship between the Covert Action operations of the Intelligence Community and special actions undertaken by SOF. The sensitive results of collection must be handled in a manner so as to sustain the source and method over time, and creative ways must be derived to adequately share the product of such specialized collection without exposing the source. In particular, HUMINT professionals must find ways to better evaluate their sources, and it is possible that technology and other new management and policies can be applied in this critical area.

Intelligence collection and analysis must support the effective conduct of Information Operations and Warfare (IO/IW). Impacting the minds of the adversary and his support system, and conveying a

sense that they are not in control of their environment and forces, is a subtle activity, and must be supported by deep penetration collection operations in order to discern the thoughts, plans and direction of the threat leadership and support elements. There is a special obligation in counter-terrorism to remove the root causes of this threat, and intelligence support for the effective conduct of IO/IW can play an important role in achieving that goal. Intelligence is under-invested in supporting these activities.

All of the other intelligence functions have areas where they can contribute. Major upgrades in SIGINT, IMINT/MASINT and Open Source (OSINT) access are required. Most critical to the success of such upgrades would be most widespread convergence and integration of the back end of the intelligence system. This back end would be highly interactive with the front-end collection, but it would also be characterized by disciplinary and general purpose all source analysts who are physically and/or collaboratively collocated so as to create the maximum degree of target development and focus defined above.

In dealing with the hard and elusive terrorism target, it is not possible to maintain separation between either the collector and the analyst, nor the collectors and analysts of the individual disciplines. This suggests that major organizational, process, doctrinal and collaboration approaches are required to create a more pervasively horizontally integrated community, and to define new methods in which the security of activities is to be maintained while maximum information sharing is facilitated, a difficult but not impossible task.

Finally, in the collection area, as with other areas, the partnership that exists between government and industry is critical to the success of transforming the DoD and IC to more effectively deal with the terrorism threat target base. This means defining new ways of doing business, maximum use of DCI special authorities for streamlined acquisition, and most of all, creating the dynamic which inspires new levels of excitement and creativity in the collection, analysis and information access business. The current trend toward "horizontal integration" and better and more efficient convergence and melding of the communities overall means is important to a successful

outcome in the terrorism collection and related areas, and this effort should be more explicitly defined, resourced, and managed by intelligence and the industry which supports these fields.

5.0 FINDINGS AND RECOMMENDATIONS

5.1 *STRATEGY AND PLANNING*

There is an urgent need for overall leadership and guidance for the many information-sharing initiatives underway in the Department of Defense and between the Department and federal, state and local entities. Absent a coordinated approach, these efforts will continue to expand to address specific requirements but will not improve the overall national homeland security effort.

RECOMMENDATION #1:

Bring coherence to DoD information-sharing initiatives through establishment of a joint working group sponsored by USD(I) and the DoD CIO and including OSD, the Commands, and Defense agencies. The goals of this effort should include:

- Development of DoD guidance for the sharing of HLD/HLS information with federal, state, and local entities, including policies and procedures for sharing sensitive-but-unclassified as well as classified information
- Use of the DoD CIO's "Net-Centric Data Management Strategy" as the framework, collaborate with DHS and other agencies in the design and deployment of a national HLD/HLS information-sharing architecture involving all stakeholder communities and addresses all information needs in a common technical and operational environments

5.2 *POLICY AND PROCEDURES*

The absence of the Secretary of Defense's signature on the Information Sharing MOU signed by the DCI, Attorney General, and Secretary of Homeland Security is a potential source of confusion and misunderstanding, especially for DoD agencies that are part of the Intelligence Community.

RECOMMENDATION #2:

The Undersecretary of Defense (Intelligence) should issue an implementing instruction to clarify DoD's support of the Information Sharing MOU and to promulgate guidelines for implementation.

- Current policies derived from use of the traditional national security classification schematic do not facilitate the sharing of homeland defense and homeland security information among all stakeholder communities.

RECOMMENDATION #3:

DoD should explore creation of a new class of data and commensurate security policies and procedures to guide implementation. This new data class and associated policies and procedures may exist outside the traditional national security information classification schema and will be inclusive of any/all U.S. homeland security stakeholders.

- The new data class should be built around the concept of "sensitive but unclassified" information, a term derived from the discussions of the Computer Security Act of 1987 and in growing acceptance for a variety of applications. (For example, the term "Law Enforcement Sensitive" is used for sharing sensitive-but-unclassified information within that community.)

Existing guidance on the handling of "U.S. persons" information inhibits the exchange of counterterrorism information among intelligence, law enforcement, and homeland security professionals.

RECOMMENDATION #4:

The Secretary of Defense and DCI, with the Department of Justice, should co-sponsor a thorough review of current laws and regulations and determine the best approach for treating U.S. persons data in the context of terrorist threat information. The new approach must allow for the free exchange of terrorist-related information between the intelligence, defense, and law enforcement communities while at the same time protecting the privacy of American citizens.

- Yearly re-indoctrination in the rules for minimizing intrusiveness—e.g., U.S. Signal Intelligence Directive (USSID)-18—should be accompanied and balanced by the counterpoint recognition of the importance of sharing.
- Information subject to one minimization regime—e.g., USSID-18—should be releasable to another accountable intelligence organization with its own minimization implementer similarly approved by the DoJ.

Current incentives policy, including Departmental, agency, and organizational promotion and rewards policies, inhibit sharing by stressing the value of data “ownership” as opposed to sharing.

RECOMMENDATION #5:

DoD should promulgate a policy requiring increased information sharing and rewarding those individuals and organizations who aggressively implement the new policy by expanding incentives to encourage greater sharing.

5.3 TECHNIQUES AND OPERATIONAL APPROACHES

Information sharing for HLD/HLS data is hampered by the lack of a coherent network or network architecture that allows for the exchange of classified as well as Sensitive-But-Unclassified (SBU) information among all stakeholder communities.

RECOMMENDATION #6:

DoD should initiate a study of the feasibility of a national SBU network for sharing homeland security information with results due in one year.

RECOMMENDATION #7:

Develop a national SECRET network to support federal, state, local and private sector stakeholders to enhance information sharing of classified HLD/HLS data.

- National SECRET Network – While the “federated SBU” network described above will allow for the exchange of sensitive-but-unclassified data and will accommodate much of the information sharing requirements for homeland security,

there is also a need for a “national SECRET network” to allow for the exchange of classified information among homeland security stakeholders at the national, regional, state, and local levels. DoD’s SIPRNet is the network of choice for SECRET information today, including some subscribers (e.g. Coast Guard) who are not part of DoD. As homeland security information exchange protocols mature and more state/local and private sector officials are cleared, SIPRNet capabilities will be stretched, if not physically then in terms of DoD policy: how many non-DoD users should be on SIPRNet? A national SECRET network, using commercially available communications and information assurance technologies is well within reach in one year and should be pursued. This national SECRET network would employ the concepts and as appropriate the architectures embodied in the DoD CIO’s framework for “horizontal fusion” and “power to the edge” to push the boundaries of information sharing technologies.

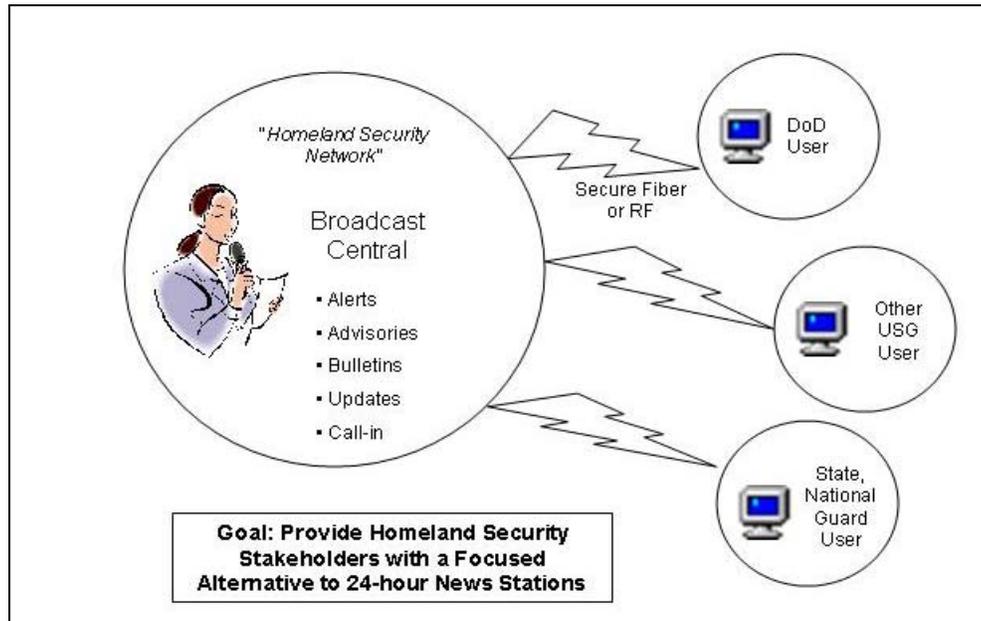
RECOMMENDATION #8

Build a secure TV broadcast to share HLD/HLS information with all stakeholder communities.

- Experience has shown that classified information provided to a few, select, cleared individuals tends to appear on TV within a short time. Aggressive reporting and robust communications architectures allow commercial news broadcasts to flash breaking news around the globe instantly. DoD and the government generally take advantage of this phenomenon: every operations center has televisions tuned to CNN, MSNBC, and other 24-hour news networks. The trend towards real-time news is growing and must be considered as part of the overall information sharing architecture for homeland security. Using the secure video teleconferencing capabilities already provided by DHS to the states, the homeland security broadcast would add value to real-time commercial news broadcasts by providing up-to-the-minute, behind the scenes information for use by governors, national guard elements, and federal departments and agencies. The “HLS Network” could expand or contract its service depending on the flow of events, and could be augmented by special presentations, features, call-in shows,

etc., to greatly enhance the overall understanding of homeland security events and information. (See Figure 12)

Figure 12. Homeland Security Network Concept



RECOMMENDATION #9

Within 5 years adopt paradigms and assured procedures that allow meaningful function exchange of SBU and SECRET data.

- The ultimate goal of some for sharing homeland security information is to provide all information up to SECRET over one network is and will remain a significant challenge. However, assured procedures can accomplish the necessary exchange of information at the SBU and SECRET levels, and it should be possible for any homeland security stakeholder anywhere to have access to specific information or (for SBU users) at least to know that information exists at a higher classification level.

The adversarial Information Operations threat is growing and must be considered in any new concepts, networks, and architectures for the sharing of HLD/HLS information

RECOMMENDATION #10

Significantly increase U.S. collection requirements on foreign Information Operations capabilities, organizations, players and partners, including at least the following specific actions:

- Increase analysis and reporting on foreign IO issues.
- Share this growing body of insight with those responsible for National Information Assurance policy and solutions.
- The National Security Agency's Information Assurance Directorate should be tasked with becoming the national focal point for Information Assurance as it relates to national security. The necessary resources and authorities needed for this increased responsibility must be made available.
- Institute a threat reduction investment strategy. Research, technology investments, and production should be directly tied to decreasing the advantage of the IO adversary.
- Identify data and applications where the benefit of sharing is minimal and the consequence of compromise (confidentiality, integrity, or availability) is unacceptable and provide appropriate technical and procedural measures to ensure isolation. Nuclear Command and Control would be an example of this.
- Identify nodes where a single point of failure could result in dramatic consequence and minimize the application of foreign software and hardware in these nodes. Where foreign components must be utilized, the most rigorous security evaluations must be conducted.
- Develop risk management processes that balance: threat technical/operational capabilities, defensive measures in place, vulnerabilities, operational risk to the adversary, technical and operational cost to the adversary, costs of technical and procedural measures that can offset adversary advantage, and impact of a successful adversary operation.
- Educate senior decision makers on this process and its associated elements.
- Task the National Research Council to baseline U.S. Information Assurance research and its associated impact on mitigating the threat.

- Design our systems and networks to deal with penetrations, insiders, and smart adversaries.
- Commission a national study to examine, in depth, the issues identified in Recommendation #10.

5.4 IMPROVING THE ANALYTIC CORPS

There is a critical need for focusing resources and management attention on hiring, training, and providing career paths for counterterrorism analysts.

RECOMMENDATION #11

That the Under Secretary of Defense for Intelligence join with the DCI and the Secretary of Homeland Security in creating a professional community with career tracks for counter terrorist intelligence analysts.

Counterterrorism training is still in its early stages of development in the Defense, Intelligence, and Homeland Security communities with unrealized opportunities for synergy to achieve more effective analytic training.

RECOMMENDATION #12

The CIA University and Joint Military Intelligence College should be tasked with a joint study to explore cross-training and other opportunities to build a robust national CT training program that would support DoD, the Intelligence Community, and DHS.

Multiple analytic tools have been developed and are being deployed to support the CT mission in various agencies; absent a common framework these tools may or may not be compatible and/or interoperative.

RECOMMENDATION #13

The Under Secretary of Defense (Intelligence) should establish, in concert with the DCI and DHS, a joint Defense/Intelligence Community study to evaluate existing technology developments in the context of intelligence analytic needs for automated tools and techniques, and make choices for programs to be supported with resources and standards, and also minimize "one-off" programs in favor of interoperable systems of broader utility to the HLD/HLS community at large.

5.5 ADVANCED CONCEPT TECHNOLOGY DEMONSTRATION

There is currently no facility for the comprehensive testing of policies and technologies to facilitate controlled sharing in the context of HLD/HLS. The Homeland Security/Homeland Defense Command and Control ACTD provides the framework for testing C2 concepts, but is not focused on testing new policies and procedures for information sharing in general.

RECOMMENDATION #14

Expand the ACTD on "Homeland Security Command and Control" to include requirements for testing of new policies and procedures within the DoD and HLD/HLS environment. This ACTD should also:

- Serve as the testbed for new procedures, techniques, and tools for a network that will span many users at all levels of government. Serve DoD and DHS needs jointly

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A: TERMS OF REFERENCE

THIS PAGE INTENTIONALLY LEFT BLANK



ACQUISITION,
TECHNOLOGY
AND LOGISTICS

THE UNDER SECRETARY OF DEFENSE

3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

06 JAN 2003

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference - Defense Science Board 2003 Summer Study on the DoD Roles and Missions in Homeland Security

You are requested to form a Defense Science Board (DSB) Task Force addressing the Department of Defense (DoD) roles and missions in homeland security.

DoD's historic missions of homeland defense and civil support are under review in light of grave terrorist and other threats to US territory and citizenry. The DoD has access to many of the systems engineering, technical capabilities, relevant technologies, logistics expertise, and modeling and simulation capabilities needed for effective homeland security. Defense forces are also critically dependent upon various infrastructures operated by DoD or provided by commercial sources and civil utilities to support its force projection war-fighting mission and also provide force protection to forces stationed within the homeland.

The development of an effective homeland security capability will involve not only the Department of Defense but the direct participation of many other existing federal, state and local agencies as described in the "National Strategy for Homeland Security," Office of Homeland Security, July 2002.

Some of the key questions related to homeland security, which will be addressed by this DSB 2003 Summer Study, are:

- a. What is "homeland defense" and what specific roles and missions will the Department of Defense (DoD) be responsible to accomplish? What are the derivative unique operational responsibilities of US Northern Command?
- b. What are the prioritized goals for DoD support to civil authorities in a national security emergency? What are the derivative unique operational responsibilities of US Northern Command?
- c. What is the role of the National Guard and Reserve in homeland security? What are the implications for their warfighting mission?



d. What are the inter-agency processes that need to be put in place to support an integrated security strategy, planning function and operational capabilities? What are the processes for interacting with State and local governments?

e. What are the specific information sharing/fusion requirements with DoD and other governmental and non-governmental agencies? Define the processes and evaluate potential technologies to accomplish this requirement. Determine the optimal communications/hardware architectures.

f. What refinement is needed of theater security cooperation methods with Canada and Mexico? What are the short term and long term optimal goals with respect to homeland defense and military assistance to civil authorities for U.S. cooperation with these countries? Suggest a strategy to achieve these goals that addresses treaties, trade, relations, and impacts.

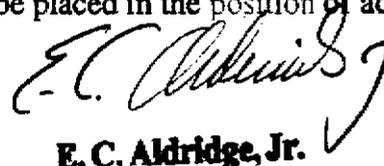
g. There are known and many unknown vulnerabilities regarding DoD force projection. How will projection issues and responsibilities be addressed in the larger context of homeland security?

h. What are the classes of technologies and systems that DoD should have the lead in developing and fielding which have applications for homeland security as well?

Other areas to be addressed by the 2003 Summer Study include: emergency preparedness and response, defending against catastrophic threats, and consequence management in dealing with weapons of mass destruction (chemical, biological and nuclear).

This study will be co-sponsored by me as the Under Secretary of Defense (AT&L), Assistant to the Secretary of Defense (Nuclear, Chemical, and Biological Defense Programs), Under Secretary of Defense (Policy), and Northern Command (NORTHCOM). The study will be co-chaired by Mr. Donald Latham and Admiral Donald Pilling, USN (Ret). Mr. Paul Bergeron, DATSD Chemical/Biological/Defense, Colonel Neal Anderson, NORTHCOM, and Lieutenant Colonel Craig Costello, Homeland Security Task Force, will serve as Executive Secretaries. Lieutenant Colonel Scott Dolgoff, USA, will serve as the Defense Science Board Secretariat Representative.

The Task Force will operate in accordance with the provisions of P.L. 92-463, the "Federal Advisory Committee Act," and DoD Directive 5105.4, the "DoD Federal Advisory Committee Management Program." It is not anticipated that this Task Force will need to go into any "particular matters" within the meaning of section 208 of Title 18, U.S. Code, nor will it cause any member to be placed in the position of acting as procurement official.



E. C. Aldridge, Jr.

*APPENDIX B: INFORMATION SHARING AND ANALYSIS
MEMBERSHIP*

Panel Co-Chairs

Dr. Joe Markowitz	Private Consultant
Mr. Larry Wright	Booz Allen & Hamilton

Members

Mr. Jim Gosler	Sandia National Laboratory
Mr. John Grimes	Raytheon Company
LTG Pat Hughes, USA (Ret.)	PMH Enterprises LLC
MajGen Ken Israel, USAF (Ret.)	Lockheed Martin
LTG Jim King, USA (Ret.)	MZM, Inc.
Mr. John MacGaffin	Private Consultant
Dr. Roy Maxion	Carnegie Mellon University
VADM Mike McConnell, USN (Ret.)	Booz Allen & Hamilton
Ms. Judy Miller	Williams & Connolly LLP
Mr. Bob Nesbit	MITRE
Dr. Pauletta Otis	Colorado State University
ADM Bill Studeman, USN (Ret.)	Northrop Grumman
Dr. Terry Thompson	Private Consultant

Government Advisors

Dr. Alenka Brown-Van Hoozer	Oak Ridge National Laboratory
Dr. Richard Gault	DIA
Ms. Rosanne Hynes	OASD(HD)
Mr. Paul Ryan	DTIC
Ms. Carlynn Thompson	DTIC
Ms. Michelle Van Cleave	OUSD(Policy)

This page intentionally left blank

APPENDIX C: BRIEFINGS TO THE INFORMATION SHARING AND ANALYSIS PANEL

FEBRUARY, 2003

COL Marenic	JREIS
Mr. Winston Wiley	Discussion
Ms. Carlynn Thompson	DTIC
Mr. Scotty Skotzko	DCI Study: Partnership and Sharing Issues between CIA and NSA
Mr. John Osterholz	Review of Data Sharing in Support of Homeland Security
Mr. Fred Turco	Information Operations
Mr. Steve Fee	JIVA Architecture

MARCH 5-6, 2003

Mr. Ben Riley and Mr. Jeff Gerald	Homeland Security C2 ACTD
Mr. Tom Benjamin and Mr. Gilman Louie	In-Q-Tel
Mr. Dave Brant	Discussion
Mr. Rich Colbaugh	Complex Additive Systems Analysis
Mr. John Osterholz and Ms. Marian Cherry	Horizontal Fusion
Mr. Tom Mitchell and Mr. Ed Phillips	CIFA Oil/Gas Pilot Brief on Critical Infrastructure Protection
BrigGen Irv Halter	Discussion
Mr. John Lauder	Overview of NRO support to Homeland Security
Mr. Brian Hack and Mr. Alan Eland	NRO Comms - NRO backbone facilitating sharing of data across the community
Mr. Bob Silsby	ICMAP: building the future framework of IC data sharing
LtCol Kelly Gaffney	QRC - CONOPS and technologies revolutionizing overhead support
LCDR Mike Larios	CMMA/BVI - Providing the current toolbox for IC/customer information

	sharing for ISR management
Maj Jonathan Mundt	NRO Support for Analytical Tools
Mr. Jim Gosler	IO Threat Assessment
Mr. Paul Sullivan, Ms. Anjela Messer and Mr. Richard Saunders	National Guard Information Architecture
Mr. Harvey Eisenberg	Maryland Terrorism Task Force
MG Keith Alexander, USA	Discussion

APRIL 23-24, 2003

Mr. Rich Haver	Discussion
Mr. Rob Zitz	NIMA Innovision
Ms. Fran Townsend	USCG Intelligence

MAY 29-30, 2003

Ms. Carol Haave	Discussion
Mr. Alan Wade, Mr. John Brennan, and Mr. Russell Travers	CIO and TTIC
Mr. Steve Dennis	Discussion
NSA	Discussions

JUNE 23-24, 2003

Mr. Paul Redmond	Discussion
Mr. Tom Lockwood and Mr. George Foresman	MD's Homeland Security Advisor
DIA	Discussions

JULY 18, 2003

Mr. Ron Plesser	IT Privacy Issues
-----------------	-------------------

*APPENDIX D: (SUMMARY OF KEY STAKEHOLDER INTERVIEW FINDINGS)
TO HLS INFORMATION SHARING AND ANALYSIS
WORKING WORK, 2003*

Purpose. This annex provides a summary of the key observations and recommendations offered by a variety of internal and external DoD stakeholders. The goal of this effort was to develop a general overview of key internal and external stakeholders' expectations of and needs from the DoD vis-à-vis homeland security related information sharing and analysis.

Background. In support of the working group's overall efforts, over fifty onsite and telephonic interviews with current DoD employees and a representative sample of interested external DoD parties, from both the public and private sector, were conducted during the period March – June 2003 on behalf of the Information Sharing and Analysis Panel. The objective of the interviews, and the subsequent analysis was to : a) identify relevant stakeholders b) map how HLS-related information is flowing, and how it should flow, within the DoD and between the DoD and external organizations; c) provide insights into stakeholders' expectations of key issues, and how they may try to influence DoD's perspectives or thinking towards these issues; d) highlight key issues and obstacles to data sharing, and e) provide possible recommendations for DSB consideration.

Overview. The central recommendation emerging from the interviews is that the Secretary of Defense should charter a study to fundamentally rethink how HLS-related information should be shared within the Department of Defense and with key partners, to identify what information must be shared, and to determine which high impact actions and programs are needed to thoroughly improve information sharing for homeland security, in order to enable the DoD's longstanding mission to protect its own forces and critical infrastructures, as well as to support lead civil agencies implementing the *National Homeland Security Strategy*.

Most interviewees indicated their belief that although the DoD has always had a homeland defense responsibility as part of its mission to protect and defend the United States from enemies both foreign and domestic, the new post 9/11 environment poses new homeland security-related challenges, and hence a need to rethink the information sharing requirements. The new environment in which the DoD must now conduct its traditional homeland defense and civil support missions requires the DoD to fulfill new roles - some not yet defined and others likely to change as the security environment changes. Serious harm to the United States and its people can emerge from new combinations of rogue states, terrorists, narco-traffickers and organized criminals acting inside and outside the United States. These domestic, national, and transnational forces can work together to attack the homeland, making it difficult, and often impossible, to distinguish between foreign and domestic attacks at the time of an event. The magnitude of the threat posed by these forces, however, may require capabilities unique to the military, or manpower most readily organized by the military. Due to the magnitude of these threats to the homeland, the difficulty of assigning attribution to attackers, and the resources necessary to address the challenge, the DoD may be called upon to play a supporting role in homeland security. Within the context of the new environment, neither the DoD nor civilian agencies have fully explored the potential homeland security-related information sharing implications.

The table below (Figure 1) depicts and overview of the key issues and general findings revealed during the interviews:

Key Issues	General Findings
<ul style="list-style-type: none"> ▶ Changing communities of shared mission. New players in homeland security with new missions and existing entities with different priorities leave roles, responsibilities, and interfaces between agencies unresolved and/or immature. ▶ DoD and interagency misunderstanding of roles and supporting mission in homeland security. DoD is generally unclear on information sharing needed internally for its own core missions, and some Defense entities are unaware of DoD-held information needed by other agencies for HLS. DoD and interagency lack of understanding of the potential support DoD may be asked to provide for HLS has created a false perception by some in DoD that they face <u>no</u> major information sharing challenges. ▶ Significant information sharing breakdowns. Anecdotal, yet potentially significant, information sharing breakdowns exist in key HLS fields (e.g., threat reporting, CIP, intelligence sharing, and support to NORTHCOM). ▶ Current sharing methods and processes are not scalable and are inadequate for new security environment. Linear, hierarchical information flows and legacy databases contribute to an increasingly outmoded "push" system of information sharing. Complex networks of relationships encouraging horizontal information flow may be a better model (e.g., current information-centric warfighting operating concepts). 	<ul style="list-style-type: none"> ▶ Significant cultural barriers to sharing, largely the result of a mentality that emphasizes data ownership; "push,"-based information sharing requiring DoD to know the needs of other agencies, a limited view of the "need to know," and institutional disincentives to openness. ▶ Perceived lack of leadership commitment and focus conveys low priority on HLS-related requirements. ▶ Limited interagency interface or understanding as to what information is needed from DoD by other agencies, from other agencies by DoD, and among DoD agencies. ▶ Policy and doctrinal guidance shortfalls inhibit mature information sharing relationships and processes. ▶ Legal misinterpretations of laws regulating information sharing, and often times undue caution result in greater risk-aversion to sharing than is merited by the laws themselves. ▶ Classification procedures encourage over-classification and inhibit efficient, standardized processes such as tear sheets for declassifying and sharing information. ▶ Technology is necessary to enable improved information sharing and analysis—HOWEVER, without leadership, cultural, and organizational change, improved HLS-related DoD info sharing will not occur even if technology exists.

Figure 1: Summary of Key Issues and General Findings

These issues and findings, as well as specific recommendations offered during the interviews are addressed in further detail below.

A significant hurdle to reassessing information sharing within the DoD lies in the differing DoD views on the nature of the problem. Not all of our interviewees agreed on the nature of the information-sharing problem, or even that there is one. Three different views of information sharing emerged during the interviews:

VIEW #1:

Generally, no significant information-sharing problems exist.

This group indicated that current methods of sharing are adequate and frequent enough to share all information necessary. To the extent that there are challenges posed by the new security environment, steps taken already have largely addressed these needs. This group viewed any further information sharing study as unnecessary. Although this group was relatively small in numbers

(consisting of approximately 5% of those interviewed), this view was expressed by certain key leaders. These interviewees generally believe that the status quo is sufficient, and that the security environment within the homeland does not fundamentally affect how the DoD should be exchanging and sharing information. There is no need for the military to take on any *new* missions nor are there fundamentally new information sharing needs. Rather, the extent of current sharing and coordination both within the DoD, and with partners (e.g., Department of Homeland Security) is appropriate.

This group of respondents generally recognize the need for the DoD to continue providing traditional military assistance to civil authorities (MACA) and homeland defense capabilities (citing the establishment of U.S. Northern Command or USNORTHCOM), but emphasize that the mission of *homeland security* is largely a non-DoD mission. They emphasize that USNORTHCOM is largely like any other combatant command, and that its creation does not cause any fundamentally new information sharing needs, at least from a DoD perspective.

To the extent that challenges exist, they see the problem of information sharing to be primarily an intelligence analysis issue, and not an operational problem that impacts traditional DoD missions. Therefore, to the extent that they see anything new as needed for information sharing, many claim that the newly established Terrorist Threat Integration Center (TTIC) will solve the problem. This group tends to overestimate the information they know, may not understand what information they need to know, and tend to believe that HLS issues are largely outside DoD's responsibility.

VIEW #2:

Additional information sharing is needed, but more of the same will suffice

This group, consisting of approximately 25% of those interviewed, generally perceives that the post 9/11 homeland security environment is causing some changes in how the DoD must share information both internally and externally. This group acknowledged that there were new players and partners (e.g., DHS,

USNORTHCOM) that needed new types of information from both internal and external DoD sources, and that the military needed improved information sharing internally in the new threat environment. However, the group generally suggested that the incremental adjustment in what information is shared, and *how* it is shared, since 9/11 is largely sufficient for DoD requirements. Respondents noted that the increase in standard information sharing practices, and the leveraging of additional technology, is sufficient for the scope of the challenges, to the extent that they exist. Some suggested that the increase in daily secure video - teleconferences and liaison officer placements since 9/11 has been adequate to the task, and suggested that only more of the same was needed. Of note, upon further questioning, many of these respondents would acknowledge that little important information was shared through standard, on-going video-teleconferences for fear that it would create additional tasking from outside agencies, and that liaisons were costly and often unreliable sources of information. Moreover, they acknowledged that under current circumstances even "more of the same" was not possible, as the understaffed agencies could not afford more liaison officers and specific DoD directives had forbidden additional outside liaison placement. Lack of policy also instilled a great reluctance to share information horizontally

VIEW #3:

There is a fundamentally new information sharing challenge, and new methods of sharing, along with new forms of relationships, are needed

By far, the most predominant view, consisting of approximately 70% of those interviewed, is a strong perception that there exist homeland security-related information sharing breakdowns and problems with current methods of sharing (both within the DoD and with critical partners) that can be resolved only through fundamental change. The group stressed that to fulfill its homeland defense role and to support homeland security activities predominantly led by civil agencies, DoD needs better information sharing internally and externally. Old and new civilian partners need more information, more immediately, from the DoD. The DoD, particularly USNORTHCOM, also needs new information from civilian agencies.

Respondents cited poor threat information flows and disconnects between threat reporting and action, the inability to adequately declassify information for sharing, a general lack of policy, and an absence of strategic, operational and tactical doctrinal guidance defining DoD roles and responsibilities in homeland defense and civil support activities.

The group believed fundamental change was needed, but emphasized the risk averse culture that is inhibiting new thinking about *what* information needs to be shared, and *how* that information should be shared. They stressed the need to rethink how the military interacted within the interagency environment, called for cultural transformation to move from data ownership to data stewardship, and believed that new processes and policies were needed to encourage and enable sharing.

While these views favoring change were in the overwhelming majority, most respondents indicated that they believed change was unlikely without a clear commitment by DoD leadership. Respondents claimed that risk aversion, the current DoD incentive structure, and the perceived lack of leadership commitment to enhance homeland security-related information sharing inhibited bottom-up efforts from bubbling up through the system and enabling change. They believed that for change to occur, it would need to start at the top. The sections below highlight the major issues, findings, and recommendations offered by holders of this view during the course of the interviews.

Information Sharing Challenge 1:

The Scope of Information

The need to improve intelligence sharing for homeland security has garnered much attention, largely due to the hearings on presumed intelligence “failures” before September 11. While intelligence sharing will be required of military intelligence agencies, as it is required of the rest of the intelligence community, respondents emphasized that information sharing for homeland security has a much broader scope. Civilian agencies need to know information on

a realm of operational and situational awareness issues, such as National Guard capacities and their deployment status. In the event of an emergency, respondents noted that the military will need to have at its fingertips – or have already shared with other response agencies – its capabilities in responding to chemical, biological, radiological, nuclear and explosive (CBRNE) incidents; incidents in different locales; the availability of military doctors with particular specialties; the availability of hospital beds for overflow; and similar information. For example, the public health system, trying to detect early warning signs of biological attacks, may ask military hospitals and pharmacies for constantly updated medical statistics and prescription records as they are starting to tap other public and private health care facilities to enable early warning reporting. Several of the respondents noted that scenarios run over the course of the last two years have detected a host of other DoD-related information sharing needs, many of which have yet to be fully realized.

Some respondents, particularly those with key operational relationships with homeland security-related civil agencies, noted that information sharing is not a one-way street running from the DoD to civilian agencies. The DoD, if it is called on for new homeland security duties or if it is called to respond with logistics and transport equipment following existing Memorandums of Understanding (MoUs) and Memorandums of Agreement (MoAs), is also likely to want information that it does not now possess. “Battlefield” situational awareness of the type required before deploying to a foreign area generally does not exist to the level of maturity for the United States as it does for other combatant commands. The military may desire to know about civilian airport capabilities, traffic patterns on major roadways, and similar information that would be necessary for homeland deployment or evacuation. Not only is such information not generally collected by the military in a systematic way, but also some respondents noted that in some case, no one currently knows whom to contact to begin tracking down such information.

Information Sharing Challenge 2:***New Roles, and New Actors, In Homeland Security***

In considering what information the DoD will need to collect and share within its own walls and with other agencies, respondents noted that the DoD must also share an understanding of its potential mission with other key homeland security response agencies. The broadly held view by almost all respondents, buttressed by recent civil exercises (e.g., Top Officials exercise series) is that the DoD is unlikely to ever be a first responder or even the main responder to attacks against the homeland, unless the attack is directed against a U.S. based military installation. Generally, local first responders and the DHS will direct response efforts, and will be supported by unique DoD capabilities and assets. However, some respondents noted that the military's role in an emergency is likely to be broader than these specialized capabilities. During an event, non-specialized military assets may be called upon, such as overflow hospitals, transport equipment, and trained doctors. The National Guard, under federal or state call-up, is expected by many agencies and politicians to have a significant role in recovery. Such an expectation requires information sharing to ensure that a governor does not have a false sense of security, expecting to be able to use his or her Guard forces while in fact those forces have been deployed to an overseas theater.

Sharing information for its homeland defense and civil support missions requires the DoD to coordinate and actively exchange information across the public-private and civil-military divides. In the past, these conversations were held within standing relationships forged over years of cooperation, and generally solidified with MoUs and MoAs. Interviewees noted that now, new relationships must be forged with new actors, from private owners of critical defense infrastructure, to new agencies such as the DHS. Many of these actors are themselves not yet mature and have not yet determined their roles in homeland security. Moreover, old relationships, such as that between the U.S. Army Corps of Engineers and the Federal Emergency Management Agency, must be reconsidered in light of organizational changes. For example, interviewees were quick to note that the shakeup of agencies to create the DHS,

USNORTHCOM, and TTIC has left many homeland security roles and responsibilities unresolved.

New actors, undefined needs, and the likelihood that needs will alter as the security environment changes over the next few decades, means that a more extensive focus on information sharing for homeland security is necessary. Neither DoD nor civilian agencies have fully explored the potential role DoD may need to fulfill for homeland security. Some interviewees noted, as of early Spring 2003, that although the DoD is currently waiting for the civilian leadership in the DHS to define itself, top DoD leadership has not actively sought their partnership with civil agencies. Leadership desires to retain a limited role in homeland security, largely due to budget implications of assuming new missions. Several interviewees noted that regular sharing of information can be a way to limit the military's potential role; if only the DoD has information, it will be forced to actively engage in analyzing and responding to homeland security situations, while if it shares information, it enables other agencies to respond without being directly engaged itself. Yet even this scenario cannot take place unless the DoD participates in defining its supporting role in homeland security. A major concern expressed by some was that if the DoD does not actively participate in the *national* HLS debate, its role (and hence, information sharing requirements) would be defined for it.

Information Sharing Challenge 3:

Information Sharing Breakdowns in Traditional Roles required for Homeland Defense and Civil Support

Even if the DoD assumes no new roles in homeland security, some respondents emphasized that DoD faces fundamental information sharing challenges that must be overcome to allow for successful deployment abroad in the face of new security challenges at home. Protecting defense critical infrastructure, for example, is a core need for the military. As the DoD has outsourced, infrastructure critical for deployment, C4ISR, and engagement is often owned and/or operated by private companies, who are hesitant to share various important pieces of proprietary information for fear

that it could be used against them by competitors. Even infrastructure wholly owned within the military is subject to information sharing breakdowns. In charting the community of actors that share the mission of classifying and protecting critical infrastructure, the interviews revealed that those groups responsible for classifying critical infrastructure had almost no communication with those groups responsible for identifying vulnerabilities in the infrastructure. The latter, in turn, had no clear channels to communicate with the intelligence community or the community of critical infrastructure owners, the two groups most likely to receive threat information. Only one organization, the Joint Program Office – Special Technical Countermeasures (JPO-STC), crossed these three stovepipes in an informal and spotty manner.

Several respondents also opined that information sharing also breaks down in the critical area of threat reporting, intelligence, and warning. If a threat to a U.S. military base or defense critical infrastructure is uncovered within the defense industrial base, is learned of by the DIA, is reported to one of the FBI's Joint Terrorism Task Forces (JTTFs), or is reported through a particular service, there is no clear path for this information to move through the system to a decision-maker, or for that decision-maker to initiate action to mitigate the threat. Information is reported through personal connections rather than formal channels, and there is a near complete disconnect between threat reporting and action, as well as between decision-making and follow-up.

This type of homeland security-related information sharing breakdown can have real military consequences, particularly when parties do not know what needs to be shared, or how. One example involves a local FBI JTTF learning of a threat to the telephone infrastructure. The JTTF may or may not realize that the local military base depends on the same infrastructure for critical communications devices, and could fail to relay the specific nature of the threat to the base commander. The base, in turn, would not recognize the need to find backup systems. The private owner of the infrastructure, if alerted to the threat, would undertake a private cost-benefit analysis, but could decide that adding a great deal of additional security was not economically efficient. The military base,

had they known of the threat, may have wished to offer their own protection to the assets – a possibility the private owner may not have even considered. The lack of information sharing leaves everyone worse off – and the military far more vulnerable. Although only an example, this type of scenario was cited by several interviewees as representative of cases where DoD entities may not realize what information they need.

Moreover, even if the DoD takes on no new roles, DoD information will be needed by civilian agencies to enable these civilian agencies to do their jobs and plan for emergencies. The DoD has roles in the Federal Emergency Plan and has MoUs and MoAs with many civil agencies that could be activated in case of an emergency. The extent of the DoD's current commitments to civil agencies is reportedly not now known in by any one entity of the DoD. No DoD agency has apparently collected all MoUs and MoAs. USNORTHCOM is just beginning to catalogue these, as they are brought to its attention by various incidents that have occurred since its stand-up. Even now, civil agencies within DHS desire information from the DoD that the DoD is not currently sharing – or even collecting, on medical capabilities, overflow capacity, logistics, and National Guard readiness, among other subjects.

Information sharing is not just an interagency or public-private issue. Within the DoD itself, there are serious needs. In the SORTS system for ascertaining combat readiness, for example, there is no separate rating for homeland security readiness. A unit that may be perfectly equipped for homeland deployment in an emergency may have a low Combat rating, potentially leaving USNORTHCOM with no visibility on their true potential assets. One interviewee recommended that the creation of an "HLS" rating alongside the "C" rating could solve such an information need. SORTS also lacks National Guard data, which cannot now be readily gathered from the various state Guards. Without such data, USNORTHCOM has no picture of its actual homeland readiness posture.

The magnitude and scope of technical information sharing initiatives, both within DoD and externally, and the apparent lack of coordination among these initiatives, highlighted the fact that there is

also little information sharing between the various fixes the DoD is currently implementing to enhance information flow. Multiple technologies to improve information sharing are now being developed in different portions of the military's scientific research arms, all are being created in an expedited fashion, and there appears to be little information sharing among technological development teams. Interviewees noted that the DoD is providing research money to multiple teams without necessarily publicizing their efforts or sharing information across teams, reducing both the speed of technological development and intellectual cross-fertilization.

INFORMATION STYLE WITH THE DoD: THE CURRENT PERCEPTION

Based on the main themes and issues addresses during the interviews, this effort revealed that information sharing within the DoD and between the DoD and other agencies is:

- **Personality based:** In the absence of formal information flows, information is being sent through personal contacts, with no systematic way of ensuring that information gets to the proper place where it can be assessed and acted upon. This is a particular problem with threat reporting.
- **Not open:** Frequent secure video-teleconferences are useful for sharing routine situational awareness, but people are inhibited from sharing information publicly that has not first been vetted through their chains of command, and which might generate questions and additional work from other agencies
- **Personnel intensive:** A significant amount of sharing is done through liaison officers who are often detailed from other duties with no past experience or expertise in HLS related missions areas. Personnel are often accused of "going native" rather than accurately representing DoD positions and needs to outside agencies, and do not always provide the most open

channels of dual communication. As one respondent noted, they are in a situation of “the food is bad, and there’s not enough of it”, in which liaison officers’ effectiveness faces significant constraints.

- **Based on “push” systems:** The DoD is perceived to have an information-ownership culture, which requires information to be specifically requested by both internal and external agencies before it is “pushed” out. This requires other organizations to know what information the DoD has, and requires the DoD to understand the needs of other agencies – knowledge that does not currently exist.
- **Curbed by disincentives to sharing:** Policies such as the *Patriot Act* have reduced legal barriers to sharing on the civil side, yet cultural risk-aversion continues to provide significant disincentives for sharing. While few individuals can be made responsible and attributed for *not sharing effectively*, tracking down the person responsible for sharing the “wrong information” is simple. One respondent opined that true information sharing across DoD will not occur until the consequences from *not sharing* matches the current threat of sharing information in the wrong manner or with the wrong person without the proper authorization.
- **Stovepiped:** Most information databases are built on legacy systems that are not interoperable. Efforts to build new information sharing technologies are increasingly themselves stove-piped, and little knowledge of similar efforts percolates between technical projects. Interviewees knowledgeable about HLS related research & development activities noted that the interface between technology designers and potential users is also limited
- **Seeking technological answers to cultural problems:** Current methods of sharing within the military and between the DoD and other agencies tended to rely on:

secure video teleconferences, liaison officers posted to different agencies, paper and soft-copy reports, telephone calls, and personal contacts. While these methods may suggest that improved computer technology is the answer, most interviews uniformly agreed that *entrenched culture*, rather than technological inability, was the primary source of information sharing challenges. Therefore, understanding the military's views of the issue is crucial to improving the situation.

MAJOR RECOMMENDATIONS OFFERED DURING INTERVIEWS

The following reflect the main recommendations that were either offered explicitly by a specific interviewee, or were derived from the compilation of ideas generated during the course of the multiple interviews. These recommendations reflect the comments of the interviewees, and are not qualified in terms of importance or overall worthiness.

- Clarify DoD's information sharing needs by determining its homeland security roles and missions through interagency dialogue. The Department of Defense will probably never be in the lead, or even the primary responder, for homeland security. It will always participate under the direction of civilian authorities as part of a larger community that *shares the mission* for homeland security. The DoD must define its supporting role, or other members of this community will define its role for it. While determining roles and missions is difficult, particularly when the DHS is still in its organizational phase, this step is crucial to determining what information must be shared between agencies.
- **Determine internal and interagency information sharing needs:** The DoD (probably led by the new Assistant Secretary of Defense for Homeland Defense)

needs to determine *what* information is needed by military agencies from other DoD agencies and from civilian organizations, *who* needs that information, and *how* they should obtain it. The ASD-HLD will also need to gain an understanding of what information is needed from the DoD by civilian organizations to carry out their homeland security missions, who needs it, and whether/how they should obtain this information.

- Speed creation of policy and doctrine on the role of homeland defense and civil support, and how they relate to overall national homeland security. Homeland security policy is needed to clarify what relationships are necessary within the DoD and interagency. Doctrine is essential to operationalize policy and to train the next generation of military officers. Creating policy and doctrine takes time, and progress on other information sharing issues cannot wait until policy and doctrine are fully fleshed out. However, these processes must begin immediately, and should become a major priority.

Many respondents noted, at least as of Spring 2003, a lack of clearly delineated policy and doctrine with respect to role of the DoD in homeland security. Interviewees cited anecdotal evidence of instances where the DoD is experiencing suboptimal performance and conflicts between agencies that understand homeland security policy differently. Currently, various policies and doctrines exist that govern different areas, and many of these homeland security related operations fall under multiple, sometimes conflicting, policies. This overlap and confusion is allowing those who believe they have no new mission to carry on business as usual, fending off intra-DoD and interagency requests for coordination. Meanwhile, others who believe fundamental change is needed are gathering as much information as possible from agencies within and outside the DoD, much of it of possibly marginal value, since their needs are not defined. At the same time, they are often failing to use their established interagency channels to collect information from civil

agencies that are needed internally by the DoD. The lack of coherence in homeland defense policy and doctrine allows different segments within DoD to act as they prefer, creating contradictory responses.

Similarly, some cited the need for a homeland security doctrine, recommending that current efforts within the Joint Staff to develop this doctrine should be fast-tracked immediately. Although normally doctrinal development process can take years to develop, the need for a homeland security doctrine to operationalize policy and begin training the next generation of officers is real and essential.

- **Clarify USNORTHCOM's role and mission:** When USNORTHCOM first stood up, many of its elements attempted to forge interagency relationships, often without clear policy guidance. Some respondents noted that increasingly, as DoD begins to define homeland security related policies in greater detail and take a strong role in centralizing the flow of information and coordination activities, the development of external relationships has slowed. Several respondents noted that USNORTHCOM and DHS should establish a robust relationship at the operational level. Observers note that currently DHS has very little understanding of USNORTHCOM's role, and there is a widespread sense that USNORTHCOM is constrained from interacting directly with DHS. Neither agency has an understanding of what the other knows or needs to know.
- Within DoD, there tends to be an overestimation of the amount of information that USNORTHCOM is receiving, and subsequently an overestimation of its ability to respond. One interviewee noted that USNORTHCOM did not yet have a collection of all standing homeland security-related MoUs and MoAs between the DoD and civilian agencies. Some respondents noted that other DoD agencies on which USNORTHCOM often depends for information,

troops, and assets provided only grudging support to a command they did not fully understand.

- **Enhance a new culture that reinforces information sharing:** Several respondents opined that although in recent years the military has recognized the importance of sharing information on the battlefield to distribute the ability for leaders to make informed decisions, and allow more rapid communication, homeland security information flows remain vertical, and horizontal information flows between military and civilian agencies have been discouraged. The nature of the shared community response likely during an attack on the homeland calls for more comprehensive situational awareness and distributed decision making between DoD and the civil agencies it supports. In a networked world, traditional hub-and-spokes models of information sharing are likely to create bottlenecks of information just when spreading is necessary. To enable the devolution of information sharing, the DoD should address a broad range of possible policies that would seek to create a culture that encourages enhanced cross civil defense sharing. One example of the possible unintended consequences of fully centralized information sharing channels is the confusion that could occur during an event if pre-event relationships and existing agreements are not fully understood at the lowest possible implementation level. While coordinating the DoD response is useful and necessary, limiting long-standing relationships and channels of communication at lower levels in favor of centralized control and information flows could create unnecessary command and control challenges during a crisis. Several respondents indicated that decentralized coordination and information exchange was critical to ensuring that DoD effectively provides the necessary civil support when required.
- **Transform culture of data ownership into culture of data stewardship:** The culture of data ownership is

reflected by two main trends within DoD. On the one hand, as in many other organizations, knowledge equals power. DoD entities fear that sharing information will reduce their importance and may leave them out of the loop of important decisions that will affect them. By holding onto information, they ensure that they will be consulted and integral to any decision-making process. Information sharing also collides with the military's strong sense that secrecy equals security. The sense that sharing information imperils military missions, and even lives, is deep, pervasive, and often true. While the need for better information sharing is generally accepted, it runs into both a deep-seated fear of improperly sharing information, and a fear of loss of power.

- Changing these cultural mindsets is essential to enabling information sharing, but very difficult. Leadership needs to make clear that information is not owned by the military, but is simply stewarded by them for the U.S. government, and that it must now be shared to defend the nation. Agencies should gain prestige not by what they know that others do not, but by how well they share and manage data to accomplish an overall mission. Real changes in performance measurement may be the easiest method for encouraging cultural change. Interviewees who discussed the issue generally believed that it is unlikely that such deep seated aversions will change until the consequences for *not sharing* equal the punishments for *improperly sharing*, and the rewards for *sharing well* equal the power gained by keeping information close hold.

In concert with other stakeholders, DoD should build greater interagency cultural understanding, through more widespread allowance for liaison officers, briefings, greater openness to non-policy peer-to-peer dialogue across agencies, and even a possible interagency career track. Improving interagency relationships is

essential to making data interactive, reducing misunderstandings, and improving information flow. While computers can move data from place to place, only an understanding of different agency needs, and personal relationships, can turn the mounds of passive data sitting unused in a database into active information.

- **Improve understanding of the laws governing information sharing:** The Patriot Act and other recent laws have altered the legal landscape that has governed information sharing within DoD and among intelligence and law enforcement agencies for decades. These new laws are not understood or internalized by those who deal with information that may need to be shared. Some respondents noted that their agencies followed overly cautious, and often wrong, interpretations of laws and regulations. This caution has been augmented by years of allowing naturally risk-averse lawyers to build “moats” around actual laws to avoid breach, creating a mythology of legal restrictions that do not exist. Several knowledgeable interviewees noted that much legitimate, legal information sharing is believed to be illegal by those who deal with the information. This problem is particularly pervasive in intelligence, but it also applies to other issues. For example, *Posse Comitatus* restrictions are frequently incorrectly cited by the military as an obstacle to fully engaging in homeland security. Improving the understanding throughout the military of the actual laws that now govern information sharing, and separating real restrictions from mental blocks, would immediately enable a greater flow of information to be shared.

- **Review and improve classification guidelines:** Threats to the homeland have created a wider community of non-traditional clients for the intelligence community. Private owners of defense critical infrastructure, local politicians, first responders, and others may need

sudden access to threat information. In order to deploy troops, USNORTHCOM may need to share intelligence with other commands that hold its deployable assets. The intelligence community as a whole, including but not limited to the Defense intelligence agencies, must develop new information sharing processes to balance the need for secrecy and security against the need to share information with those who need to know in order to mitigate threats. Efficient standard operating procedures are needed to scrub and rapidly declassify information; tear sheets should be in more prevalent use; and information that does not actually require high levels of classification should not be over-classified initially.

- The DoD should work with the Intelligence Community to improve information sharing. Interagency dialogue could improve issues that are now impeding DoD's performance of its missions. For example, the habitual overuse of the Originator Control (ORCON) and No Foreign Distribution (NOFORN) classifications are perceived by users of information as impediments to the DoD's ability to share information, within military channels, and with other agencies and people on whom it relies. In addition, several respondents expressed frustration with slow and unwieldy clearance procedures. Several noted the need to decrease the time necessary to process clearances, and to facilitate transfers between agencies. The need to develop a standard clearance procedure across the intelligence community was one requirement highlights as a way to address this problem. Security concerns are real, however, and must be balanced with the need to share in a more systematic manner.
- **Improve coordination of technical information sharing research:** While the interviews unanimously concluded that a technical "solution" for information sharing would be useless without improved policy and

doctrine and cultural change, technology will be an element of the information-sharing solution. Secure and inexpensive communication links to allow information to be “pulled” from databases rather than “pushed” out will be needed among the intelligence community and between some civilian and military agencies, such as the National Guard, USNORTHCOM, and the Department of Homeland Security. Standard XML data tagging is needed to allow the mining of stove-piped databases. New technology is needed to help analysts make sense of the glut of new intelligence data they face. Technology can also assist in the standard declassifying of information and the sharing of intelligence along different levels of classification.

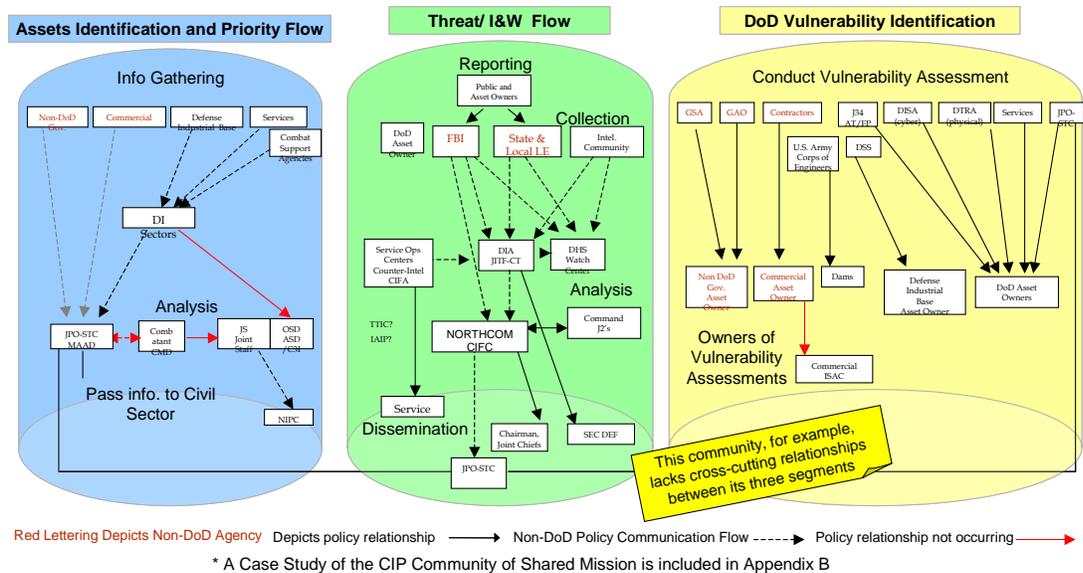
Multiple parallel information sharing technologies are now under fast-track development within the DoD. These projects are not currently linked, and their technologies may not be interoperable. Information fusion technologies are ironically being developed without information sharing between them. The DoD can improve the speed and cross-fertilization of these projects by linking technical development more closely with similar projects and with the users of these technologies.

- **Strengthen relationship between USNORTHCOM and the National Guard:** Several interviewees noted the need for USNORTHCOM to strengthen its relationship with the National Guard Bureau, and with the Guard units of the Separate States. Only by strengthening their working relationship with the State Guard can USNORTHCOM garner the information it needs in a consistent and timely fashion.
- **Conduct a systematic scenario-based interagency study:** The DoD will be a supporter, not a lead agency, in homeland security. An interagency study will place their information sharing needs within the larger realm of the community with which they share a homeland security mission. A study should also illuminate the

information sharing needs within the DoD itself. Such a study could take a dual track approach, with one track working within the DoD, and another operating at an interagency level. This study would systematically address many of the issues illuminated by this stakeholder analysis:

- Within DoD, begin creating policy and doctrine, in conjunction with other stakeholders, which defines realistic roles various DoD entities can be expected to fulfill in homeland security prevention, response, and recovery. Review current MoUs and MoAs to begin this process. Conduct focused wargames and scenario-based interviews to determine the likely scope of DoD's role.
- Map the community of shared mission to uncover information flow gaps and bottlenecks. For example, mapping of CIP community of shared mission uncovered three stovepipes: vulnerability identification, threat & warning, and critical asset identification. Only one agency was found to bridge these stovepipes, and it receives only partial information. Many policy-determined relationships were found to be non-operational, while many robust relationships bypassed policy and needed to be formalized. Sharing between DoD and commercial sectors was nearly non-existent, while new players such as TTIC and DHS IA/IP are not integrated into the CIP structure. No clear information channel exists to alert infrastructure owners or even the operational arm of the military to mitigate these threats.

Figure 2: Defense Critical Infrastructure Protection Community of Shared Mission



Using scenario-based interviews, determine information sharing needs for: situational awareness, prevention/detection, warning/preparation, pre-positioning/response/consequence management. The study should uncover the communities of shared mission who must be able to communicate easily with their counterparts.

Use scenario-based interviews and wargames to determine what information is needed by the DoD from other agencies within the DoD, what information the DoD needs from other agencies outside the DoD, and what information other agencies need from the DoD. Build an information-sharing architecture that maps peer-to-peer connections needed for daily communication.

Clarify laws, policies, and regulations governing information sharing, by creating an Information Transformation Board led by lawyers and non-lawyer practitioners to review, clarify, and publicize

in readable language the laws and policies governing military information sharing. *Posse Comitatus*, EO 12333, and Patriot Act need particular attention. The DIA, for example, already took close look at EO 12333 with team of lawyers and found that the document empowered sharing, not withholding, contrary to popular belief. More needs to be done, and findings need to be clearly articulated and publicized.

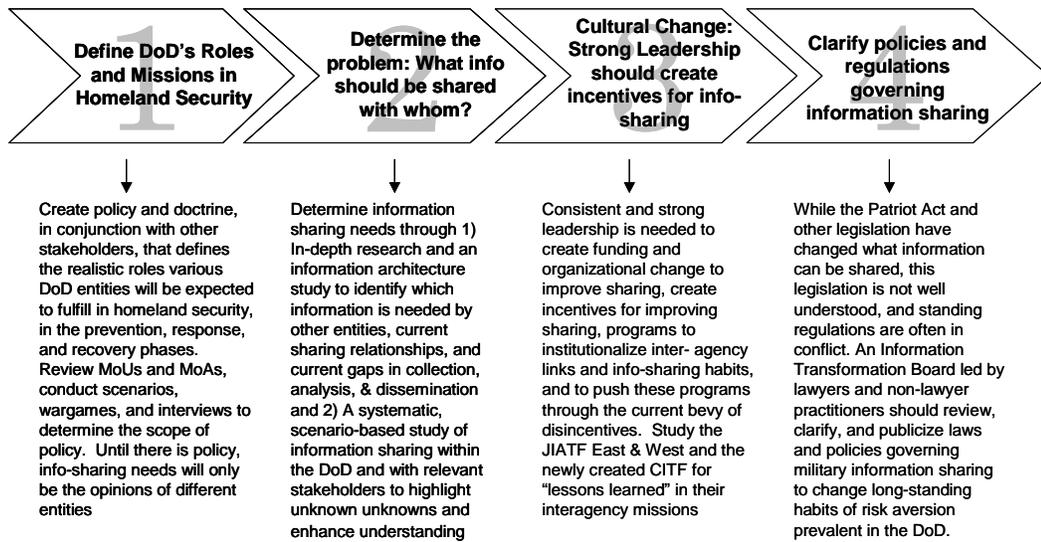


Figure 3. Information Sharing Needs within the DoD

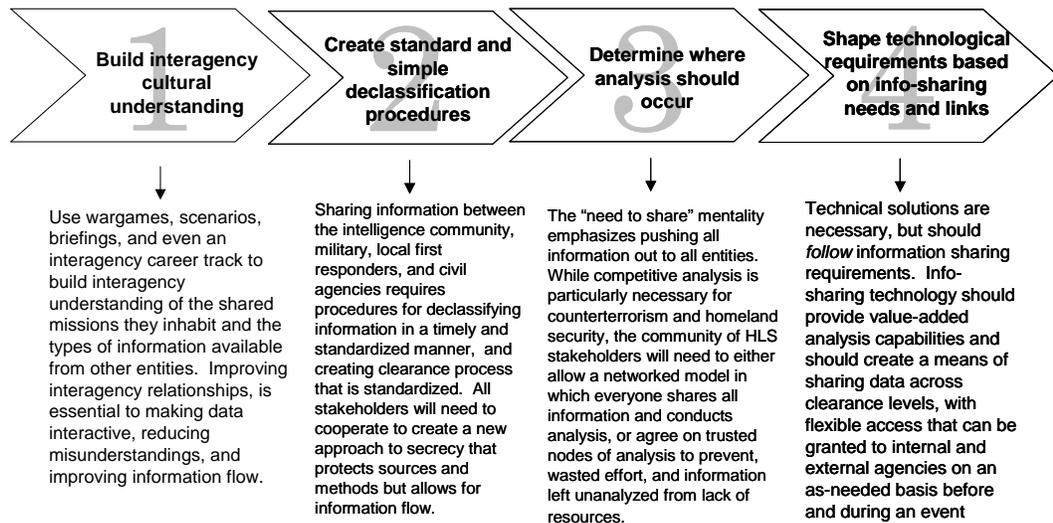


Figure 4: Information Sharing Needs in Concert with External Stakeholders

CONCLUSION

As Vice-President Dick Cheney has said, echoing warnings from top intelligence officials, "the prospects of a future attack against the United States are almost certain...[it is] not a matter of if, but when." Without improved information sharing within the DoD and between the DoD and new civilian agencies such as DHS and TTIC, mitigating another catastrophe will be more difficult and recovery will likely be impeded. Based on the overall findings from these interviews, it appears there exists a lack of DoD commitment and sense of urgency in tackling information-sharing challenges problem.

In part, many respondents believe that DoD is waiting on the civilian leadership to stand-up DHS and provide guidance, arguing that this is an issue of civilian control. While this goal is understandable and praiseworthy, DHS is likely to take some time to fully organize, and as one senior leader directly responsible for a

defense related operational mission noted, "the middle of the next disaster is no time to begin distributing business cards." Nor is it necessarily advisable for the military to wait to allow its role to be defined for it, when it knows best its capabilities. The DoD should begin a high-level review and discussion of information sharing now, to work out roles, standard operating procedures, and sharing processes now, so that all will flow smoothly when they are needed.

The Department of Defense is likely to continue to have a relatively limited role in homeland security. Enhancing its internal information sharing, though, will allow it to better perform the homeland security and homeland defense roles it already has. Paradoxically, only through interagency information sharing will the DoD be able to maintain a limited role within the United States. If information sharing is not improved, the DoD will could find itself having to assume a larger domestic role, because it alone will have pertinent information and the ability to interpret and act on that information. Information sharing in intelligence and operations for homeland security is essential to maintaining the security of our nation, and the proper balance between the civilian and military branches of our government.

APPENDIX E: ACRONYMS AND ABBREVIATIONS

ACTD	Advanced Concept Technology Demonstration
CIAU	Central Intelligence Agency University
CIO	Chief Information Officer
CONUS	Continental United States
COP	Common Operational Picture
COTS	Commercial off the Shelf
CT	Counterterrorism
DARPA	Defense Advanced Research Projects Agency
DCI	Director of Central Intelligence
DHS	Department of Homeland Security
DHS/IAIP	Department of Homeland Security Information Analysis and Infrastructure Protection
DIA	Defense Intelligence Agency
DoD	Department of Defense
DoJ	Department of Justice
DSB	Defense Science Board
DTIC	Defense Technical Information Center
DTS	Defense Transportation System
ELINT	Electronic Intelligence
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FISA	Foreign Intelligence Surveillance Act
GAO	General Accounting Office
GOTS	Government of the Shelf

HLD/HLS	Homeland Defense / Homeland Security
HUMINT	Human Intelligence
IAC	Information Analysis Centers
IAD	Information Assurance Directorate
IAIP	Information Analysis and Infrastructure Protection
IC	Intelligence Community
IMINT	Imagery Intelligence
IO/IW	Information Operations/ Warfare
ISR	Intelligence, Surveillance and Reconnaissance
IT	Information Technology
JFCOM	Joint Forces Command
JITF-CT	Joint Intelligence Task Force for Counterterrorism
JIVA	Joint Intelligence Virtual Architecture
JMIC	Joint Military Intelligence College
JPACE	Joint Aircrew Ensemble
JRIES	Joint Regional
MASINT	Measurements Signatures Intelligence
MOU	Memorandum of Understanding
MSNBC	Microsoft Network Broadcasting
NATO	North Atlantic Treaty Organization
NIMA NGA	National Imagery and Mapping Agency/ National Geospatial Intelligence Agency
NIPRNet	
NORTHCOM	Northern Command
NSA	National Security Agency
OJT	On the Job
OSD	Office of the Secretary of Defense

OSINT	Open Source Intelligence
OSIS	Open Source Information System
OTA	Office of Terrorism Analysis
RISSNet	Regional Information Sharing Support
S&T	Science and Technology
SBU	Sensitive-But-Unclassified
SHSI	Sensitive Homeland Security Information
SIGINT	Signal Intelligence
SOF	Special Operations Forces
SOUTHCOM	Southern Command
STEs	Secure Telephone Instrument
TIA	Total Information Awareness
TPPU	Task, Post, Process, Use
TRANSCOM	Transportation Command
TTIC	Terrorist Threat Integration Center
U.S.	United States
USD(I)	Under Secretary of Defense for Intelligence
WMD	Weapons of Mass Destruction

This page intentionally left blank
