ISB

Intelligence Science Board

Concept Paper

on

Trusted Information Sharing

November, 2004

Executive Summary

The Intelligence Science Board (ISB) has been studying the issues related to securely sharing intelligence information within and across organizations in the National Security community. While countless studies on various dimensions of this problem are currently seeking a solution, it is the ISB's contention that no single solution exists because information sharing is not a single problem. Rather, Trusted Information Sharing (TIS) is a complex collection of technical, cultural, legal, and political issues. By identifying, categorizing, and scoping these issues and their relationships to one another, the ISB intends to define a structured and ongoing method of researching TIS as a complete "field of study." The definition of this field will provide a clear set of goals, an ongoing list of target disciplines, a common vocabulary, and a structured methodology for consistently articulating research in the TIS "context." By promoting the use of this structure throughout the National Security community, the ISB hopes to act as a catalyst for realistic and measurable advances in the field.

To help advacne the TIS field of study, the Intelligence Science Board suggests that the Director of Central Intelligence join with the Secretary of Homeland Security, the Director of the Federal Bureau of Investigation, the Secretary of Defense, and other interested parties to establish an "institute" for the study of trusted information sharing. Such an institute would provide a longer-term exploration of the broad field of Trusted Information Sharing from a variety of interrelated perspectives (technical, social, organizational, political, public and private). This will lead to the definition of fundamental information sharing principles, the establishment of TIS rules and best practices, and the identification of research and experimentation programs focused on ensuring that any and all information that can support our national security mission is readily and securely available to those who need it.

The ISB believes that while some progress can be made through individual initiatives, the broad issues of trusted information sharing cannot be solved piecemeal and in the short run. The ISB encourages the Intelligence Community leadership to recognize the complexity of these issues and establish a long-term and strategic environment for advancements. To achieve this strategic view of the information sharing landscape, the Trusted Information Sharing institute will need to be free from tactical and operational encumbrances. The Intelligence Science Board offers its assistance to the DCI to help the National Security community establish TIS as a field of study by acting as a sounding board for operating principles for the institute, as a reference source for appropriate business models and potential inaugural members, and as an ongoing oversight organization to monitor the relevance of issues addressed by the institute and the viability of solutions that they devise. A possible first step toward these goals may be to leverage the DCI Post-Doctoral program by coordinating several integrated research projects within the field. This would be a concrete and achievable way to establish the "institute."

Background - The Utility of a TIS Framework

Over the past year or so, the Intelligence Science Board (ISB) has been contemplating the topic of trusted information sharing (TIS). Whether viewed as horizontal integration (HI), horizontal fusion, integrated terrorist watch lists, or support for the location of weapons of mass destruction, the topic of information sharing deals with getting the right information to those who need it in a timely, accurate, and usable way. The notion of trusted information sharing reminds us that such information, particularly intelligence information, must be carefully shared in a protected manner that does not do more harm than good.

The ISB began by asking the simple question, how many groups or initiatives were similarly addressing this general topic? We soon concluded that information sharing (by whatever name) is currently a hot topic attracting considerable interest across the Intelligence Community and the government at large. The motivation for this interest includes not only the subjects of current news stories but Congressional inquiries into past performance as well. Indeed, the DCI has declared information sharing a major Community initiative for 2004 and beyond.

We decided that the Intelligence Community did not need yet another advisory board concluding that the Community should "just share more," and so we focused our attention on the value that might be obtained by a rigorous attempt to define or structure the field. In the course of our discussions with government personnel, we encountered a broad spectrum of opinions about who is responsible for information sharing, motivations for sharing more, and technologies that might be helpful.

We hypothesized that the various factors that affect the flow of information might be categorized into a simple framework (*see Figure 1*). This framework attempts to organize the issues that impact the sharing of information in "technical" and "non-technical" bins. Within this, it separates issues that are related to security, information definitions, and sharing. It not only helps us sort out the relevant issues but can also be used to focus related ISB studies and activities around this integrating theme. The warm reception to our initial depiction of this framework led us to conclude that it might be useful to Community leaders as they struggle to understand and relate the complex technical and social dynamics of the "information sharing problem."

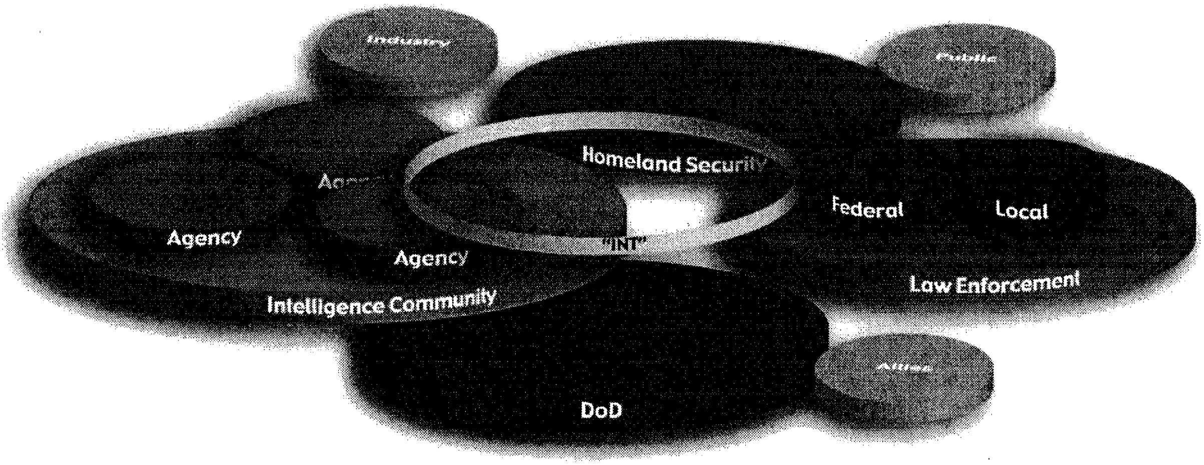
	Trusted	**Information**	**Sharing**
People	*Who is trusted downstream?* *Who is trusted upstream?* *Who has "need to know?"* *Cost/Benefit of trusting (or not)* *US/Foreign/"US Persons"/Industry* *The Clearance Process* *The Classification System*	*What information is important?* *What information is used?* *Privacy* *The feedback process* *Tasking & Requirements* *Fusion* *Managing Consumer Priorities* *Raw Data vs. Analysis Product*	*Motivation* *Mission Priorities* *Metrics* *Ownership vs. Stewardship* *Credit & Incentives* *Collaboration* *Competition* *Adjudicating Conflicts*
Technology	*Identity Management* *Authentication* *Identification* *Access Control* *Multi-Level Security* *Auditing?* *"Tear Lines"*	*Tasking & Collection* *Data Warehousing & Mining* *Data Format and Standards* *Foreign Language Translation* *Reporting Confidence Levels* *Link Analysis*	*Protocols* *Enterprise Architectures* *Push vs. Pull* *Consolidation* *Federation* *Counterintelligence* *Web Services* *Marketplaces*

Figure 1

By categorizing these issues, we came to the realization that the individual issues could not be resolved independently of each other; a prospective solution to one issue must consider its potential impact on several other issues if it is to truly succeed in enabling the sharing of information. Thus, programs that seek to install automated tools or systems to support human-human collaboration, analytic searching and integration across multiple databases, or high-volume document handling will still encounter substantial roadblocks to their successful implementation due to potential conflicts with statutes, policy, business processes, or fundamental human behavior – regardless of the technical merits of the tool or system.

Observations - Sharing Information about Information Sharing

During the course of our study, we have interviewed several senior leaders from the Intelligence Community and its customers. We devoted a recent ISB quarterly meeting to the subject of trusted information sharing. We also attended Community-level symposia focused on information sharing, and reviewed several emerging publications addressing this topic. Several consistent and important themes have emerged from these investigations. First, there are quite a few organizational and mission perspectives on sharing intelligence that each look at things differently (see Figure 2). To make any discussion fruitful, it's critical to first establish common definitions and scope.



Second, we encountered an astonishing number of groups and activities concurrently pursuing the subject of trusted information sharing (each with different perspectives). There appears to be an opportunity to establish some coordination between these efforts. In effect, we aren't even sharing information about information sharing.

Horizontal Integration Senior Steering Group
Information Sharing Working Group
DHS Enterprise Information Architecture
DHS-ITIC Knowledge Discovery and Dissemination Research
Terrorist Threat Integration Center (TTIC)
Defense Science Board Study
Information Sharing Experiments
ICMAP and similar programs

Some of the current information sharing activities

Third, we have come to understand that there are many instances where information is effectively shared every day. Many successful models exist, including the traditional vetted intelligence production stream, various DCI information integration centers, and informal human-human networks. We do not mean to imply that the Community does not share information within itself or with its customers, but that often these sharing activities have been developed ad hoc and without recognition of an explicit set of operating principles for information sharing. As a result, they may not be consistent or complete. We believe that there is value in more formally studying and identifying various information sharing business models, including their individual suitability for specific circumstances and needs.

Several other more specific themes are shown in Figure 3. These represent a summary of the viewpoints that we consistently encountered across the IC and its customers. We believe that many of these can be used to guide further exploration of the field.

Information sharing is a topic of considerable interest within and beyond the IC

- Different people mean vastly different things by the phrase "trusted information sharing"
- A national-level perspective is required
- Leadership is needed to define the TIS principles

Information sharing challenges are not inherent to the IC

- Must shift from "need to know" to "need to share"
- IC needs to share and protect information
- A trust classification scheme is needed
- Risk Management, not Risk Avoidance

Viewing trusted information sharing as an integrated field of study is essential

- There are many complex and inter-related issues that must be addressed concurrently
- A common perception of the field and common vocabulary is essential
- No single all-encompassing solution is possible
- Metrics are needed for measuring progress

The IC may not adequately understand the needs of its customers

- Intelligence is too often treated as an end unto itself rather than support for a mission requirement
- Customers and analysts need smarter push and pull of information
- Customers should not be forced to specify requests in platform-specific terms
- Customers do not adequately understand the capabilities/constraints of the IC

Technology can enable information sharing but it is not enough to ensure success

- Changes in organizational cultures will be required to achieve information sharing
- Changes in culture will require consistent changes in formal reward structures
- There must be mission/business drivers to ensure that information sharing will occur

Extensive information management is essential to effective information sharing

- Information sharing does not mean free and unfettered access to all information holdings
- Technical interoperability and inter-connectivity is only part of the picture
- Information stewardship of Government-owned data is key

The Private Sector is a key component to mission accomplishment.

- Much of the potentially targeted infrastructure is owned and operated by the Private Sector
- First responders can also be sources of information
- The Private Sector needs to see value in sharing information with the Government

New techniques need to be explored

- Separating source and method from information
- Establishing a well-defined, protected, and accessible intelligence sharing space
- Creating a positive reinforcement system for information sharing behavior
- Developing a process for effective metadata marking of intelligence information

Figure 3

Some insights into Information Sharing

Suggestion - Establish a Field of Study for TIS

It has become obvious that trusted information sharing is not just a "problem to be solved" (by some expensive monolithic program or slick collaboration tool); rather, it is a whole field of study comprised of multiple disciplines, perspectives, objectives, and approaches. It's like trying to solve a metropolitan traffic problem with one "silver bullet." In that case, what is really required is many separate but related endeavors addressing mass transit, population housing and employment growth patterns, trends in fuel costs, vehicle pollution concerns, the application of queuing theory to traffic light timing, and a host of others. Implementing a "fix" in one area will not result in solving "the traffic problem" any more than implementing a "fix" in distributed data mining or search engines will solve the overall "trusted information sharing problem." Each step can make a contribution, but we also must consider its potential impact on the other issues. For instance, if someone figures out how to get more cars into the city faster, that's great, but not if makes the air unbreathable.

Treating trusted information sharing as a field of study allows us to establish a dialog among the different perspectives; to share information among these perspectives about challenges, needs, opportunities, and concerns; and to enable synergy in identifying and pursuing a common approach. Agreeing upon some common vocabulary, key definitions of scope, and a unified way to think about the field can be a significant first step in making progress toward a set of common objectives for sharing intelligence information. Appendix I illustrates some of our initial thoughts on this.

In order to facilitate the kinds of multi-disciplinary interaction and coordination necessary to advance the field of trusted information sharing, an environment is necessary where the science of information sharing can be fully explored, unfettered by the organizational and performance pressures associated with producing regular intelligence streams.

To create a center of gravity around which the field can develop, the Intelligence Science Board suggests that the science of information sharing can best be explored in a Trusted Information Sharing Institute devoted to that pursuit. The establishment of and participation in such an institute should be of considerable interest to not only the Intelligence Community, but to the consumers of intelligence and their derivative customers as well. The level of interest in information sharing that we have seen across the IC, the Department of Homeland Security, the Federal Bureau of Investigation, the Department of Defense, and Industry would seem to imply a significant opportunity for jointly creating, tasking, and operating such an institute. It's our feeling that this institute ought to be established within the research community to help avoid the distractions associated with being part of a production organization and to broaden participation to academia and industry. Although it is not the intention of the ISB to dictate how a Trusted Information Sharing Institute might be structured, there are several framing ideas that we thought might be helpful.

Research

The Trusted Information Sharing Institute should reside in a research environment rather than a production one. They should have the freedom to pursue relevant scientific paths without being constrained by short-term operational deliverables. A peliminary step may be to leverage the DCI Post-Doctoral Program by sponsoring several integrated research projects across the field.

Publications

The Trusted Information Sharing Institute should foster advances in research through open communication. Perhaps they will publish a Trusted Information Sharing Journal that showcases promising research. They also may host conferences that bring together players from various disciplines.

Broad Sponsorship
The Intelligence Community is the natural catalyst for the creation of the institute, but sponsorship for it should also come from DHS, DoD, Federal Law Enforcement, and Industry. All of these organizations share a common interest in resolving the challenges of Trusted Information Sharing.

The Intelligence Community is ideally suited to lead the emerging field of Trusted Information Sharing. The ISB believes that creating an environment where advances can be coordinated is an important first step and we are anxious to assist in the design and implementation of such a strategy.

Appendix I
Preliminary Principles of Trusted Intelligence Information Sharing

Intelligence is vital information about those who would do harm to the United States

- It may involve foreign or domestic actors who are sponsored by states, groups, or individuals who seek mass destruction, mass disruption, or mass deception against the US homeland, persons, assets, or allies.
- Intelligence may be obtained from open sources, grey sources, or closed sources.
- Intelligence will provide only part of the information stream needed by decision-makers.

The purpose of intelligence is to support good decision-making

- Intelligence is provided in response to consumers' stated or implied needs.
- Intelligence information is to be stated in terms as specific or as actionable as possible, but it needs to be as clear, timely, accurate, and unbiased as possible.
- Intelligence must be available to all appropriate decision-makers who need it and presented with confidence-levels clearly stated.
- Intelligence should be offered with access to knowledgeable providers for follow-up or clarification.

Intelligence information is the property of the US Government

- It is subject to all applicable US laws, rulings, and regulations and subject to maintenance and protection by multiple stewards.
- It is to be available to all legitimate consumers, but separable by classification, content, and intended use.

We will seamlessly share intelligence information with those who need it

- We will share within the Intelligence Community and with intelligence consumers.
- We will share among individuals and across organizational boundaries.
- We will share at multiple levels of aggregation and within multiples levels of classification.

We must protect our intelligence sources and methods

- We must protect against inadvertent or deliberate leaks or disclosures by any with direct or derivative knowledge of those sources and methods.
- We need to preserve our ability to continue to exploit those sources and methods.
- We need to protect ourselves against subsequent disinformation or deception.

We will incentivize Federated sharing behavior

- We will build information sharing into our business processes and systems.
- We will foster collaborative teamwork where effective, including external expertise.
- We will adopt self-adjusting marketplace principles for information sharing.
- We will organize our planning, programming, and budgeting around national missions.

We must know what we know

- We will align descriptive metadata to facilitate subsequent access.
- We will maintain effective audit trails of data collection, storage, and access.
- We will maintain effective records of what information has been shared and with whom.

We will continuously take advantage of advances in information technology

- We will align our investments in IT and information sharing research and development.
- We will provide a supportive, maintainable, and affordable information infrastructure.
- We will emphasize trusted information sharing across appropriate system boundaries.
- We will design systems and processes with information sharing in mind.
- We will protect the privacy of US persons.
- We will adopt a risk management approach to information operations and the insider threat.
- We will improve our system acquisition process to emphasize mission accomplishment.

We will measure and manage the effectiveness of our intelligence information sharing

- We will simplify customer access to critical intelligence information.
- We will improve intelligence analysis and production.
- We will focus intelligence collection.
- We will balance information sharing and information overload.
- We will monitor "classification creep" or other barriers to information sharing.
- We will log and assess undesirable outcomes (spillage, loss of productivity, etc.).