REGIONAL READINESS FOR INTELLIGENCE INFORMATION SHARING TO SUPPORT HOMELAND SECURITY

by

CHRISTINE GENET KEMP
B.S. University of Rochester, 1984

A thesis submitted in partial fulfillment of the requirements
for the degree of Master of Science
in the Department of Criminal Justice
in the College of Health & Public Affairs
at the University of Central Florida
Orlando, Florida

Summer Term
2005

ABSTRACT

The *Markle Task Force on National Security in the Information Age* was created to produce recommendations on how to best leverage intelligence and information to improve security without compromising existing civil liberties. Their second report proposed that the government set up an information-sharing network using currently available technology to improve our ability to prevent terrorist attacks, while protecting civil liberties. The Markle recommendations have been incorporated into the recent *Intelligence Reform and Terrorism Prevention Act of 2004.* The proposition is that the Markle task force recommendations are sufficient to achieve the required data integration in the United States. To affirm or falsify the proposition, three existing systems will be reviewed: Alabama's Law Enforcement Tactical System Portal (LETS), Florida's Statewide Data Sharing Effort (FINDER), and Orange County, Florida's Integrated Criminal Justice System.

This study found that there is no overall model for national intelligence analysis that incorporates the capabilities that law enforcement has for collection and analysis in with the federal capabilities for collection and analysis. This may ultimately limit the regional systems' success. Recommendations for potential initial models are made. In addition, recommendations for improvement in each regional system are provided. Finally, further research is needed to refine a national intelligence analysis model that can be supported by a distributed information sharing network.

This thesis is dedicated to my former colleague, Anil Bharvaney, who died on September 11, 2001.

ACKNOWLEDGMENTS

Thanks go out to many people who have contributed in many ways to this project. Thanks first to my thesis chair, Dr. Mike Reynolds for guiding this research and for reading and commenting on revisions. Thanks also to Dr. Ronald Eaglin, and Dr. Bob Ford who provided valuable insights. Thanks also to the staff at Orange County, Florida who have allowed me to have the pleasure of working on the Orange County Integrated Criminal Justice System project – a project that provides me with a place to actually implement what I write about here. Finally, I need to thank my friends, family, and coworkers for their words of encouragement and support in completing this project during this time of change in my life.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS/ABBREVIATIONS

ARS	Arrest Reporting System
ASAP	Atypical Signal Analysis and Processing
BI	Business Intelligence – This describes a set of techniques to improve business decision-making by using fact-based data.
BOLO	Be on the Lookout (for a specific person, activity)
CIA	Central Intelligence Agency
CORBA	Common Object Request Broker Architecture
CSCW	Computer-Supported Cooperative Work
CSR	Customer Service Representative
DC #	Department of Corrections Number
DCOM	Distributed Component Object Model. This is an extension of the Component Object Model (COM) that allows COM components to communicate across network boundaries.
DOD	Department of Defense
FBI	Federal Bureau of Intelligence
FDSS	Florida's Data Sharing System
FIC	Field Interrogation Card
FIR	Field Intelligence Report
GJXDM	Global Justice XML Data Model
HUMINT	Includes collection of intelligence collected by human sources
HTTP	HyperText Transport Protocol
IC	Intelligence Community
ICJIS	Integrated Criminal Justice Information System
IJIS	Integrated Justice Information Systems

IMINT	Includes collection of images using devices such as lasers, radar, optics
ISE	Information Sharing Environment
ISWG	Infrastructure and Standards Working Group
IT	Information Technology
JTTF	Joint Terrorism Task Force
KM	Knowledge Management
LETS	Law Enforcement Tactical System
MASINT	Includes scientific and technical intelligence obtained by data collection
MDC	Mobile Data Computer
MDS	Mobile Data System
MSDN	Microsoft Developer Network
NLETS	National Law Enforcement Tactical System
OCSO	Orange County Sheriff's Office
ORG	Object Request Broker
SGML	Standardized General Markup Language
SIGINT	Includes communications, electronics and foreign instrumentation signals intelligence
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
TTIC	Terrorist Threat Information Center
UML	Unified Modeling Language
WSDL	Web Service Definition Language - This is an XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information

XML	Extensible Markup Language - is a subset of SGML. Its enables generic SGML to be served, received, and processed on the Web similarly to HTML

CHAPTER ONE: PURPOSE OF THE STUDY

Introduction

The year is 2001. The Intelligence Community (IC) budget has remained under pressure and manpower cuts have continued, but bureaucratic politics and legislative prerogatives have perpetuated about a dozen national-level agencies and forced a further division of analytic labor. By the turn of the century, analysis had become dangerously fragmented. The Community could still collect "facts," but analysts had long ago been overwhelmed by the volume of available information and were no longer able to distinguish consistently between significant facts and background noise. The quality of analysis had become increasingly suspect. And, as had been true of virtually all previous intelligence failures, collection was not the issue. The data were there, but we had failed to recognize fully their significance and put them in context. At a time when the interrelationship among political, economic, military, social, and cultural factors had become increasingly complex, no agency was postured to conduct truly integrated analysis. From the vantage point of 2001, intelligence failure is inevitable. (Travers (1997, ¶ 1)

Due to the terrorist attacks on September 11, 2001, the prediction became undeniably true, and the clamor for better information sharing between intelligence agencies began. As a result of this, the *Markle Task Force on National Security in the Information Age* (Fleishman) was created. This is a group of leading national security experts from the administrations of Presidents Carter, Reagan, George H.W. Bush, Clinton, and George W. Bush. It was created to produce some answers on how to best leverage intelligence and information to improve security without compromising existing civil liberties.

> The report concluded that by using currently available technology, the government is able to set up a network that substantially improves our ability to prevent terrorist attacks and protect civil liberties… (They) outlined details for the necessary elements of a proposed System-wide Homeland Analysis and Resource Exchange (SHARE) Network that would more

effectively combat terrorism than does our current system, while protecting privacy." (Baird & Barksdale, August 31, 2004).

In this thesis, the Markle Foundation's recommendations in its second report, *Creating a Trusted Information Network for Homeland Security* (Markle, 2003) are reviewed within the context of the overall intelligence agency reform effort set forth in the 9-11 Commission (9-11 Commission, August 21, 2004) Report, and other intelligence community writings.

Statement of Purpose

It is evident that the intelligence community was created in a different era, for a different purpose than is relevant to today's threat situation. Existing legislation intended to address our ability to respond to terrorist threats focuses on organizational structure, not on business processes within the organizations. Similarly, existing recommendations for information sharing focus on preserving the status quo within independent agency systems, while sharing whatever data is there to be shared. Given the substantial change in the frame-of-reference from the old threat environment to the new threat environment, neither the legislation nor the information sharing recommendations is likely to be overly successful in the long run. The FBI's recent $170 million failure in its Virtual Case File System provides evidence of how a frame-of-reference change can contribute to overall software failure. "Initiated in June 2001, the Virtual Case File System suffered from having to adapt to the FBI's dramatic post-9/11 mission change, which called upon the bureau to focus on preventing terrorism as much as fighting more conventional crimes" (Greenemeier, 2005)

At the root of the Markle Foundations recommendations[1] was a desire to come up with a mechanism to integrate local law enforcement intelligence and enforcement activities that are primarily focused toward crime prevention with national intelligence that is more directed towards terrorism. Ultimately, a single national system and process for intelligence information sharing should be the implementation result. The purpose of this study is to evaluate existing regional initiatives within the context of the Markle recommendations, and use that information to identify policy implications and possible insufficiencies in the recommendation. In addition, it will recommend a process and technology-based framework for intelligence information sharing. This framework will be designed to support new intelligence collection and analysis processes from the ground up, without being dependent on large-scale agency reorganization.

Rationale

Historically there has been a clear distinction between the methods and business objectives of local law enforcement intelligence and those of national security intelligence agencies. The missions and customers of the agencies involved in local law enforcement are very different from those of national intelligence organizations. Local law enforcement performs intelligence functions with the ultimate goal of increasing local public safety. National intelligence organizations perform intelligence functions with the goal of detecting and preventing incidents that threaten our country and its inhabitants as a whole. We need to be able

[1] The recommendations included: A directive to the President to create Executive Orders to set up a decentralized information-sharing network, a directive to the President to create an Executive Order to govern the TTIC, a directive to DHS to coordinate efforts with state, local and private sector entities, a directive to the FBI to share information with state and local law enforcement, a directive to all agencies to create ways to produce more useable information while protecting civil liberties, and a directive to Congress to review performance of federal agencies.

to combine and leverage relevant information regarding local events, such as an FSU/UF football game in Gainesville, FL, with national intelligence analysis regarding similar events.

Our challenge is to determine how best to merge the capabilities of each type of organization to create cooperative processes that not only meet the needs of local law enforcement, but those of national intelligence agencies' customer base. This study explores a mechanism to integrate local law enforcement with the national intelligence initiatives. This is broader than simply integrating the intelligence functions because the scope of data gathering needs to be considered with respect to the scope of the analysis.

When dealing with terrorism, data is gathered locally, but needs to be analyzed globally for it to make sense. Local law enforcement processes such as field investigative reporting, or incident reporting, also need to be integrated with the national intelligence initiative. Integrating only the local intelligence functions with the national intelligence functions would perform a disservice to the entire intelligence community.

Justification of Importance of the Study

The research contained in this is significant, because its outcome could help guide specific local implementations of information sharing to support the *Intelligence Reform and Terrorism Prevention Act of 2004*. (U.S. Senate, 2004). It could also guide grant distribution to local law enforcement, as it would provide some guidance to how to distribute grants to local agencies. One of the key points in the bill establishes the National Counterterrorism Center [2]to coordinate

[2] The National Counterterrorism Center is the primary United States organization to analyze and integrate intelligence pertaining to terrorism and counterterrorism, it provides operational planning for counterterrorism activities (diplomatic, financial, military, intelligence, homeland security and law enforcement, ensures that agencies have access to all-source intelligence, and ensures that agencies receive the intelligence needed to accomplish their assigned jobs. It is allowed to disseminate information from any Federal, State, or Local agency, and can allow authorized agencies to query Center data to assist in their assigned responsibilities. (White House, 2004)

terrorism-related intelligence and conduct "strategic operational planning," which will include the mission, objectives, tasks and interagency coordination. This center will require unprecedented national information sharing in order to be effective. (White House, 2004).

Scope of the Study

To affirm, or falsify the propositions, the existing literature was reviewed. In addition, three existing information sharing systems were reviewed: Alabama's Law Enforcement Tactical System Portal (LETS), Florida's Statewide Data Sharing Effort (FINDER), and Orange County, Florida's Integrated Criminal Justice System (ICJIS). These programs served as case studies.

Limitations of the Study

As with any study, weaknesses exist that need to be acknowledged. Some limitations do exist in this study.

- This study is limited by the fact that knowledge about existing intelligence processes was obtained from solely unclassified sources. It is possible that there are additional relevant techniques or technologies in place today that are not considered in the scope of this study because they are classified.
- Minimal design documentation exists for the Alabama Law Enforcement Tactical System Portal (LETS) or for the Florida Statewide Data Sharing Effort (FINDER).
- The actual requirements for national intelligence information sharing are not known. There is no known comprehensive approach to cross-agency intelligence collection and analysis. Each independent agency seems focused on having its own 'fusion' center, each with its own sources of data. Without a comprehensive set of requirements for the 'enterprise' needs for intelligence collection and analysis in

today's environment, and national directives encouraging their implementation, local agencies will most likely continue to invest in systems that meet their local operational and political objectives[3].

Propositions

The key proposition in the study is that the Markle task force recommendations are sufficient to achieve the required data integration in the United States. The Markle recommendations include:

- The President should create Executive Orders to set up a decentralized information-sharing network.
- The President should create a second Executive Order to govern the TTIC and taskings.
- DHS should coordinate efforts with state, local, and private sector entitites.
- The FBI should share information with state and local law enforcement.
- All agencies should create ways to produce more useable information while protecting civil liberties.
- Congress should review performance of federal agencies. (Markle, 2002)

[3] The adoption of the UPC bar code serves as a useful analogy. In 1932, students at Harvard University proposed that customers select catalog merchandise by removing punched cards from a catalog. In 1948, ink patterns were proposed by a graduate student at Drexel University. Bar codes were not commercialized until 1966. There were various locally successful vendor-specific barcodes created by Logicon, and then NCR corporation. Finally, the "event that really got bar coding into industrial applications occurred September 1, 1981 when the United States Department of Defense adopted the use of Code 39 for marking all products sold to the United States military." (Adams, 1995). Similarly, intelligence information sharing will reach its zenith when the national requirements have been well-defined an implemented.

Research Questions

1. Will the Markle recommendations be sufficient to support interconnection of regional and state systems like Alabama LETS, Florida FINDER, and Orange County, Florida.
2. Are there aspects of Alabama LETS, Florida FINDER, and Orange County, Florida that are not sufficient to accomplish the interoperability and therefore need to change?
3. What are possible insufficiencies in the Markle recommendations?
4. Are there any non-technical human barriers to system development and implementation?

Contents

The existing literature was examined the in areas of intelligence analysis, legislation, and information sharing technology. It then describes the study methodology and presents the analysis results of the three existing regional information sharing systems, and finally draws conclusions for how to structure intelligence information sharing in the future.

CHAPTER TWO: LITERATURE REVIEW

This section of the study first describes what is meant by the term intelligence from intelligence analysis, nature of the threat, and organizational change perspectives. It then describes requirements for intelligence information sharing, relevant legislation, technology, technical architecture solutions. Then the research questions are addressed by the literature review.

Process: Intelligence

What does it mean to collect and share intelligence information within the United States? In essence, intelligence involves gathering and analyzing data about who, what, where and when someone is planning an attack of some kind. To do this, we must gather information about people and organizations that have not yet violated the law. Simply gathering the information does not make it intelligence, however, analyzing it does. In international security, there are many different types of intelligence; including Signals Intelligence (SIGINT), Human Intelligence (HUMINT), Communications Intelligence (COMINT), Imagery Intelligence (IMINT), Measurements and Signatures Intelligence (MASINT), and open source information (Clark 2004, p. 64). These are also called stovepipes in Intelligence Community jargon.

- SIGINT – Includes communications, electronics and foreign instrumentation signals intelligence
- IMINT – Includes collection of images using devices such as lasers, radar, optics
- HUMINT – Includes collection of intelligence collected by human sources
- MASINT – Includes scientific and technical intelligence obtained by data collection

- Open Source Intelligence – data available to the public

The type of intelligence most appropriate to be shared between local law enforcement and the international intelligence community is human intelligence (HUMINT). That is what is discussed in this paper. It is also worthwhile to note that there are other local government sources of data that may be valuable to share at a national level; such as parking ticket data collected by parking enforcement bureau's, text data on law enforcement's incident reports. It is also important that we define the routine low-level police records that are most important to feed into the human intelligence process. Some of the requirements:

- Local law enforcement needs to know when a known terrorist is in their vicinity.
- International intelligence needs details of what a known terrorist is doing in a local community and details of specific targets within the United States
- Local resources may need to be tasked to look for anything involving certain targets and weapons such as: explosives, infrastructure, biological materials, known terrorists, suspected terrorists, weapons of mass destruction, or financial transactions

Intelligence information is critical to fighting terrorism, organized crime, and drug trafficking enterprises. Accurate characterization of our terrorist adversary must drive intelligence processes. "To design effective programs, allocate resources, and evaluate results, policymakers need information about existing and impending trends in the illicit narcotics trade." (Kenney, 2003, p. 212) Having an information system, or network that supports the intelligence creation activities is a critical success factor in combating the actions of any cell-based, or distributed organization.

Intelligence Analysis

We are undergoing a major overhaul of the way our intelligence community detects, analyzes, and acts on threats to keep our society safe. Carter (2001, p. 7) describes the need to deal with the problem of catastrophic terrorism. The focus of his article is on the "need to reengineering the architecture of governance, security institutions and their modes of operation – when war-scale damage results from terrorism." Law enforcement, by nature, is programmed to respond to incidents usually precipitated by 911 calls. Carter (2001, p. 8) states "the U.S. law enforcement paradigm is also ill-suited to deal with catastrophic terrorism. This paradigm centers on the post facto attribution of crimes to their perpetrators and to prosecution under the law." Business processes[4] within law enforcement have evolved over the years to support this reactive paradigm. Once entrenched, the business processes become a culture. This culture of reactivity makes it difficult, but not impossible, for uniformed patrol law enforcement to take a more proactive role in intelligence gathering and analysis[5]. In one sense, they must change to be able to work proactively, because we simply do not have enough data collection points to deal with the detection of our highly creative enemy. Depending on the new business processes that

[4] A business process is comprised of steps taken to achieve a business goal. It has inputs, ,methods, and outputs.
[5] A person might ask if it is realistic for a patrol deputy on the street who is focused on a local domestic violence incident to be concerned with gathering information for intelligence. It is important for the data the deputy needs to gather on the street to be defined. For example, if *language spoken*, and *citizenship* are important fields to be captured in an intelligence information sharing database, then the deputies should be required to enter that information into their incident or arrest reporting system. The patrol deputy does not necessarily need to know that that information is useful for terrorism-related intelligence analysis. This is analogous to a sales contact management system. Many salespeople are trained to gather information such as gross sales, number of employees when they make sales calls even though this information is not used by them specifically. Marketing analysts use the information later to proactively plan the salespeople's activities later.

are created while reengineering our homeland security capabilities, a multitude of scenarios can be created that the Markle Foundation proposal does not address[6].

It is intelligence analysis that "organizes and interprets the intelligence (information) in a way that significantly enhances its value and the possibility of its success in combating organized crime. Analysis identifies and predicts trends, patterns or problem areas requiring action." (Carter, 2004, p. 57). For example, supposed that law enforcement patrol officers were trained to report on suspicious persons near bridge structures in their field investigative report narratives. Assume that the field investigative report data would be shared through the distributed information network. Then suppose a tip came in that terrorists were going to target local bridge structures in certain cities. An intelligence analyst could then query the shared information network to see if there was a sudden increase in this number of incidents. The tip is used to begin a deductive process whose result may be an inductive process of looking at related facts to determine if there is a related pattern similar to the tip, or see if the tip is the beginning of real activity.

"The fundamental point to draw from this discussion is that pieces of information gathered through the collection process are not intelligence. Rather, intelligence is the

---

[6] Consider a situation where an officer responds to a domestic violence incident and the suspect blurts out that someone is plotting to blow-up the Daytona International Speedway during the next NASCAR™ race. The officer would make the arrest and check a box on the charging affidavit that a potential terrorist statement was made. The details of the statement could be documented on the charging affidavit and incident report. The affidavit could then be sent electronically to a local "analyst." The officer could also notify his sergeant who then notifies a local "analyst". The analyst would then formulate a hypothesis that there may be terrorists planning activities against NASCAR races. The Local "analyst would search through shared databases to look for other reports of similar activities/reports throughout the country to confirm the hypothesis. This "tasking" could also be sent out to other regional analysts to perform similar analysis. A national intelligence "analyst" could bring together the viewpoints of all of the regional "analysts". If the data supported the hypothesis that there are terrorists planning activities against NASCAR™ races, then national BOLO's could be issued for race stadiums.

knowledge derived from the logical integration and assessment of that information …" (Carter, 2004, p. 63). The entire intelligence cycle is reactive in nature. It is not initiated by observing large collections of facts and observing patterns. Rather, a customer defines a requirement for intelligence and the relevant agencies are subsequently tasked to create analytic products meeting the requirements. If a distributed information network exists, then an intelligence analyst can hypothesize new ways that terrorists might attack us, then query the network to see if any evidence supporting the hypothesized methods exists. For example, they might hypothesize that a terrorist might use a crop duster to spray a chemical over a populated area, and look through the network for incidents involving crop dusting, or airplane training incidents.

Tips may also drive inquiries into the distributed system to start an intelligence analysis process. Suppose that an anonymous call comes into a 9/11 call center stating that Joe Bob is a terrorist living in Orlando, Florida. The 9/11 center documents the anonymous call on an FIR. A checkbox (new) on FIR indicates possible terrorist activity. The operator/detective routes the information to the local "analyst." Information about person, and location, and tactic is documented in a local intelligence database. A local "analyst" determines the validity of the claim and possibly dispatches a detective to investigate. If the information is deemed to be 'qualified', it is 'shared' with national intelligence database from the person, location, and tactic (target-centric) perspectives. A national "analyst" may also be notified for further investigation. The next time someone is looking for information on that person, location, or tactic, (either a national or regional or local analyst), it will be there.

Another interesting point is that the performance of the tasks in the cycle is compartmentalized. Collectors do not analyze. People who write intelligence requirements do

not collect raw data. The cycle is organized along the same management principles as organization of labor in a manufacturing plant for efficiency. (Carter, 2004).

When the FBI is involved, the intelligence cycle changes somewhat because the FBI has the responsibility to integrate local law enforcement and national intelligence. Once the analytic products have been created, they must be disseminated. The FBI disseminates information in three standard products – FBI Intelligence Information Reports, Intelligence Bulletins, and Intelligence Assessments. (Carter, 2004)

Clark (Clark, 2004) describes an intelligence cycle as well. The traditional intelligence cycle includes requirements, planning, collection, processing, analysis, and dissemination. Requirements define the intelligence problem to be solved. Planning determines how the components of the cycle will solve the problem. Collection involves actually gathering the information needed. Processing involves activities such as linguistics, translation, or signal processing. Analysis requires human thought process to synthesize and make sense of the gathered information, and to create an analysis product. Finally, dissemination involves sending data to the original customer. (Clark, 2004 p. 15-16) "All intelligence involves creating a model of the target and extracting knowledge from that model". In a generic, iterative model described by Clark, data is gathered and synthesized to create an initial model called "Model Version 1". Information is then added to this picture, synthesized again, to create another version of the model, "Model Version 2". The information in "Model Version 2" is then analyzed to begin to create knowledge, and yet another version of the model emerges, called "Model Version 3" until the product at the end is actionable intelligence. (Clark, 2004, p. 36).

Grabo's book (Grabo, 2004) provides a detailed description of the specialized tasks involved in the overall intelligence process, and of the difference in strategic and tactical

warning. She does not overtly describe the traditional cycle, but rather, describes the steps within it. Collected data, such as suspicious activity around likely targets documented in field intelligence reports, or by certain individuals, leads to indications (information). Indications lead to warning (analytic products) She describes warning intelligence, which is "to anticipate, insofar as collection and analysis will permit, what potentially hostile entities are likely to do, and particularly whether they are preparing to initiate adverse action". (Grabo, 2004, p.1) One of her key points is on the very human failing of not necessarily 'accept' what should be a logical conclusion.

Different Views on Intelligence Analysis

One key difference between the Grabo (Grabo, 2004) and Clark (Clark, 2004) perspectives is in the level of compartmentalization. In Grabo's model, the task workers function in their specialized area without benefit of an overarching reference model, other than the requirements specified by the customer. In Clark's model, there is an overarching reference model that guides all activities through the cycle. Unsurprisingly, the approach described in Grabo shows a work breakdown created using a manufacturing model of organization of work. Each type of analyst is highly specialized. Indications analysts are different than order-of-battle analysts. Clark on the other hand presents a 'systems-approach' to intelligence analysis. His approach starts with a target goal to create a reference model is created, and information synthesis/analysis are performed to refine the model. The difference between Grabo and Clark can be described as bottom-up vs. top-down. Clark points this out, "An alternative to the traditional cycle is to make all stakeholders (including customers) part of the intelligence process….the cycle must be redefined, not for convenience of implementation in a traditional

organizational hierarchy, but so that it can take full advantage of evolving information technology and handle complex problems" (Clark, 2004, p. 17)

Another key difference is in the scope of the data collection, and of the analysis itself. Local law enforcement intelligence analysis, even when performed as part of a metropolitan or regional task force has access to limited sources of collected data. In many cases, the information available from upstream (national) sources is in the form of analytic products. Local law enforcement intelligence analysis efforts also include community outreach efforts that help educate local communities as to the actions, behaviors and events that constitute 'suspicions' from a terrorism perspective. (Clark, 2004)

Today's Context: The Character of our Adversary

During the Cold War, our adversaries were conventional in nature. Harris (2002, p. 4) describes them as hierarchical, formal, with concentrated leadership, centralized command and control, with formal budgeting processes. Our post Cold-War adversary has an entirely different shape. Threats to national security in early 2001 increasingly dealt with threats such as terrorist organizations, organized criminal networks, or drug trafficking. In early 2001, the Central Intelligence Agency's Directorate of Intelligence conducted a review to determine future needs for intelligence products and create a vision for the optimal structure for the United States Intelligence Community (IC). The IC realized that they needed to redefine the skills and information that intelligence analysts needed to do their jobs. They also realized that they needed to find better ways to synthesize their secret information with more open sources of information to create actionable intelligence. (Lahneman, 2003, p. 573).

The events of September 11, 2001 increased the urgency of these efforts. Harris (2002, p. 1) states "the terrorism we face is decentralized, self-generating and is tied to the existence of failed states and the battle for the soul of Islam."

These events also led to the creation of the *National Commission on Terrorist Attacks Upon the United States*, (9-11 Commission, 2004) which most people know as the *9-11 Commission*. Their web site provides the details of the 9-11 Commission's composition, activities and reports. It describes that this commission was an "an independent, bipartisan commission created by congressional legislation and the signature of President George W. Bush in late 2002". It was "chartered to prepare a full and complete account of the circumstances surrounding the September 11, 2001 terrorist attacks, including preparedness for and the immediate response to the attacks." The Commission is also mandated to provide recommendations designed to guard against future attacks." (9-11 Commission Web Site, 2004)

Organizational Change

There appears to be some lack of clarity at the Federal level as to how to architect the overall intelligence information sharing initiative. The Markle foundation recommended a completely distributed approach to sharing data. The near-term approach, the SHARE network, assumes that the information that is available to be shared is will be useful information needed for information sharing. The Markle recommendations also state that agencies should create ways to produce more useable information while protecting civil liberties (Markle, 2003) It also assumes that the existing processes for intelligence collection and analysis are the right ones, as

the recommendations do not include any consideration for process change. In fact, there has not yet been an analysis performed that leads to this conclusion.

There are significant challenges facing the Department of Homeland Security today. According to the RAND Corporation testimony before the Committee on Homeland Security and Governmental Affairs in the United States Senate, "the first challenge is the lack of robust strategic planning and analysis capability in the Department." (Wermouth, 2005, p. 2) Without a strategic planning capability, it is not likely that an overall strategy for intelligence collection and analysis will be developed.

Deborah G. Barger is a senior intelligence officer who is interested in the topic of change in the U.S. Intelligence Community. More specifically, she believes that what is needed is a Revolution in Intelligence Affairs (RIA). "There is both a need and an opportunity for the Intelligence Community to change in ways that would change its form and function well beyond what is currently contemplated, let alone imagined, by the various proponents of reform." (Barger, 2005, p. 2). An RIA does not focus on organizational structure; rather, it establishes a process for continual reinvention. Ms. Barger states, "so much has changed in the geopolitical, social, and technological backdrop for the intelligence mission that few of the old assumptions – about why we have an intelligence apparatus, what its missions are, and what capabilities give U.S. intelligence a dominant advantage over its adversaries – apply." (Barger, 2005, p.8)

Barger points out that a fundamental shift has occurred. Nation-states are no longer our primary concern. Instead, we now have a large potential for weapons of mass destruction to be in the hands of small disaffected groups such as criminal enterprises, domestic terrorists, foreign terrorists). Another concern she raises is that the Intelligence Community "may be locked into outmoded technologies, collection operations, and analytical methodologies when new and

possibly better ways of developing knowledge are available." (Barger, 2005, p. 19) Most importantly, she talks about the fact that the distinction between collection and analysis has been called into question by the distinction between information and intelligence created by the information age. Based on this line of thinking, it may be possible to create an environment that transcends the rigid organizational structures and processes of the intelligence community through effective creation of intelligence information sharing systems.

Structure: Intelligence and Law Enforcement Organizational Structures

Our intelligence structures and processes are one step behind our adversary. Harris (2002, p. 5) states, "The United States is comfortable fighting adversaries that are similar to itself and is equally comfortable collecting intelligence against such adversaries." The following highly simplified diagram illustrates the disparities in the organizational structures of the adversaries. Note that while the CIA and Defense Intelligence groups are omitted from the diagram, they are still considered part of the overall intelligence community being discussed.

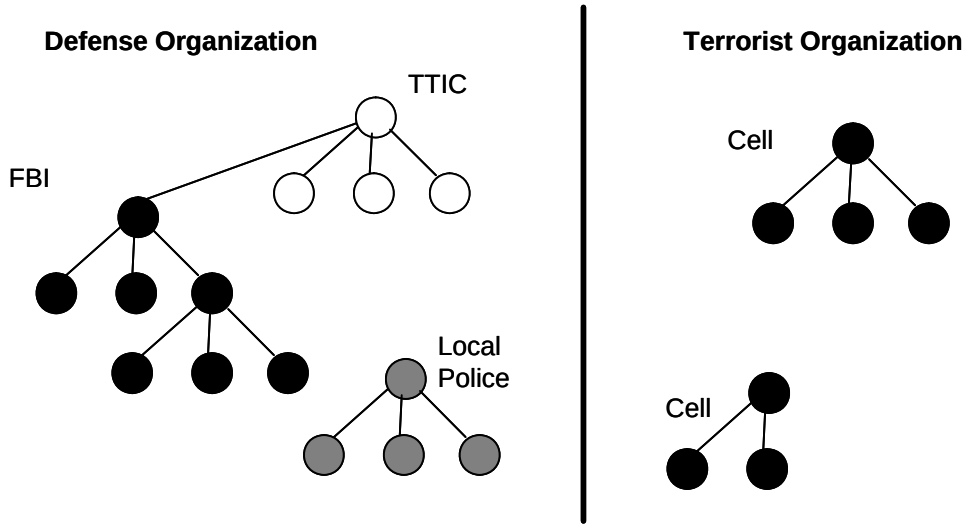


Figure 1 – United States Intelligence Hierarchy vs. Cell-based Terrorist organization

In figure 1, the FBI is shown as a hierarchical organization using solid black circles on the diagram. The FBI is currently reorganizing so that transmission of intelligence information up the chain of command to the central organization consolidates counterterrorism information to the Terrorist Threat Information Center (TTIC). If the FBI deems information relevant it is then disseminated from there to other organizations performing intelligence analysis such as the Terrorist Threat Integration Center. The TTIC, in turn, receives intelligence information from many other organizations.

The FBI's key mechanism for sharing information with local law enforcement is the Joint Terrorism Task Forces (JTTF), which is comprised of FBI, local agencies, and other federal agencies. The purpose of a JTTF is to share information regarding terrorist activities. Sometimes the JTTF members frequently are not allowed to share information back to their originating agency without permission of their JTTF leader. This in some ways defeats the information sharing purpose of the JTTF. (DeRosa & Lewis, 2004, p. 2).

Compare that to the activities of the terrorist cells shown as solid black circles on the right-hand side of the diagram. More flexibly run, the cells can be combined to participate in terrorist acts anywhere. They have no such restrictions on who they can work with, and are brought together, or come together in combinations to achieve their goals. "With grassroots origins, the adversary will morph and adapt, regroup, generate new leadership, shift geographic locus, adjust tactics, and evolve into a collection of cells and networks different from the ones we have engaged fairly successfully since September 11. " (Harris, 2002, p. 1)

The question we need to answer is how we make information available to people investigating terrorist activity regardless of which agency they work for. Also, how do we make the information available in a timely manner to actually proactively detect and prevent an event?

It is easy to blame terrorist successes on lack of information sharing between intelligence and defense agencies, but the overall problem is also a structural and process problem. The intelligence community has not yet adapted to the new shape of the adversary. In addition, oversimplified approaches to information sharing and enterprise architecture rarely yield the desired results of improved operational performance.

This section describes the errors with applying the Markle Foundations' proposal to all types of problems. Baird and Barksdale (2004, ¶ 1) specifically state that "While the discussion over how to implement the 9/11Commission's recommendations to restructure the intelligence community is important, another key commission recommendation, creating a "trusted information network" to facilitate better information sharing among our intelligence agencies, needs immediate attention. Implementing such a network would make America safer today." The information-sharing network is a necessary, but not sufficient solution to the overall goal of increased public safety through better intelligence about terrorist networks. Within this context, implementation of sharing limited data sets using their proposal (e.g. watch lists) could not harm anything, and would prove beneficial.

Requirements

In developing the requirements for a national law enforcement data sharing initiative, viewpoints from three intelligence authors were used to provide a framework to combine local intelligence initiatives with national intelligence initiatives.

Law Enforcement Intelligence (Carter)

Law enforcement intelligence is primarily focused on multi-jurisdictional illegal activities such as "Commodity flow, trafficking, and transiting logistics". Law enforcement intelligence focuses on "Who poses threats", "who is doing what with whom?", "What is the modus operandi of the threat?", "What is needed to catch offenders and prevent crime incidents or trends?" (Carter, 2004, p. 43)

In some law enforcement agencies, field interview reports are managed by an intelligence unit, while in others, they are simply entered into databases, or onto paper forms by uniformed patrol officers. If you look at a traditional law enforcement intelligence operation that is focused on local or regional crime control, it is sufficient for a law enforcement intelligence analyst to be narrowly focused on the law enforcement reports in the context of the related activities in the geographic region. However, in a terrorist-related situation, the actors may be widely dispersed by time, location, or activity, so the scope of the data being analyzed needs to be far different than that produced by the law enforcement agency alone. It is necessary, but not sufficient for a law enforcement analyst to be able to review analytic products created by other law enforcement analysts and federal intelligence analysts. In order for the analyst to draw the right conclusions and 'connect the dots', he needs to have access to similar information in other jurisdictions without it being subjected to pre filtering or analysis[7]. This data, such as the narrative information on FIR cards, or other data such as incident reports at particular target

[7] It is also worth noting that the process of "connecting the dots" is most effective when it starts with a trigger, or tip about a specific target (person, place, tactic). Starting with the trigger, data in a shared information system can then be queried by deduction, with query results either proving or disproving an analytical hypothesis. The sparse nature of raw data in the case of terrorism limits the appropriateness of an inductive approach where tools evaluate the data and predictions are output.

locations, would need to be made available in an unclassified form that does not reveal sources or methods.

Analysis for Strategic Warning (Grabo)

Grabo's (Grabo, 2004) describes the overall intelligence process, and it also points out some very human problems associated with intelligence analysis such as our inability to see threats with low probability but potential great danger, inadequate collection against this category of threats, communication breakdown between collectors, analysts and agencies, not listening to the minority opinion, and the processes overall susceptibility to deception. (Grabo, 2004, p. ix)

Intelligence Analysis: A target-centric approach (Clark)

The first step in any analysis is determining the target or objective of the analysis. Clark discusses the use of models, or "a replica, or representation, of an idea, an object, or an actual system. The model forms the end-goal for the intelligence analysis. This goal provides the requirements within which to structure the overall combined intelligence sharing initiative. (Clark, 2004)

Integration of Local Law Enforcement Intelligence with National Intelligence

In integrating local law enforcement intelligence and activities with national intelligence directed towards terrorism, an overall model, as Clark (Clark, 2004) suggests, needs to be built.

This monitor would be built using both person information, and field investigative report information. It could also include analytical end-products. The data facts, combined with the history of queries by investigators and analysts would be used to build a big-picture for decision makers. Rather than having intelligence analysts create individual analytical products that are subsequently shared with other agencies up the chain of command or laterally, the entire raw data database would be made available to the intelligence analysts throughout the analytical network, with protections on individual sources and methods built into the database. This database would include not only information about persons and activities, but also information about vehicles, and property information.[8] The processes that connect local law enforcement to national intelligence agencies are also important.

Consider this example; a person is stopped by a law enforcement officer for speeding. The officer observes bomb-making materials in the car. The officer writes a traffic ticket, and also a charging affidavit that documents the presence of bomb-making materials. He arrests the person. On the charging affidavit, the officer checks the "terrorist" checkbox and notifies his Sergeant. The Sergeant notifies a local "analyst". The Information about person, and location, and tactic is documented in a local intelligence database. The local "analyst" determines validity of claim and possibly dispatches a detective to investigate and qualify the data. If the information is deemed to be 'qualified', it is 'shared' with national intelligence database from the person, location, and tactic (target-centric) perspectives. There may also be other task forces that deal with domestic terrorists that need to be notified. The next time someone is looking for

[8] This is likely to be a significant quantity of data. For example, the FINDER system has 300,000 queries from January – June of 2005. FINDER currently includes participation from 90 agencies. Performance analysis of this quantity of data in a distributed system is not within the scope of this thesis.

information on that person, location, or tactic, (either a national or regional or local analyst), it will be there.

Legislation

This section focuses on legislation that impacts intelligence information sharing initiatives. It describes aspects of the final report of the National Commission on Terrorist Attacks Upon the United States, the Intelligence Reform and Terrorism Prevention Act of 2004, and the REAL ID Act. (*Real ID Act*, U.S. House. 2005. H.R. 418)

Final report of the National Commission on Terrorist Attacks Upon the United States

The 9-11 Commission produced a widely distributed final report, entitled *Final Report of the National Commission on Terrorist Attacks Upon the United States* (9-11 Commission, 2004*)*. Contained within this is an endorsement of a proposal by the Markle Foundation for the creation of the *Trusted Information Network for Homeland Security*. The Commission recommendations include "unifying the many participants in the counterterrorism effort and their knowledge in a network-based information sharing system that transcends traditional government boundaries." (9-11 Commission , 2004, p. 400). Title II of the 9-11 Implementation Act (*Intelligence Reform and Terrorism Prevention Act of 2004*, U.S. Senate. 2004. s.1016) authorizes creation of the trusted information network, and creation of incentives for inter-agency information sharing. (U.S. Senate, 2004, p. 5) Since the act was just implemented, its direct implications have yet to be realized. Fortunately, Florida's Data Sharing (FDSS) model, a working example of the Markle Foundations' network architecture provides us with a possible outcome of the

capabilities of the proposal. "In the past, police investigating burglaries spent countless hours calling around to find out if stolen property had been pawned. Now they just enter a description of either the property or the suspect's name in the FDSS and see if there's a match." (Solomon, 2004, p. 23)

Intelligence Reform and Terrorism Prevention Act of 2004

Section 1016 of the *Intelligence Reform and Terrorism Prevention Act of 2004* (*Intelligence Reform and Terrorism Prevention Act of 2004*, U.S. Senate. 2004. s.1016) provides for the President to create an "information sharing environment" (ISE) to facilitate the sharing of terrorism information. This approach may include any methods determined necessary and appropriate for carrying out this section. This section also provides for staged development and reporting. "The President shall, to the greatest extent practicable, ensure that the ISE provides the functional equivalent of, or otherwise supports, a decentralized, distributed, and coordinated environment that (A) connects existing systems, where appropriate, provides no single points of failure, and allows users to share information among agencies, between levels of government, and as appropriate, with the private sector" (*Intelligence Reform and Terrorism Prevention Act of 2004*, U.S. Senate. 2004. s.1016) Other key concepts include "establishing an initial capability to provide electronic directory services, or the functional equivalent, to assist in locating in the Federal Government intelligence and terrorism information and people with relevant knowledge about intelligence and terrorism information" (*Intelligence Reform and Terrorism Prevention Act of 2004*, U.S. Senate. 2004. s.1016)

The Act should facilitate at least initial efforts towards a nationally integrated intelligence system that serves local, state, and federal law enforcement and intelligence. A method that eases agencies into the concept of information sharing, by promising to allow them to 'keep their existing systems' has the advantage of lowering each agencies' resistance to change[9]. This is most effective for sharing automated information with 'like' data elements such as the terrorism watch lists, or perhaps some of the 'indicators' per Grabo's (Grabo, 2004) Carter's (Carter, 2004) guide is focused on law-enforcement, so it's likely that the bill will facilitate this type of information sharing (horizontal: connection between similar agencies).

The bigger barrier to information sharing remains the cultural problems with the concept of information sharing in general and agencies' reluctance to change. Law enforcement agencies main focus for technology is to automate their paper records. "A significant number of local law enforcement agencies still submit and maintain records on paper, rather than using an electronic format" (Vest, 2005). The bill in effect reinforces this reluctance to share, by 'integrating existing systems'. While this is a necessary starting point, and in fact, putting broader language in the legislation would probably stop integration efforts completely, the cultural issue does still need to be addressed at some point for maximum information sharing benefit that supports a target-centric approach. As we move towards a target centric intelligence model as described by Clark (Clark, 2004) the requirements for intelligence information sharing become more process-oriented. As the process integration becomes more important than raw data sharing, the importance of evaluating individual agency business processes in addition to

[9] It is reasonable for agencies to keep their own systems to meet their individual operational objectives, while modifying those systems to promote information sharing. "Your organization's decision-making capabilities will be turbo-charged with consistent data, rather than diverting inordinate attention to data inconsistencies and reconciliations" (Ross, 2002, p. 2)

arms-length XML-style data sharing becomes more important. The bill does contain language to keep tighter business process and systems integration options open, "connects existing systems, where appropriate" (*Intelligence Reform and Terrorism Prevention Act of 2004*, U.S. Senate. 2004. s.1016) so this again facilitates information sharing.

H.R. 418 (Introduced 1/26/2005) Real ID Act of 2005

The problem of person identification is quite significant in the context of integrated intelligence information sharing, as it is in general justice system information sharing initiative. Without a way to uniquely identify a person in each system that is standard across systems, multiple fields, such as name, race, and date of birth will need to be used to connect the data in the disparate databases. In most contemporary databases, this type of data can be unreliable because of data entry errors, or simply because it is not known. Common problems related to person data include; names being recorded in different forms such as with middle initial, or no middle initial, a person may legitimately be known by multiple names, and the scope for error in data entry when personal information is first recorded. (PIU, 2002,71)

On January 26, 2005, House Judiciary Committee Chairman Jim Sensenbrenner (R-WI) and 115 cosponsors introduced the REAL ID Act (*Real ID Act, 2005*) . "In December, House Judiciary Committee Chairman James Sensenbrenner (R-WI) reluctantly agreed to shelve important immigration reform provisions of last year's homeland security legislation so that vital intelligence reforms could be enacted as quickly as possible." (Federation, 2005, ¶1) This act strengthens some of the provisions related to driver's license loopholes in the states, without taking the person identification as far as a national identification card. Current efforts to

implement a national identification card are being blocked by special interest groups such as the ACLU. "For this reason, we would urge, in the strongest terms, that you jettison the controversial national ID card provisions in H.R. 10 (embodied in sections 3052 and 3053 of the House bill), and Subtitle B of S. 2845. …These sections would give federal bureaucrats the regulatory authority to determine who can and cannot get a driver's license or state-issued photo ID" (ACLU,2004, ¶3-4)

The next section of this document describes some of the technology-related background for this thesis.

Technology

Technologies are needed to support process automation, however, they need to be implemented in such a way that they support overall enterprise goals. This section describes some of the recent issues that have plagued federal information system development, possible blueprints for information sharing, and technical architecture[10] solutions.

Federal Information Systems

Enterprise information architecture is a nontrivial problem. Congressional auditors recently told the Department of Defense that it "isn't doing enough to implement its information architecture." (Chabrow, 2004, ¶ 1) The Department of Homeland Security (DHS) is in the midst of creating overall consolidated information architecture. "DHS still is struggling to merge terrorist watch lists" (Miller, 2004, p. 44) The FBI has also been criticized for its inability to use

[10] Here, technical architecture is used to refer to various ways that information technology professionals might create a solution to implement an information sharing initiative using various low-level techniques.

technology. “A December report by Justice Department Inspector General Glenn Fine particularly criticized the bureau’s inability to utilize technology to combat terrorism.” (as cited in Clark, 2003, ¶ 4)

The IC comprised of the CIA and Defense Department knew it had issues with translating facts into analysis. Travers (1997, ¶ 1) wrote a haunting prediction:

The year is 2001. The Intelligence Community (IC) budget has remained under pressure and manpower cuts have continued, but bureaucratic politics and legislative prerogatives have perpetuated about a dozen national-level agencies and forced a further division of analytic labor. By the turn of the century, analysis had become dangerously fragmented. The Community could still collect "facts," but analysts had long ago been overwhelmed by the volume of available information and were no longer able to distinguish consistently between significant facts and background noise. The quality of analysis had become increasingly suspect. And, as had been true of virtually all previous intelligence failures, collection was not the issue. The data were there, but we had failed to recognize fully their significance and put them in context. At a time when the interrelationship among political, economic, military, social, and cultural factors had become increasingly complex, no agency was postured to conduct truly integrated analysis. From the vantage point of 2001, intelligence failure is inevitable.

On September 11, 2001, the prediction became undeniably true, and the clamor for better information sharing between intelligence agencies began.

Blueprints for Information Sharing

All computer-based information sharing systems follow an overall pattern, or blueprint either by design or by accident. These blueprints are frequently called “application architecture” in the Information Technology (IT) industry. Application architecture is analogous to mass transportation design. A subway that requires that all riders travel to a central hub to change

trains to go to another line is a centralized transportation system. A subway that provides a circular route around a city that intersects the spokes of the system that go downtown may be considered more flexible from a rider's perspective. The design of information sharing systems follows similar patterns, even though all but the most technical observers don't know the patterns are there. Since these patterns form the building blocks for the design of overall intelligence information sharing systems, this section describes the various blueprints, or "application architectures" that may be used to construct an overall system.

Most articles about information sharing in the criminal justice area focus on two basic conceptual application architecture models for information sharing; vertical and horizontal. "The exchange of information between two or more agencies is known as inter-agency or business-to-business integration. There are generally two types of integration, vertical and horizontal." (IJIS Institute, 2004, p. 1) In reality, there are more types of conceptual information sharing models that are relevant to intelligence and criminal justice information sharing. Each conceptual model can, in turn, be implemented using a variety of technology architectures. This section describes each conceptual model in turn, then puts the Markle recommendation into this context.

Vertical Integration

Vertical integration, as used in this document, refers to the sharing of data and information between dissimilar agencies, such as a Sheriff's office and a State Attorney's office within a single geographic jurisdiction. The term 'upward' is used to describe it as information is shared from the bottom of the triangle below to the top. What ties vertical integration together is business process flow both up and down the model as shown in Figure 2 below. In

the Orange County, Florida integrated criminal justice system project, arrest data is captured wirelessly in law enforcement's mobile data computers. The arrest data is then shared up the model to the Clerk of Court, who assigns and shares a court case number for that arrest. The aggregate data is then shared with the prosecutor, corrections, and other justice agencies. So, the actual pattern of information sharing is not strictly vertical in one direction, but rather, flows both up and down the model vertically.

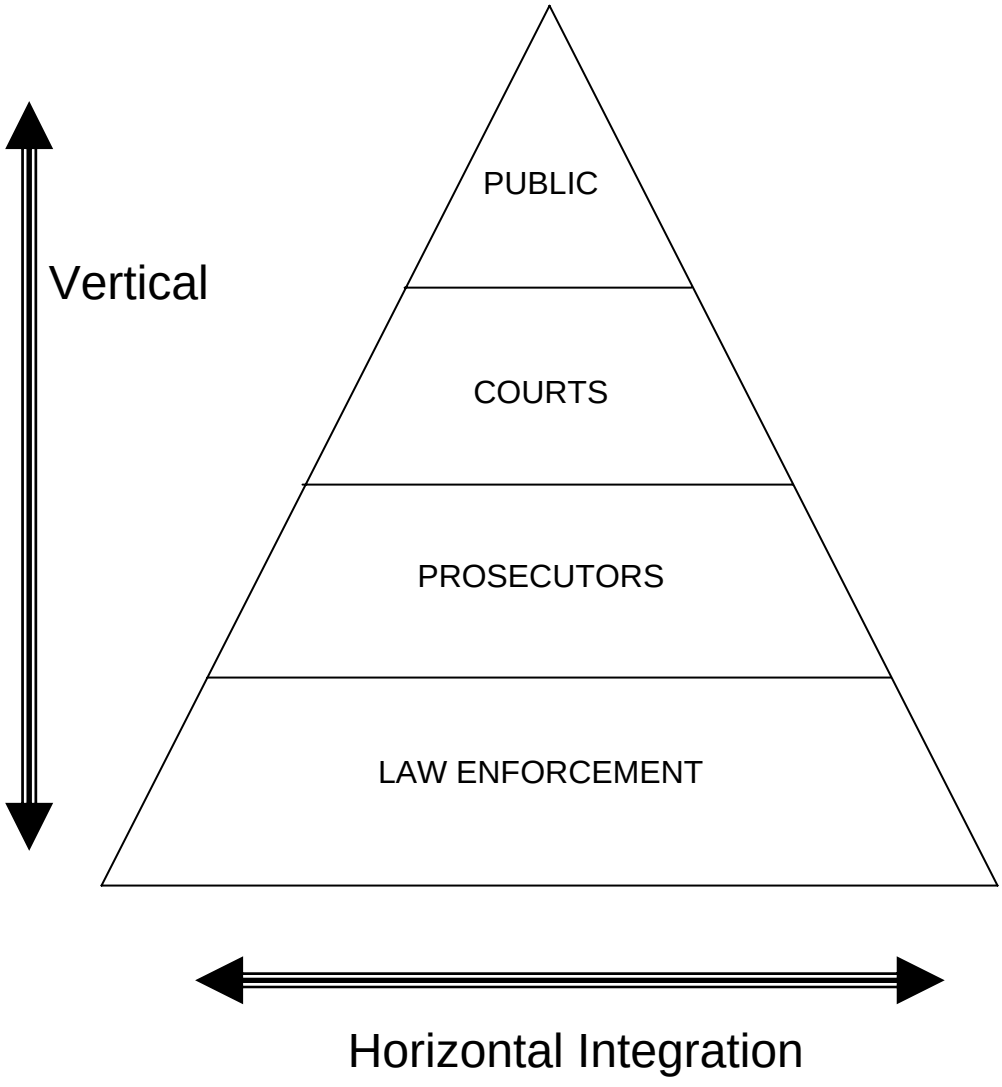


Figure 2 – Traditional Horizontal vs. Vertical Model

Advantages

This model for information sharing can cause the agencies participating in the information sharing initiative to examine their business processes to make sure they make sense in the context of other agencies processes. For example, in Orange County, criminal traffic charges and felony/misdemeanor charges were typically documented on two separate charging affidavits. The ICJIS steering committee realized that with the data flow in ICJIS, this was causing extra court cases to be created. The Sheriff's office proposed that criminal traffic charges be combined with the felony/misdemeanor charges on a single charging affidavit and the ICJIS Business Committee brought the proposal forward to the various agencies. Although this caused manual process changes in the Clerk of Courts, and it caused felony/misdemeanor judges to agree to hear criminal traffic charges, the group of agencies realized that the savings of several thousand court cases per year was worth the process change effort. Similarly, when the group realized that making citizenship a field on a charging affidavit would enable more efficient consulate notification when a foreign national was arrested, they changed the charging affidavit to include the field. Consulate notification can now be triggered automatically, instead of through having Corrections personnel manually inspect each charging affidavit that comes into the jail. Kemp (personal communication, June 25, 2005)

The benefit of business process examination is that it can eliminate processes that are being done, "because we always did it that way," thus streamlining the performance of the overall organization. It also enables cross-agency process automation and the creation of an overall enterprise process for whatever the information sharing objective is. Finally, it exposes deficiencies in information systems that need to be improved in order for individual agency objectives to be met. When a system comprised of processes and technology has been in place

for a long time, the people in the system typically compensate for the deficiencies in the technology. The Orange County ICJIS project has identified many instances of this occurring, and is in the process of improving the system integrations to eliminate the need for compensation. For example, in the late 1990's in Orange County, electronic automated fingerprint identification replaced inking and manual classification of fingerprints. This had the unintended side-effect of causing the Offender-Based Transaction Number (OBTS), which had been provided as a sequential sticker by the Florida Department of Law Enforcement, to be generated by the AFIS machine. After automation, there was no way for the OBTS number to be affixed to the paper copy of the charging affidavit that flowed through the system. This meant that the agencies that had formerly relied on this number no longer had access to it. The Corrections department had a requirement to use the OBTS number when they transferred an inmate from their jail to another County. The other County requires the OBTS number in order that the reporting to FDLE is done correctly. The Corrections department invented a manual process of calling the Sheriff's Record's Identification Section on the telephone and having them look up the booking in a system called the NIST archive that stores index data to the fingerprints for prior arrests. These are examples of longstanding deficiencies that need to be fixed in order to automate cross-agency processes. Kemp (personal communication, June 25, 2005)

Disadvantages

Vertical integration is not a quick fix. It requires strong commitment by each participant's leadership, and the patience to thoroughly perform the business analysis. In addition, it requires development of an overall enterprise goal for information sharing. In many

organizations, getting buy-in politically or organizationally to an overall goal is very difficult to do. In the context of the national intelligence information sharing effort, this may seem impossible to do because of the number of agencies involved and the differing cultures. In fact, it may not be impossible. If an approach is taken that limits the scope of the goal, and information being shared, then it will be possible. For example, if it is determined that having access to narratives on incident reports and FIR cards will provide information useful to intelligence analysts, then the national information sharing initiative could focus solely on sharing that information. Implementation would focus only on that data being shared. In effect, the FINDER system provides the basic infrastructure to enable dissemination of this specific information. FINDER could be expanded to include the additional fields needed per the limited national goal.

Horizontal Integration

Horizontal integration, as used in this document, refers to the sharing of information between agencies in different geographic jurisdictions with similar missions and objectives. For example, the Florida FINDER project shares data horizontally between law enforcement agencies in Florida, "Many major law enforcement agencies in the Central Florida area have expressed a determination to engineer and deploy effective data sharing architectures. In partnership with the University of Central Florida (UCF), these police organizations have joined in an effort to build an economical system for exchanging information. The initial effort to deploy an efficient data sharing capability will focus on tracking pawned property transactions. This project will be followed by the development of an integrated Field Interrogation Card (FI) capacity." (UCF, 2002 , p. 1) In addition, FINDER sees vertical integration to non-similar

agencies that are different classes: local police, state police, federal police. Reynolds. (personal communication, June 28, 2005)

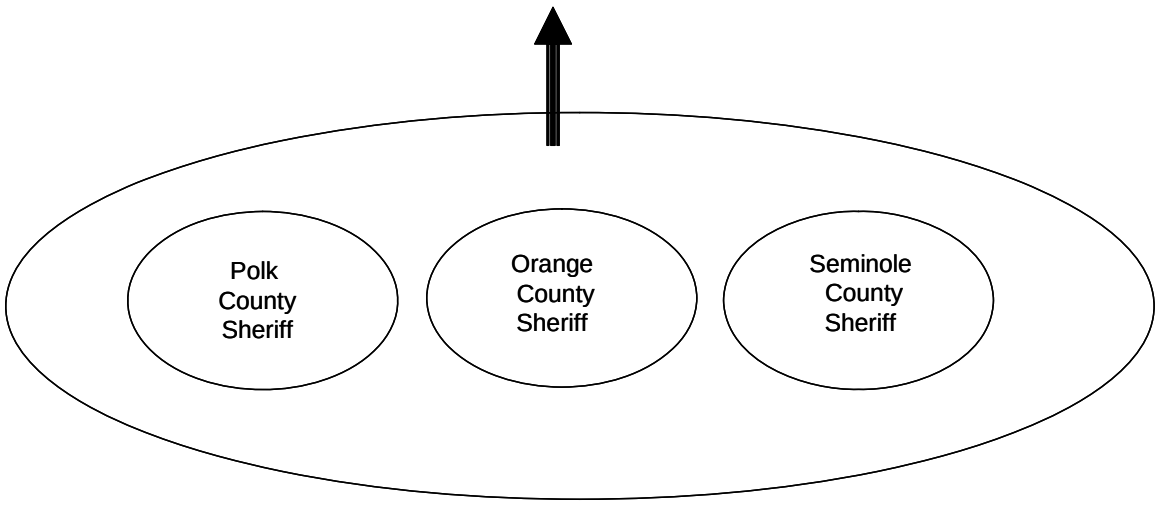


Figure 3 – Horizontal Information Sharing Between Similar Agencies

Advantages

There are some business advantages to this type of information sharing initiative, particularly in a political situation where agencies are not ready to relinquish control of their data. In the national information sharing arena, this will be a significant factor. These include the ability to maintain 100% control over their own data and determine what to share, minimal changes to their core systems are needed. Sometimes this solution is advertised as needing no changes to a system, which may or may not actually be the case.

Disadvantages

One of the disadvantages of this approach is that it does not support consolidated reporting particularly well. As the number of participating systems increases, and the desire to query data across agencies increases, the performance of the system overall could suffer. In

addition, something to be aware of is that semantic differences in data can yield unexpected results[11]. The more the data being queried has its format legislated or standardized, the more consistent query results will be. Each system being queried needs to have similar meanings to the data being queried. For example, a 'name' needs to mean the same thing across the systems. The Global Justice XML Schema is an attempt to standardize semantics of data definitions nationally. "The Global Justice XML Data Model (Global JXDM) is intended to be a data reference model for the exchange of information within the justice and public safety communities. The Global JXDM is a product of the Global Justice Information Sharing Initiative's (Global) Infrastructure and Standards Working Group (ISWG). It was developed by the Global ISWG's XML Structure Task Force (XSTF)." (USDOJ, 2004, p. 1)

Centralization to Support Reporting / Data Warehousing

Another type of integration is centralization of data. This is in essence, reporting facilitated by combining of data from local agencies to regional, state or federal agency. Centralization could also be performed by combining data to a regional server. Some agencies also call this "vertical information sharing between agencies at the local, state, and federal level." (Pinal County, 2003, p. 1), however, it is distinct from the previously discussed vertical integration. In the criminal justice system, the most familiar form of reporting to a central database is the FBI's uniform Crime reporting statistics. Other areas where this type of consolidation is common is in reporting of local agency data to state agencies, such as the reporting of circuit court data to a state court association. For example, the Clerk of Courts in

[11] The Global Justice XML Data Model is intended to reduce semantic differences. As the third-party vendors that build the systems that support their operations start using the model, the semantic differences will be reduced.

Florida report their data to the Florida Association of State Clerks' Comprehensive Case Information System (FACC, 2003). Other jurisdictions may choose to share information via other centralized approaches such as a consolidated database approach where all agencies choose to share a centralized database.

Advantages

Centralizing data has major performance advantages. Database technology has the capability to efficiently access centralized data. In contrast, a solution that requires querying the distributed databases must perform queries individually to each system, and combine the data in real time in memory.

Disadvantages

The centralized data is a replication of data stored in detail at other locations. If the databases at the locations being centralized changes, it may not immediately be recognized in the centralized reporting database. A centralization strategy for multiple agency databases can cause lack of attention on consistency issues. Ross (2003) states "Vendors promote centralization as a miracle elixir to treat data warehouse ailments. They claim it spins independent, disparate data marts into gold by reducing administrative costs and improving performance. Physical centralization may deliver some efficiencies; however, you can't afford to bypass the larger, more important issues of integration and consistency."

Data warehousing has political and legal implications. Data warehousing involves copying data from its source location to a shared location for reporting. Many agencies are reluctant to let 'copies' of their data out to a location that is not within their control.

Business Intelligence or Portal Solution

Business Intelligence, or a portal solution, is not necessarily a true integration from a data or process perspective; it provides a unified user-level view for the information consumer across data from multiple systems[12]. The view may pull information from agency systems that would fall into a horizontal category (e.g. all law enforcement), or they may be from agencies that that fall into a vertical category, or from a combination of the two. Behind the scenes, other integration strategies may need to be used to structure the data so that it can be displayed. An example of this type of solution is the government gateway at http://www.gateway.gov.uk/. "The government portal, part of Blair's new e-government initiative of having 100 percent of government transactions online by 2005, is designed to connect the 200 central and 482 local government institutions with the United Kingdom's 60 million citizens and 3 million businesses." (Microsoft, 2001, ¶4)

Advantages

This approach can yield results very quickly, that will make decision-making in the short-term. In some cases, it also requires minimal changes to existing systems. Another advantage is that it can eliminate the need to replicate data into a reporting database. Replication has the potential to introduce errors if the data is not synchronized or replicated properly. (Ross, 1999, ¶7) states "centralization without data integration and semantic consistency will distract an organization from focusing on the real crux of the problem. Inconsistent data will continue to flummox the organization's decision-making ability."

Disadvantages

This approach requires that the data in the systems being viewed has a way to 'connect' it. For example, a person identifier in one of the systems needs to be replicated in the other. This can be problematic. For example, if a Department of Corrections system used a "Department of Corrections DC#" to uniquely identify a person, but a law enforcement record management system used a "state identification number" or "FBI number" to identify a person, and neither system had the others number in it as a cross-reference, then the two systems could not be pulled together for display in a business intelligence system.

Combination Conceptual Models

It is a mistake in any large-scale integrated systems solution to assume that a single conceptual model will meet all the requirements of a particular information sharing initiative. In particular, with respect to Intelligence Information Sharing, combination of the models can yield the best solution overall. Stonebraker (2004) describes how combined enterprise application integration models are necessary to meet enterprise integration objectives.

As figure 2 on page 35 illustrates, the different integration models can be combined to meet different integration goals. In this system, FINDER is the horizontal integration solution linking law enforcement. Within Orange County, Florida, the ICJIS solution is what is responsible for coordinating positive biometric identification of individuals and tying that to specific arrest documents. The ICJIS hub communicates with other agencies' systems to build

---

[12] A related topic is a federated database in which multiple databases on disparate systems are made to look like a single database. It is technically different from a portal, or business intelligence solution because the integration is done at the data layer, not at the user interface or business layer.

up its internal indices. The Judicial Dashboard, a business intelligence/portal solution takes advantage of a global person index and a case index in the Orange County, ICJIS hub.

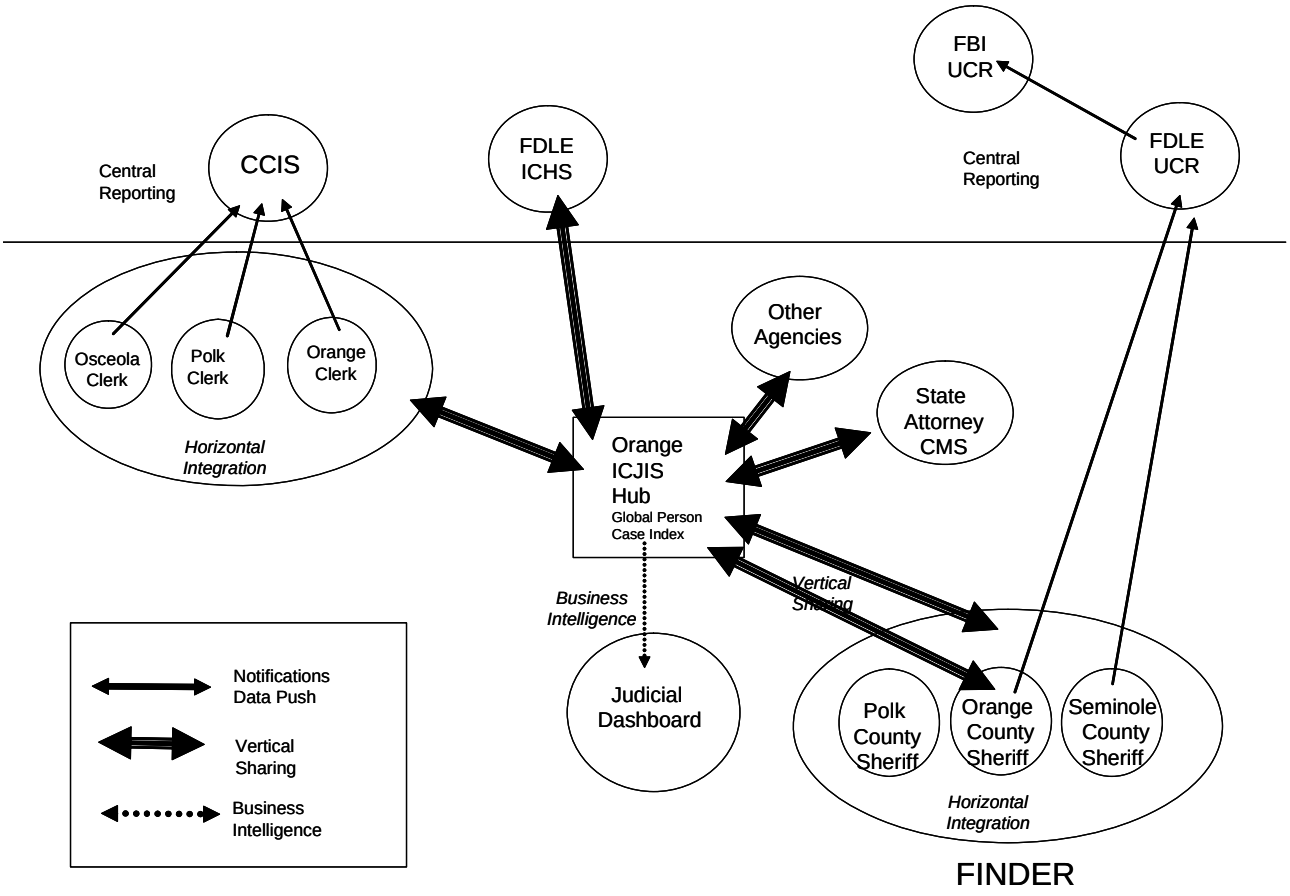
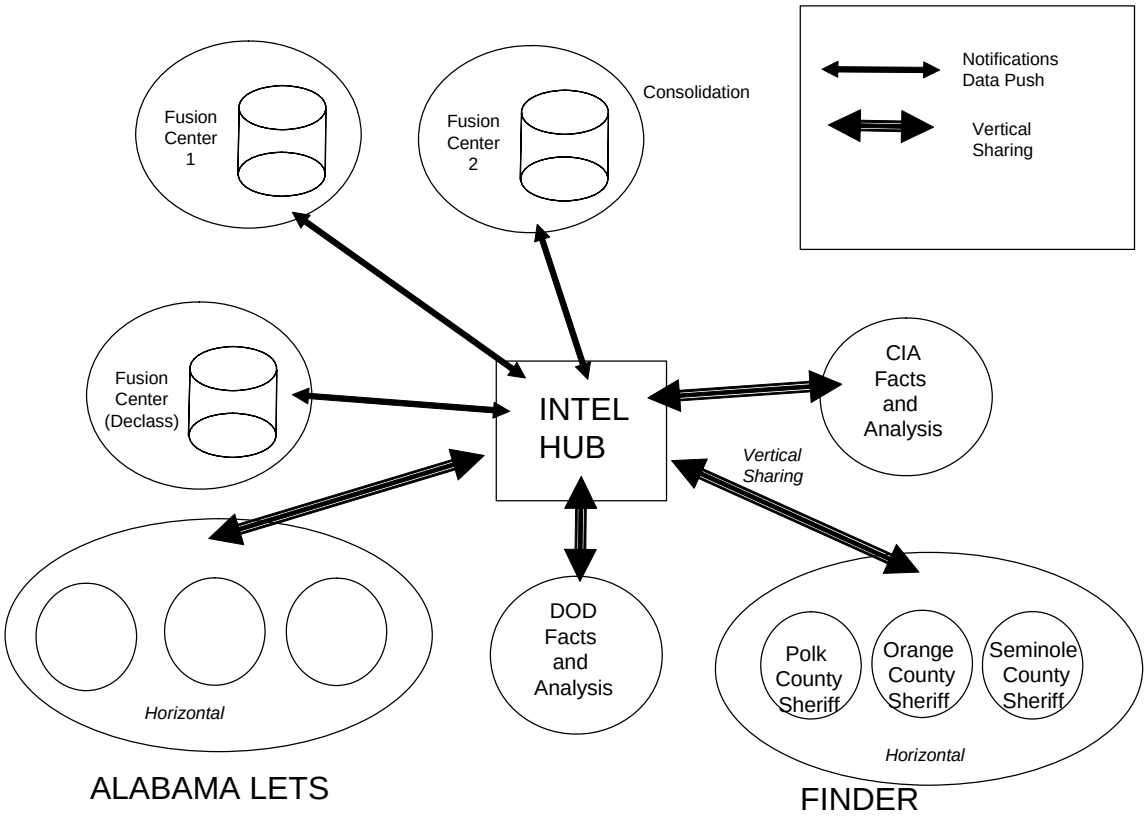


Figure 4 – Combining Integration Models in an Overall System.

In Figure 5, a similar combination is shown that shows how horizontally integrated systems can be combined to provide support for intelligence fusion centers. Essentially, regional information sharing systems are created using horizontal information sharing techniques. An intelligence hub, using predefined business processes for information sharing, is capable of pulling data from each regional information sharing system and routing it to one or more fusion centers based on subscription. The hub would have the capability to route information with different classification levels to the appropriate fusion center. The hub would

also take as input analyses prepared by the various agencies involved in national intelligence and route that to the fusion centers. The fusion centers themselves would have consolidated databases that are continually updated with information throughout the day. Other algorithms such as a 'terrorist threat network monitor' or the Atypical Signal Analysis and Processing (ASAP)[13] method (Hollywood, 2004) would be built to leverage the consolidated databases and the subscription feature of the INTEL hub.

Other agencies that play a role in gathering and analyzing intelligence would also participate in the hub, such as the Defense Intelligence Agency, the Federal Bureau of Investigation, U.S. Marshalls, the Department of Homeland Security, and private agencies.



[13] The Atypical Signal Analysis and Processing (ASAP) method is a method proposed by RAND corporation researchers to solve the problem of "connecting the dots" in Intelligence. It is targeted at solving the problem of

Figure 5 – Combining Integration Models to Support Intelligence Fusion Centers

The Federal Government System Solution: The Markle Recommendation

The Markle Foundation recommended a single, distributed architecture to solve all types of information sharing requirements identified in the 9-11 commission report. (Exhibit A, Page 1, of *Creating a Trusted Information Network for Homeland Security , December 2004,* Markle Taskforce on National Security in the Information Age):

monitoring "large and disparate data streams looking for uncertain and unclear indicators that, taken together, represent potential risks." (Hollywood, 2004, p. iii)

The President Should issue an Executive Order that does the following:

1. Sets the goal of creating a decentralized network along the lines set out in this report.
2. Sets forth specific and clear objectives for improved analysis and information sharing, which each federal agency should be required to meet by December 31, 2004.
3. Establishes guidelines for agencies' collection, use, and dissemination of information, including private sector information.
4. Establishes a process for Executive Branch review of agencies' performance in improving analysis, information sharing, and utilization of private sector information, to take place after December 31, 2004.
5. Designates the DHS as the lead agency of an interagency, public-private process to establish the concept of operations for the network, directs other agencies to offer their full assistance and cooperation, and establishes a timeframe for implementation.
6. Clarifies the respective roles of the DHS, the TTIC, and other federal agencies in information sharing and analysis.

The President should also issue a second Executive Order or other directive that does the following:

7. Establishes guidelines governing the authority of the TTIC and other intelligence, defense, and security agencies to receive, retain, and disseminate information gathered in the U.S. about U.S. persons.
8. Establishes guidelines governing intelligence agencies' ability to set requirements for (or "task") domestic collection of information.
9. Creates within the TTIC appropriate institutional mechanisms to safeguard privacy and other civil liberties.
10. The contents of the Executive Order should be unclassified to the maximum extent possible and put out for notice and comment. In addition, the President should consider introducing legislation to codify the appropriate scope of the TTIC's use and dissemination of information about U.S. persons.

The DHS should do the following:

1. Convene an interagency, public-private group to design a strategy and concept of operations for the decentralized network we describe, which should render a working plan within a year.
2. Work with state, local, and private sector entities to create decentralized analytical centers, foster their ability to communicate with other players in the network, and establish standards for digitization, retention, and communication of information
3. Establish clear mechanisms for responding to requests for threat and vulnerability information from local officials
4. Establish a process for ensuring that as much information as possible is being shared among network entities, including a dispute resolution mechanism to resolve disagreements among agencies about how much information can be shared
5. Establish a process for overseeing federal agency development and implementation of guidelines governing the acquisition, use, retention, and dissemination of private sector information and the creation of methods for ensuring oversight and accountability
6. Work with state, local, and private sector entities to institute information-sharing and analysis objectives for these entities, and establish a process with them for jointly evaluating their performance after December 31, 2004, and thereafter on an ongoing basis.

The FBI should do the following:

1. Establish mechanisms for sharing information with state and local law enforcement agencies and for encouraging those agencies to share directly with other players in the network
2. Establish clear mechanisms for responding to requests for threat and vulnerability information from local officials.

All government agencies with homeland security intelligence responsibilities should do the following:

1. Set up mechanisms to produce more information that can readily be disseminated to other players in the network, including unclassified information.
2. Identify specific categories of private sector information they need, using a scenario-driven process that considers the types of situations they might confront in investigating or seeking to uncover terrorist activity.
3. Institute guidelines governing the acquisition, use, retention, and dissemination of private sector information, and establish methods to ensure oversight and accountability.

Congress should do the following:

1. Undertake to review the performance of federal agencies in improving analysis and information sharing along the lines set out in this report, an din utilizing private sector information while protecting civil liberties.

Essentially, the task force recommended a *horizontal information sharing* solution. Their proposed architecture is very good for solving problems where the analyst is looking for specific pieces of information about something. This supports Clark's contention that intelligence analysis needs to be target-centric (Clark, 2004) and there has to be an a priori question to explore. Case studies of solved crimes from the Florida Data Sharing Model using pawn data retrieved by item description, or defendant name are proof of this. (Wang, 2004, ¶ 2) From a national perspective, sharing watch lists is the perfect example of an appropriate problem for the distributed architecture to solve. In fact, the DHS is now looking at using XML[14] to support counter terror data sharing. (Menke, 2004, ¶ 4). Technical architecture, including XML can help integrate disparate information systems.

Technical Architecture Solutions

Historically, it has been difficult to integrate disparate information systems. Differences in operating system, computer programming language, and databases made it necessary for software adapters[15] to be written specifically for each combination of technology. This led to very expensive integration efforts.

A technical architecture provides the means to implement an overall information sharing model. For example, a business intelligence or portal solution may be implemented using either a consolidated reporting database, or a service-oriented architecture. There is not a one-to-one

---

[14] XML stands for Extensible Markup Language. It provides flexible and adaptable information identification. For example, a person's name might be represented by <FullName>Person's Name </FullName>. XML eliminates *some* of the complexity typically found when integrating disparate information systems.

[15] A software adapter is analogous to a physical fitting or coupling. For example, when the space station was built, it provided adapters so that both the United States and Russian versions of the shuttle could connect to it.

mapping between an overall information sharing model and a technical architecture. This section describes some of the more common technical architectures that can be combined to support integrated justice initiatives.

Calling a Service – A Business Analogy

For years, software programming languages have sought to encapsulate functionality within objects that contain properties and methods. A service is "a fundamental building block that combines information and behavior, hides the internal workings from outside intrusion, and presents a very simple interface" to the consumer. (MSDN 2004, p. 2) Consider this human example. Not so many years ago, if you wanted to find out where your UPS package was, you picked up the telephone and you called the UPS Customer Service Desk. You asked the customer service representative to track your package and you provided a tracking number so that the Customer Service Representative (CSR) could perform the lookup. The CSR looked up the package status in the UPS package tracking computer system, and told you where the package was, and when it was expected to be delivered. The concept of calling a 'method' on an 'object' is identical to this. Instead of using the telephone, a computer program receives the request to track the package with the tracking number built into it. The computer program looks into the same UPS package tracking database, and returns information to the calling program about where the package is, and when it is expected to be delivered.

Service Interfaces

A user interface is the window, or screen, that a person sees when they are running a computer application, or accessing a web page. Behind this visible part of the software are many

different pieces. The first piece is the presentation layer. This layer positions the graphics and text on the application, and captures the data that the user enters in any fields on the screen.

The presentation layer calls another layer, called the business layer that contains business rules such as 'send the data to the purchasing database.' A way to make the business functionality accessible is called a service interface. A service-interface is created, like the telephone call described previously that provides a way for the business layer functionality to be accessed programmatically over a network. Service interfaces can be created using a variety of technologies, from HTTP Post, to web services, to the Distributed Component Object Model (DCOM) or the Common Object Request Broker Architecture (CORBA).

The first service-oriented architectures for many people in the past was with the use of Distributed Component Object Model (DCOM) or Object Request Brokers (ORBs) based on the CORBA specification" (NGA.ORG, 2003, slide 8). These older technologies tended to be vendor-specific. Microsoft created DCOM. IBM, Sun and other vendors participated in the CORBA standard. Neither was open enough to promote universal interoperability. This opened the door to what is now called "web services". A web service is what results when the "service interface is described and exposed using the XML-based standards such as SOAP, and WSDL." (MSDN, 2003, p. 7). Putting web services together into architecture requires that you also include the pieces of the system that interact with the user community, or that perform the process-focused integrations between systems.

A service interface is shown in the following diagram:

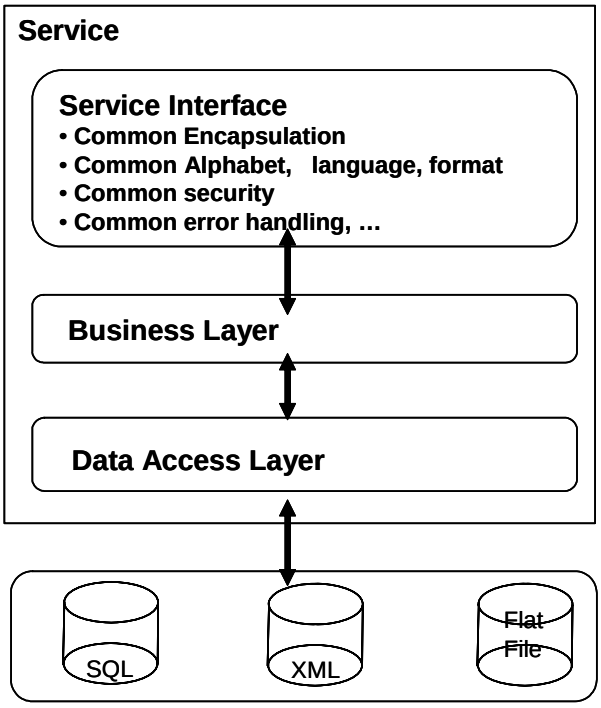


Figure 6 – Service Interface

Service-Oriented Architecture

Much of existing literature and system documentation confuses the concepts of web services and service-oriented architecture[16](SOA). "SOA is not just an architecture of services seen from a technology perspective, but the policies, practices, and frameworks by which we ensure the right services are provided and consumed." (MSDN 2004, p. 3) Service Oriented Architectures are a way of assembling services to perform business functions, not merely a collection of services that are called. Service Oriented Architectures are not a new thing.

According to the Global Justice Information Sharing Initiative, "SOA is a business-driven, open standards software technology system development process, built on existing

infrastructure (e.g. NLETS[17], LETS[18], and the U.S. Department of Labor) to enable information sharing at the local, state, and national levels that respects current diversity and heterogeneity" (Global Justice, 2003, p. 3). "A service-oriented architecture is essentially a collection of services. These services communicate with each other. The communication can involve either simple data passing or it could involve two or more services connecting some activity." (NGA.ORG, 2003, slide 8).

Table 1. - Web services and SOA (MSDN 2004, p. 4)

Enabled by Web services	*Technology neutral*	Endpoint platform independence.
	Standardized	Standards-based protocols.
	Consumable	Enabling automated discovery and usage.
Enabled by SOA	*Reusable*	Use of Service, not reuse by copying of code/implementation.
	Abstracted	Service is abstracted from the implementation.
	Published	Precise, published specification functionality of service interface, not implementation.
	Formal	Formal contract between endpoints places obligations on provider and consumer.
	Relevant	Functionality presented at a granularity recognized by the user as a meaningful service.

[16] In this context, the word architecture is used to describe how

[17] The National Law Enforcement Telecommunication System (NLETS) was created by the principal law enforcement agencies of the states nearly 35 years ago." (NLETS, 2004) It serves the justice community at multiple levels and provides a way for law enforcement to share justice information across state boundaries.

[18] The Law Enforcement Tactical System (LETS) is a system created by the State of Alabama to promote interstate information sharing.

Service-oriented architectures have many benefits when implemented properly (MSDN 2004, p. 4):

- **There is real synchronization between the business and IT implementation perspective**. For many years, business people haven't really understood the IT architecture. With well designed services we can radically improve communications with the business, and indeed move beyond alignment and seriously consider convergence of business and IT processes.
- **A well formed service provides us with a unit of management that relates to business usage.** Enforced separation of the service provision provides us with basis for understanding the life cycle costs of a service and how it is used in the business.
- **When the service is abstracted from the implementation it is possible to consider various alternative options for delivery and collaboration models.** … However it is entirely realistic to assume that certain services will be acquired from external sources because it is more appropriate to acquire them. For example authentication services, a good example of third party commodity services that can deliver a superior service because of specialization, and the benefits of using a trusted external agency to improve authentication.

Service-Oriented Architecture (SOA) implies that it "is critical to implement processes that ensure that there are at least two different and separate processes – for provider and consumer." (MSDN 2004, p. 5). In a service oriented architecture, "what we have is a significant number of process areas where (depending on the nature of the service) there is deep collaboration between provider and consumer. Potentially we have a major reengineering of the

software delivery process. Although we have two primary parties to the service-based process, there are three major process areas" (MSDN 2004, p. 5) that need to be managed: delivering the service implementation, provisioning of the service – the life cycle of the service as a reusable artifact, and the consumption process.

It is important to follow a top-down process when defining an overall service-oriented architecture, so that the overall business processes are accomplished. Several modeling techniques can be used to do this, such as use-cases, or Unified Modeling Language (UML)[19]. The simplest form of use-cases is written from a business stake holder's perspective and describe an interaction with a system from the time a user interacts with a screen in the application, to how the system executes specific program code to implement the user's instructions. Use-cases can be decomposed into their component parts which can then be implemented with appropriate technology such as services and components. When creating an overall system, all of the use-cases for the system can be defined, they can then be analyzed into supporting processes and core business processes. The supporting processes can be implemented by creating service interfaces to the various systems being integrated. This is an overall development process that should be familiar to any enterprise-class developer.

[19] Unified Modeling Language (UML) is the way that many information technology professionals model not only application structure, behavior, and architecture, but also business process and data structure. A model plays the analogous role in software development that blueprints and other plans (site maps, elevations, physical models) play in the building of a skyscraper. Using a model, those responsible for a software development project's success can assure themselves that business functionality is complete and correct, *before* implementation in code renders changes difficult and expensive to make.

Sample Use-Case: Anonymous Tip that Someone is a Terrorist

An anonymous caller calls 9-11 and provides a tip that a person is a terrorist.

Assumptions[20]:

5. *The caller is unknown.*
6. *The validity of the call is not known.*

Actors:[21]

Caller, FIR system, local analyst, national analyst, 9-11 operator

Basic Course[22]

1. Anonymous Caller calls 9-11.
2. *9-11 operator* answers the phone.
3. Results of call are documented on a field investigative report (FIR) form. Checkbox on the form is checked to indicate indicates possible terrorist activity.
4. The *9-11 operator and the system* both route the information to the "analyst"
5. Information (person, location, and tactic) is documented in a local intelligence database.
6. Local "analyst" determines validity of claim by dispatching a detective to investigate.
7. If the information is deemed to be 'qualified', it is 'shared' with a national intelligence database from the person, location, and tactic (target-centric) perspectives.

In the next section, we turn from technical considerations to research questions.

---

[20] The assumptions state what is true before the use case begins.
[21] Actors are the people, or systems that are involved in the use-case.

CHAPTER THREE: METHODOLOGY

The approach to be used is based on Robert K. Yin Case Study Research Design[23]. The unit of analysis is a specific integrated information system. Raw data describing the integrated systems and their business context was gathered using a combination of surveys, one-on-one interviews, and focus groups. Integration and Interoperability requirements (shown as R1 – Rn below) were gathered from stakeholders in the law enforcement intelligence community in an interview format, and by inspection of written project artifacts. The systems were evaluated for their ability to meet the interoperability and interconnection requirements using a matrix such as the following:

Table 2 - Requirements Matrix

System	R1	R2	R3	R4	R5	R6	R7	R8	R…	R*n*	JTTF	LEA
Florida Law Enforcement Data Sharing	[0-9]	[0-9]	[0-9]	[0-9]	[0-9]	[0-9]	[0-9]	[0-9]	[0-9]	[0-9]	[0-9]	[0-9]
Alabama Law Enforcement Tactical System Portal	[0-9]	[0-9]	[0-9]	[0-9]	[0-9]	[0-9]	[0-9]	[0-9]	[0-9]	[0-9]	[0-9]	[0-9]
Orange County Integrated Criminal Justice Information System	[0-9]	[0-9]	[0-9]	[0-9]	[0-9]	[0-9]	[0-9]	[0-9]	[0-9]	[0-9]	[0-9]	[0-9]
Total:	[0-27]	[0-27]	[0-27]	[0-27]	[0-27]	[0-27]	[0-27]	[0-27]	[0-27]	[0-27]	[0-27]	[0-27]

In addition, specific qualitative observations were documented.

---

[22] The Basic course is the way that the process will occur 90% or more of the time. An alternate course describes what might happen if a condition in the basic course, or an assumption is not true.

Business Process

Normally, when an information sharing system is designed, the first item to start with to begin to shape the system is the business requirements. For example, when creating a statewide integrated court system, a solution whose primary goal is to provide policy makers with evaluation information on the previously implemented projects (such as number of probate cases processed) will be a very different solution than one whose goal is to allow every circuit to be able to search the cases in every other circuit. In the case of intelligence information sharing, not only do no requirements exist at a detailed enough level to be useful, but even when they are known, the stakeholders in the processes are entrenched in doing business as usual. In this case, we will resolve these issues by inspecting the attempts of the various governmental entities involved in intelligence information sharing, homeland security, and international defense, as well as by inspecting the possibilities afforded by combining the regional information sharing initiatives.

Questions

These are the questions that were asked during the course of the interviews, or inspection of system documentation.

Business Questions

1. How is the governance of the integration solution structured?
2. Does the governance structure interact with the governance structure of any other integration solutions/

---

[23] Yin, Robert K. (1994) *Case Study Research: Design and Methods*. California: Sage

3. Is the data shared real-time?
4. Who are the stakeholders in the information sharing initiative?
5. At a high-level, what data (e.g. people, places, things) is being shared?
6. Are there any state or federal laws governing access to the records?
7. Is there data that the participants would like to share that is not currently accessible?
8. What considerations for accessibility by Federal homeland security agencies were designed into the system?
9. How many collectors are feeding the system?

Technical Questions

1. What are the source data systems?
2. What is the architecture of the solution?
3. Is the architecture scaleable?
4. Is the solution experiencing performance problems?
5. What steps were taken to ensure network security?

Requirements for National Information Sharing

These requirements were developed by examining the literature with respect to information sharing and intelligence, and discerning requirements from the overall goals found in the literature.

Also note that the ability or the inability of any of the regional systems to meet these requirements should not be viewed as a deficiency in the regional system, as the initial goal of the regional system may not have had anything to do with the goals of a national intelligence

information sharing effort. The reason for comparing these systems to these national requirements is simply to evaluate how feasible the Markle task force recommendations are in connecting the existing disparate systems.

Study Variables

The following variables were developed to measure and evaluate the various components of the cases under study.

R1: Ability to search for data related to a specific person.

In order for data about a person to be shared between jurisdictions, there must be a way to search for the person in each system.

Table 3 – Ratings for Person Searching

Rating	Criteria
0	There is no ability to search for data related to a person in the system
3	There is ability to search for data related to a person by name only.
5	System possesses the ability to search for data related to a person by name and a specific identifier such as driver's license or social security number.
7	System possesses the ability to search for data by name, social security number, driver's license, date of birth, gender, and race.
9	System possesses the ability to search for data by biometric, name, social security number, drivers license, date of birth, gender, and race.

R2: Data Accuracy

This requirement refers to the overall data accuracy. An example of accuracy in a data sharing system is to make sure the data in the evaluated system is tied to the correct target (person or address). The General Accounting Office (GAO) describes accuracy as reflecting "the data entered at the source or, if available, in the source documents." They further define a subcategory of accuracy to be consistency which "refers to the need to obtain and use data that are clear and well-defined enough to yield similar results in similar analyses. For example, if data are entered at multiple sites, inconsistent interpretation of data rules can lead to data that taken as a whole are unreliable." (GAO, 2002, p.8) Consistency is not considered in this rating because it is up to each agency contributing data to provide for consistency.

Table 4 – Ratings for Data Accuracy

Rating	Criteria
0	The system has no capability to ensure data accuracy.
7	The system receives data as published by agencies providing data.
9	The system receives data as published by agencies providing data and periodically performs automatic audits to verify that data matches the agencies' source data.

R3: Data Completeness

This requirement refers to the overall completeness of the data. The GAO defines completeness as containing "all of the data elements and records needed for the engagement." (GAO, 2002, p.8) An example of completeness refers to the percentage of time that the driver's license value for a person is filled into the data field. This rating refers to the systems ability to measure and manage overall completeness, not the actual data completeness itself.

Table 5 – Ratings for Data Completeness

Rating	Criteria
0	The system has no capability to ensure data completeness.
5	The system operators periodically measure completeness through query operation and communicate completeness to the operators of the source system on key fields.
9	The system has automatic capabilities to measure completeness and provide feedback to the source systems.

R4: Agency Participation

Are all of the 'right' agencies participating in the information sharing initiative? For example, if parking tickets are deemed to be relevant to the information sharing effort, is the agency that issues the parking tickets part of the information sharing solution?

Table 6 – Ratings for Agency Participation

Rating	Criteria
0	The system has 0% of the targeted agencies participating participation.
3	The system has 25% of the targeted agencies participating
5	The system has 50% of the targeted agencies participating.
7	The system has 75% of the targeted agencies participating.
9	The system has 100% of the targeted agencies participating.

R5: Person Identification

Person identification is one of the more problematic aspects of the problem of information sharing. Constitutional factors, as well as current policy debate are precluding the creation of a national identification card, or national biometric for identifying persons residing in

this country. This is one of the key issues that will need to be resolved in order to gain the most benefit from national information sharing initiatives. This requirement states that the system needs to have some way to identify a person within the system.

Table 7 – Ratings for Person Identification

Rating	Criteria
0	The system only uses name to identify a person.
3	The system has an internally generated unique identifier to identify a person.
5	The system has an internally generated unique identifier to identify a person which is tied to a non-biometric government-issued unique identifier such as a driver's license.
7	The system has some local biometric capabilities, or leverages AFIS data in addition to having an internally generated unique identifier to identify a person which is tied to a non-biometric government-issued unique identifier such as a driver's license.
9	The system incorporates a national, biometric unique identifier in addition to all criteria for a rating of 7.

R6: Leverages a Decentralized Network Approach

One requirement is that a decentralized network approach be taken. The system should not require centralization of data or process in order to operate.

Table 8 – Ratings for Decentralized Network Approach

Rating	Criteria
0	The system is centralized.
5	The system is a hybrid between centralized and decentralized.
9	The system is completely decentralized.

R7: Supports an Overall Intelligence Analysis Process

In this requirement, the regional information sharing systems' ability to support a higher-level intelligence analysis process is evaluated. Specifically, what data does each system provide for use by others in the intelligence community?

Table 9 – Ratings for Overall Intelligence Analysis Process

Rating	Criteria
0	The system provides access to no data for use by others in the intelligence community.
3	The system provides access to person information, and criminal history information
5	The system provides access to person information, criminal history information, address information, and field investigative report information
7	The system provides access to person information, criminal history information, field investigative report information, activity at address information, and 9-11 call information, and traffic ticket information.
9	The system provides access to, criminal history information, field investigative report information, and 9-11 call information, traffic ticket information, and local intelligence products.

R8: Flexibility to Change as the Intelligence Analysis Processes Change

It is apparent that the overall process for intelligence analysis and information sharing has not yet been defined. This deficiency means that each regional information system needs to be built to adapt to future needs by having a flexible architecture.

Table 10 – Ratings for Intelligence Process Change

Rating	Criteria
0	The system would need to be re-designed completely to be able to support changing intelligence processes.
5	The system architecture would need some modification to support changing intelligence processes.
9	The system architecture needs no modification to support changing intelligence processes.

R9: Provides for "tasking"

A key means of operation in the intelligence is that the intelligence analysts are able to respond to "taskings". In turn, they may need to "task" the individual collectors of raw data to be analyzed. The requirement stated here is that the system have some way to respond to a "tasking" for specific information, such as, "keep an eye out for suspicious activity around power plants" that would find its way to the law enforcement or private agency data collectors.

Table 11 – Ratings for Support of Taskings

Rating	Criteria
0	The system would need to be re-designed completely to be able to support taskings intelligence processes.
5	The system architecture would need moderate modification to support taskings back to law enforcement.
7	The system architecture needs minor modification or customization to support taskings or BOLOs back to law enforcement.
9	The system can be configured to support taskings back to law enforcement.

R10: Ability to Search by Location

The ability to search for an event by location is also important

Table 12 – Ratings for Search by location

Rating	Criteria
0	The system does not support search by location
5	The system contains the data to search by location, but no facilities to query that data.
9	The system supports search by location, and can bring up related events.

R11: Ability to Search by Keyword

The ability to search for an event in each regional system by keyword is also important for allowing analysts to search for specific type of incidents or events, such as "TNT", or "flight training."

Table 13 – Ratings for Search by keyword

Rating	Criteria
0	The system architecture does not support keyword searching
5	The system architecture technically supports

	keyword searching.
9	The system supports keyword searching for data fields and document narratives

R12: Documentation

In order for a system to be integrated with another system, documentation describing the system and its data elements needs to be available, as does information exchange packet documentation.

Table 14 – Ratings for Documentation

Rating	Criteria
0	The system does not have documentation.
5	The system has user documentation and some technical documentation.
7	The system follows a system development methodology which provides for user documentation, design documentation, and technical documentation. Some documentation has been created.
9	The system follows a documented methodology and all documentation in the methodology has been created.

CHAPTER FOUR: RESULTS AND DISCUSSIONS

This chapter presents the results of the research specific to each regional system, and how well they meet the requirements for national information sharing that were defined earlier in this document.

Specific Integration Solution Findings

This section presents the findings for each one of the case study systems. For each system, we describe the political environment, business problem being solved, agencies participating as of this writing, business process findings, technical findings, and the evaluation matrix.

Alabama Law Enforcement Tactical System Portal (LETS)

The Alabama Law Enforcement Tactical System (LETS) "is an integrated justice information system (IJIS) designed to unify the state's vast data resources – such as Motor Vehicle Department (MVD), court, and correctional facility records – which were disparately hosted and difficult for outside users to search." (Microsoft, 2003) In the regular course of law enforcement business, it is useful to be able to access driver's license records, jail records, law enforcement record management system records from other jurisdictions, and the court system. The conceptual business requirement for this system falls into the consolidated reporting category. The information from each jurisdiction *conceptually* is combined into a big-picture view that can be looked at from an overall state perspective. Due to financial and jurisdictional requirements, the LETS portal provides a mechanism to achieve this goal without actually consolidating the actual data in each jurisdictions database. It is a true portal. One of the key design aspects of this system was that "The SAICS task force wanted to leave the data "as is" as much as

possible…We did not want to do a data warehouse approach, in which data is cleaned up and massaged into a specific format. SAICS participants got to keep autonomy of their databases" (GCN, 2003, ¶6)

Political Environment

LETS was created because all agencies at the state level could not share information, and because creating a consolidated data warehouse for the information was cost-prohibitive to the State of Alabama. The agencies were open to making their data available to other Alabama agencies. The type of information that the Alabama agencies wanted to share included drivers licenses, drivers history, pardons and paroles, warrants, protection orders, and local jail data. The portal itself was modeled after a project in Nebraska. A. Parrish (personal communication, April 11, 2005)

Agencies Participating

The agencies participating in LETS include jail facilities, law enforcement, and courts (prosecutors, judges) throughout Alabama. The system has over 4500 users. (Microsoft, 2003)

Business Process Findings

The Alabama LETS system provides inquiry into multiple agencies data. It does not require any business process changes by any of the participating agencies.

Technical Findings

The Alabama LETS Portal was created using Microsoft .NET and C# for its programming environment, Microsoft SQL Server 2000 for its database, and Microsoft Internet

Information Server for its webserver. In some cases, data is replicated to the portal database and in some cases data is queried directly.

Funding Source

The project was initially funded by a $12,000,000 Congressional earmark.

Evaluation Matrix

Table 15 – Alabama LETS Requirement Matrix

Requirement	Comments	NLETS Rating
R1: Ability to search for data by person	**90% of system access is performed by driver's license number. Other data that can be used to search for a person includes social security number, name, address, gender, race, county of residence.**	**7**
R2: Data Accuracy	**Data quality in LETS is reflective of the data available in each participating agencies' systems. Data included is driver's licenses, driving history, pardons, paroles, warrants, protection orders, local jails.**	**7**
R3: Data Completeness	**Data is as complete as the source data systems**	**5**
R4: Agency Participation	**Agencies that participate include corrections, courts, and law enforcement.**	**9**
R5: Person Identification	**The primary key for a person is driver's license number.**	**7**
R6: Leverage Decentralized Network Approach	**This system is built using a decentralized approach.**	**5**
R7: Supports Intelligence Analysis Process	**The system can be queried in support of intelligence analysis by person, location, or any other available information**	**3**
R8: Flexibility to Change as Intelligence Analysis Processes Change	**The system is designed to provide a state-level view of the data in all of the jurisdictions in Alabama. It was not designed to be flexible enough to support changing intelligence analysis processes.**	**7**
R9: Provides for "tasking"	**The system is not designed to support the concept of 'taskings' back to an agency to get additional information. It is a portal system designed to view existing information.**	**0**
R10: Search by Location	**The system can be queried by location.**	**9**
R11: Search by Keyword	**The system cannot be searched by specific keyword, although it can be searched by specific data fields.**	**5**
R12: Documentation	**The system has no overall plan in writing that can be shared, but a case study is available on Microsoft's web site.**	**0**

Florida Data Sharing Initiative

Political Environment

The Florida Data Sharing Network (FINDER) was created in an environment where agencies were initially reluctant to share information by providing access to their internal computer network, or by providing their data to a central repository such as a data warehouse. The technical architecture that was created for FINDER alleviated the political concerns of the participating agencies.

Agencies Participating

FINDER has broad support within the State of Florida law enforcement community. Current members of FINDER include: Alachua County Sheriff's Office, Altamonte Springs Police Department, Brevard County , Sheriff's Office, Charlotte County Sheriff's Office, Citrus County Sheriff's Office, Collier County Sheriff's Office, Flagler County Sheriff's Office, Hillsborough County Sheriff's Office, Kissimmee Police Department, Lake County Sheriff's Office, Marion County Sheriff's Office, Orange County Sheriff's Office, Orlando Police Department, Osceola County Sheriff's Office, Polk County Sheriff's Office, Port Orange Police Department/Reg Com Cntr, Port St Lucie Police Department, Seminole County Sheriff's Office, Tampa Police Department, University of Central Florida Police Department, and the Winter Garden Police Department.

The 8 current Affiliate members include: Bunnell Police Department, Edgewater Police Department, Lake Mary Police Department, Longwood Police Department, New Smyrna Beach

Police Department, Oviedo Police Department, Sanford Police Department, Winter Springs Police Department

The 21 agencies that are currently processing the memorandum of understanding include: Belleair Beach Police Department, Belleair Police Department, Broward County Sheriff's Office, Chipley Police Department, Clay County Sheriff's Office, Clearwater Police Department, Gulfport Police Department, Indian Shores Police Department, Jacksonville Sheriff's Office - Duval County, Kenneth City Police Department, Largo Police Department, Lee County Sheriff's Office, Miami Police Department, Pinellas County DJC/Sheriff's Office, Pinellas Park Police Department, Plant City Police Department, St Pete Beach Police Department, St Petersburg Police Department, Tarpon Springs Police Department, Treasure Island Police Department

Washington County Sheriff's Office. In addition, verbal commitment has been obtained from 28 other agencies within the State of Florida,

Business Process Findings

FINDER is an inquiry-only system. Because of this, the business processes from each agency remain independent.

Technical Findings

FINDER was designed and implemented using state-of-the-art technology. In the FINDEr architecture, each agency hosts and maintains a set of inquiry web services outside of their internal network. These services allow other agencies to request and retrieve information from other agencies. (Eaglin, Reynolds, Flint, 2003). The architecture is shown in the figure below:

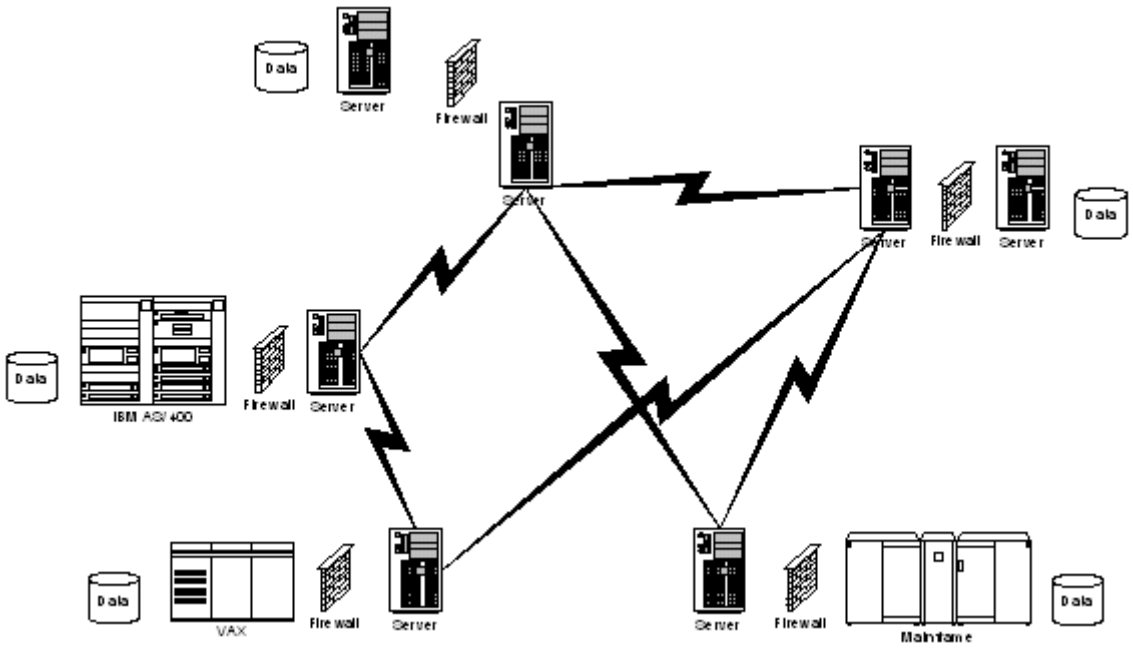


Figure 7 – FINDER Architecture

Funding Source

FINDER is funded through a combination of agency contributions based on agency size, seed funding provided by the Orange County Sheriff's Office, and grants.

Evaluation Matrix

Table 16 –Florida Data Sharing (FINDER) Requirement Matrix

Requirement	Comments	FINDER Rating
R1: Ability to search for data by person	**Data can be searched by person name, driver's license and social security number**	**7**
R2: Data Quality	**This is dependent on the quality of the participating agencies' underlying data**	**7**
R3: Data Completeness	**This is dependent on the quality of the participating agencies' underlying data**	**5**
R4: Agency Participation	**Agency participation is good**	**7**
R5: Person Identification	**Person identification is reliant on driver's license and social security number**	**7**
R6: Leverage Decentralized Network Approach	**FINDER has a very decentralized architecture**	**9**

Requirement	Comments	FINDER Rating
R7: Supports Intelligence Analysis Process	**FINDER provides data that could be used by an analyst. There may be more relevant data available that could be published using FINDER's architecture.**	**5**
R8: Flexibility to Change as Intelligence Analysis Processes Change	**FINDER is built using an easy-to-extend web services architecture. The difficulty in change will be that the agencies feeding FINDER will need to change their systems to provide additional data. FINDER itself is very easy to modify.**	**9**
R9: Provides for "tasking"	**The FINDER architecture does not support pushing information back to an agencies operational system**	**5**
R10: Search by Location	**There is no current search by location, but the address information is stored in the database**	**5**
R11: Search by Keyword	**There is no current keyword search**	**5**
R12: Documentation	**FINDER has a technical installation manual, but no design documentation was provided.**	**5**

Orange County Integrated Criminal Justice Information System

In 1993, three Criminal Justice Process focused committees (executive, management, technical) were created at the recommendation of the Kalmanoff and Coopers & Lybrand studies. These were called the Justice Information Teams. Today, the Criminal Justice/Public Safety Coordinating Council functions as the executive level committee. The committees' mission was to develop short term and long-term technical solutions to improve the efficiencies of the criminal justice community within Orange County. The teams are comprised of dedicated individuals from Court Administration, Clerk of Court, State Attorney, Public Defender, Orange County Sheriff, Orlando Police Department, Florida Department Corrections, Orange County Information Systems and Services, and Orange County Corrections Department.

In 1998, the JIT teams held a retreat to focus on specific data sharing opportunities to help all agencies improve efficiencies. The result of this retreat was consensus on the need for an integrated criminal justice system (ICJIS). Another important criterion for the creation of ICJIS was the requirement that each agency continues to meet their independent taxpayer service

objectives. For this reason, they need to maintain independent information systems that support their service objectives. An independent consulting company, Nichols Research, was engaged to identify a means to achieve these objectives. The Nichols' recommendation included a middleware solution to push and pull data between the systems using XML or other open systems architecture. They also assessed each agency's readiness to participate in an integrated middleware system. The Nichols study results from 1999 can be found online at http://www.orangecountyfl.net/dept/County_Admin/public_safety/CJC/ICJIS/default.htm

Subsequent to this, an RFI was created to gather information on available middleware solutions. Vendors with traditional Enterprise Application Integration infrastructures presented their solutions. Subsequent to the RFI, the National Center for State Courts was engaged to create an RFP requesting specific pricing for their middleware solutions.

The Jail Oversight Commission as described in the Nichols study independently validated the need for an ICJIS system in 2002. Also in 2002, a facilitation project to help the CJIS agencies understand ICJIS at a functional level was performed.

Beginning in October 2002, detailed requirements gathering began for Phase I of ICJIS. These requirements were gathered primarily from the back-end (records departments) of the agencies' operations. Business scenarios were documented to crystallize the requirements for data movement throughout the Integrated Criminal Justice System. Opportunities for incremental process improvement were also identified.

Goals

Orange County's Integrated Criminal Justice Information System (ICJIS) is intended to improve decision-making and operational efficiencies by eliminating redundant data entry and

improving access to criminal justice system information throughout the entire Orange County Criminal Justice System. Contained within ICJIS will be the ability to identify a defendant in a common manner throughout the entire justice processes. End-users also need to have the ability to create reports from the CJIS data, and access the data in text or graphical form.

Logical Design

The Integrated Criminal Justice Information System (ICJIS) connects each agency's operational system, while also providing an architecture that allows each individual Criminal Justice Agency to leverage their investment in their existing systems. This is shown in the Logical Design below.

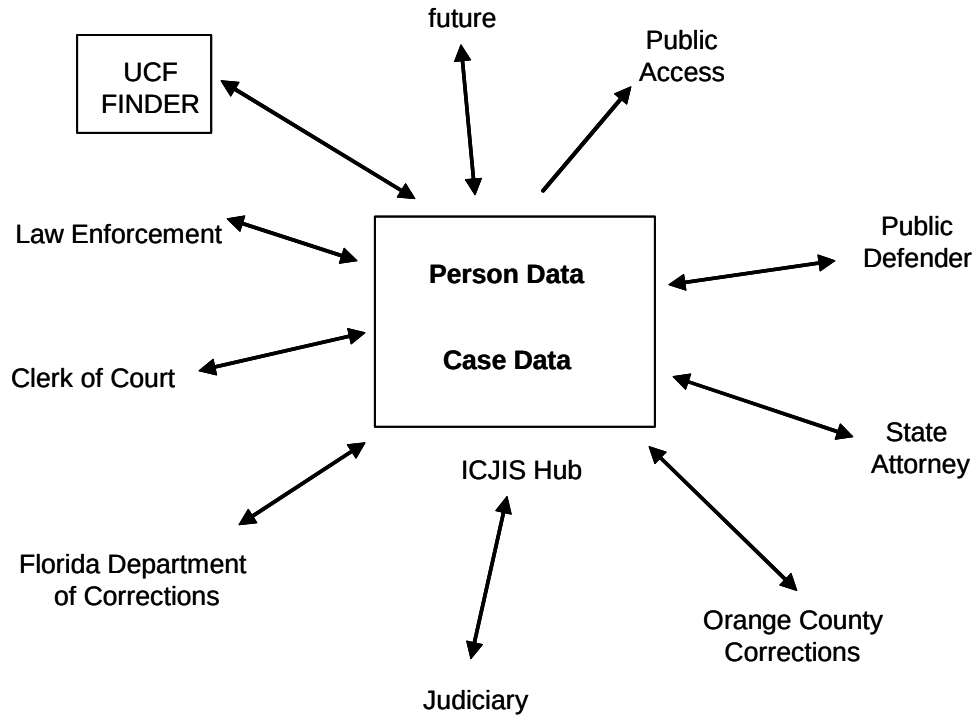


Figure 8 – Orange County ICJIS Logical Diagram

As shown in the figure above, the ICJIS system is designed to be a hub and spoke architecture that connects the agencies within Orange County to share person and case data.

Political Environment

In the startup phase of the operational part of the project (2002-2003), there was some stated disbelief by technical staff in several of the agencies that the project would actually be a success. Two things were done to overcome this resistance. First, a small initial phase was scoped out that essentially would prove the data sharing approach, and could be performed with minimal staff and resources. Second, and most importantly, the executive level committee supported the ICJIS concept, and continued to support the project during the time it took to prove the technical feasibility.

Agencies Participating

Initial agencies participating in ICJIS include Florida 9th Judicial Circuit agencies: Court Administration, Clerk of Court, State Attorney, and Public Defender. The Orange County and Municipal agencies involved include the Sheriff, Orlando Police Department, Orange County Information Systems and Services, and the Orange County Corrections Department. The Florida Department of Corrections is also an initial participant.

Business Process Findings

In this project, the business processes are of primary importance. Cross-Agency processes are documented and analyzed prior to system automation, as many opportunities to improve efficiencies through technology can be found.

Technical Findings

This system is implemented using Microsoft code blocks, C#, Microsoft BizTalk Server 2004, and Oracle 9i. All external integrations are performed using GJXDM[24].

Funding Source

This project is funded by the Orange County Board of County Commissioners. Currently, three phases of the project including arrest data, court data, and imaging are funded.

Evaluation Matrix

This is the evaluation matrix for the Orange County Integrated Criminal Justice System.

Table 17 – Orange County Integrated Criminal Justice System Requirement Matrix

Requirement	Comments	ICJIS Rating
R1: Ability to search for data by person	**ICJIS contains a global person index with fields including state identification number, sheriff's jacket number, FBI number, name,**	**7**
R2: Data Quality	**Data quality is dependent on the accuracy of initial data entry by the original data creator. Training law enforcement and other agency personnel that their data entry is what counts is of critical importance.**	**7**
R3: Data Completeness	**The ICJIS data, other than the global person index and global case index is being created on a forward-looking basis only, so historical data is not currently planned to be available. In addition, it is rare for all of the data elements, such as business address to be filled in on the charging documents that are sent to ICJIS. Finally, ICJIS does not contain all of the data of interest to intelligence analysts, such as FIR's.**	**5**

[24] The Global Justice XML Data Model (GJXDM) is an Extensible Markup Language (XML) schema that is intended to be used in all justice-related information exchanges. When agencies need to share information, they select a subset of the data elements in the data model to exchange, and exchange the data using GJXDM as a guide. It is a product of the Global Justice Information Sharing Initiative's (Global) Infrastructure and Standards Working Group (ISWG).

Requirement	Comments	ICJIS Rating
R4: Agency Participation	**ICJIS has participation by the key criminal justice stakeholders within Orange County and the Florida 9th Judicial Circuit. It is expanding to include the Florida Department of Children & Families, the Florida Department of Juvenile Justice, and the Florida Department of Law Enforcement. Other agencies that could be included could be the agencies that write parking tickets.**	**5**
R5: Person Identification	**ICJIS processes are integrated with fingerprint identification processes for defendants, however, other persons that may need to be searched for in the system are not biometrically identified. A person index that supports non-biometric person identification (e.g. drivers license, social security number, other demographics) is being developed for the civil side of the integration.**	**7**
R6: Leverage Decentralized Network Approach	**ICJIS uses GJXDM and standard information exchange packages to interact with external systems. It is only reliant on centralization within Orange County agencies (vertical integration). It is designed to integrate with other regional systems that use GJXDM and web services for communication.**	**5**
R7: Supports Intelligence Analysis Process	**ICJIS was not designed specifically to support the process of intelligence analysis. It is designed to support integration of person and case data within Orange County so that a true and accurate picture of a defendant within Orange County could be obtained at any point in time.**	**3**
R8: Flexibility to Change as Intelligence Analysis Processes Change	**ICJIS is built using a very flexible, modifiable architecture. The tools chosen for use, including the GJXDM schema, and the middleware tool selected provide the ability to change and adapt to different data sources and destinations, and different business processes.**	**9**
R9: Provides for "tasking"	**ICJIS contains the concept of work queues at many points within its process, so it is a natural extension to include taskings from an intelligence consumer that would be provided to law enforcement officers to collect.**	**9**
R10: Search by Location	**ICJIS contains addresses of arrest, business, and home addresses.**	**5**
R11: Search by Keyword	**ICJIS has the ability to search charging documents by keyword. ICJIS does not currently contain incident reports or field investigative reports.**	**9**
R12: Documentation	**ICJIS has a strategic plan, and all subsystems are documented with requirements documents, functional specifications, and technical specifications. Exchanges are also documented using Information Exchange Packages (IEP) for GJXDM.**	**7**

Discussion

This section first summarizes the rating results. It then describes how research questions are supported and answered by the findings. In summary, without an overall goal for intelligence information sharing, and a defined process for performing collection and analysis across agencies at local, state, federal, and probably international levels, any information sharing system will only have limited success.

Rating Summary

The following table provides a summary of the ratings for all three sections.

Table 18 – Overall Rating Summary

Requirement	Rating = 0	Rating = 3	Rating = 5	Rating = 7	Rating = 9	FINDER Rating	NLETS Rating	ICJIS Rating
R1: Ability to search for data by person	There is no ability to search for data related to a person in the system	There is ability to search for data related to a person by name only.	System possesses the ability to search for data related to a person by name and a specific identifier such as driver's license or social security number.	System possesses the ability to search for data by name, social security number, driver's license, date of birth, gender, and race.	System possesses the ability to search for data by biometric, name, social security number, drivers license, date of birth, gender, and race.	**7**	**7**	**7**
R2: Data Accuracy	The system has no capability to ensure data accuracy.			The system receives data as published by agencies providing data.	The system receives data as published by agencies providing data and periodically performs automatic audits to verify that data matches the agencies' source data.	**7**	**7**	**7**
R3: Data Completeness	The system has no capability to ensure data completeness.		The system operators periodically measure completeness through query operation and communicate completeness to the operators of the source system on key fields.		The system has automatic capabilities to measure completeness and provide feedback to the source systems.	**5**	**5**	**5**
R4: Agency Participation	The system has 0% of the targeted agencies participating participation.	The system has 25% of the targeted agencies participating	The system has 50% of the targeted agencies participating.	The system has 75% of the targeted agencies participating.	The system has 100% of the targeted agencies participating.	**7**	**9**	**5**

Requirement	Rating = 0	Rating = 3	Rating = 5	Rating = 7	Rating = 9	FINDER Rating	NLETS Rating	ICJIS Rating
R5: Person Identification	The system only uses name to identify a person.	The system has an internally generated unique identifier to identify a person.	The system has an internally generated unique identifier to identify a person which is tied to a non-biometric government-issued unique identifier such as a driver's license.	The system has some local biometric capabilities, or leverages AFIS data in addition to having an internally generated unique identifier to identify a person which is tied to a non-biometric government-issued unique identifier such as a driver's license.	The system incorporates a national, biometric unique identifier in addition to all criteria for a rating of 7.	**7**	**7**	**7**
R6: Leverage Decentralized Network Approach	The system is centralized.		The system is a hybrid between centralized and decentralized.		The system is completely decentralized.	**9**	**5**	**5**
R7: Supports Intelligence Analysis Process	The system provides access to no data for use by others in the intelligence community.	The system provides access to person information, and criminal history information	The system provides access to person information, criminal history information, address information, and field investigative report information	The system provides access to person information, criminal history information, field investigative report information, activity at address information, and 9-11 call information, and traffic ticket information.	The system provides access to, criminal history information, field investigative report information, and 9-11 call information, traffic ticket information, and local intelligence products.	**5**	**3**	**3**
R8: Flexibility to Change as Intelligence Analysis Processes Change	The system would need to be re-designed completely to be able to support changing intelligence processes.			The system architecture would need some modification to support changing intelligence processes.	The system architecture needs no modification to support changing intelligence processes.	**9**	**7**	**9**

Requirement	Rating = 0	Rating = 3	Rating = 5	Rating = 7	Rating = 9	FINDER Rating	NLETS Rating	ICJIS Rating
R9: Provides for "tasking"	The system would need to be re-designed completely to be able to support taskings intelligence processes.		The system architecture would need moderate modification to support taskings back to law enforcement.	The system needs minor modification or customization to support taskings back to law enforcement or BOLO's	The system can be configured to support taskings back to law enforcement.	**5**	**0**	**9**
R10: Search by Location	The system does not support search by location		The system contains the data to search by location, but no facilities to query that data.		The system supports search by location, and can bring up related events.	**5**	**9**	**5**
R11: Search by Keyword	The system architecture does not support keyword searching		The system architecture technically supports keyword searching.		The system supports keyword searching for data fields and document narratives	**5**	**5**	**9**
R12: Documentation	The system does not have documentation.		The system has user documentation and some technical documentation.	The system follows a system development methodology which provides for user documentation, design documentation, and technical documentation. Some documentation has been created.	The system follows a documented methodology and all documentation in the methodology has been created.	**5**	**0**	**7**
					Numeric Result:	**76**	**64**	**78**
					Percentage Result:	**70%**	**59%**	**72%**

Will the Markle recommendations be sufficient to support interconnection of regional and state systems like Alabama LETS, Florida FINDER, and Orange County, Florida?

There are several aspects of the SHARE network that support interconnecting the three systems, although at a very high level. Creating a decentralized network is an obvious precursor to interconnection of any regional systems. Likewise, setting specific and clear objectives for improved information sharing which each *federal* agency needs to meet is good, but not sufficient. Although federal agencies are of vital importance in intelligence information sharing, the necessity of including the local and state agencies cannot be overlooked. Because of this, the Markle recommendations, even for the SHARE network, should include encouraging setting specific and clear objectives for improved information sharing between federal, local, state, and private entities. Specific objectives were probably not included in the Markle recommendations to avoid the probable debate about the objectives. It is important that all information sharing participants recognize that setting federal or local intelligence analysis goals alone is not sufficient. All agencies play a role, or roles in a single intelligence analysis process that helps protect our Country.

Are there aspects of Alabama LETS, Florida FINDER, and Orange County, Florida that are not sufficient to accomplish the interoperability and therefore need to change?

With respect to documentation, only the ICJIS project had sufficient process and systems documentation. The Florida Data Sharing project provided only a user guide to review, and the Alabama LETS project provided a case study to examine.

One aspect of all three systems, and the recommendations, which is not sufficient, is that all three have to work-around our lack of a national person identifier. If the benefits of a person identifier are evaluated across all government services (health care, social services, criminal justice, national security), a business case can be made to have one. The issues with respect to privacy and civil liberties will need to be legislated appropriately. The ability to have a person identifier for children is as important to protect the well being of children in domestic violence cases as it is in tracking the activities of people for intelligence information sharing.

The Alabama LETS project and the Florida Data Sharing project are focused on data inquiry. The ICJIS project is focused on real-time data interchange. "Tasking" domestic collection of information (assigning collection to local law enforcement or another collector) is a vital part of any national intelligence information sharing initiative, and only a system that provides capabilities for real-time data interchange and human workflow control will provide the "tasking" capability needed. This will be a challenge to implement, as it impacts the business processes of law enforcement officers on patrol, as well as the packaged record management systems and arrest reporting systems they use every day. Patrol may be asked to respond to national BOLO's for specific targets or persons. They may also be asked to provide additional information about specific incidents if they believe that it may be terrorist-related. This is similar to how patrol must fill out domestic violence checklists when they make a domestic violence arrest.

Only the UCF FINDER project had a stated goal of being a model for information sharing in support of intelligence analysis. The other two systems were not designed with this in mind. UCF FINDER has plans to implement FIRs, however, because of the rules set forth in Code of Federal Regulations CFR 23, part 28, there can be implications to the sharing of the FIR

data even within different departments in an agency, let alone between agencies. This barrier will need to be overcome, since this is an important source of information for intelligence analysis.

What are possible insufficiencies in the Markle recommendations?

The Markle recommendations for the SHARE network are written from a national perspective. As such, they do not really concern themselves with whether regional information systems are interoperable. It is common for different systems to have different definitions for words that appear to be quite simple, such as the word, "arrest." These semantic differences need to be resolved in internal interoperability issues. The use of a national XML standard such as GJXDM can help alleviate this problem.

The recommendations made for DHS are good, however, they do not present the rationale for decentralized centers. The reason for the decentralization of the centers needs to be elaborated on. For example, if the decentralization is simply so that an agency, such as the FBI, can maintain analytical capabilities that may not be relevant in today's environment, that is not necessarily a good reason for decentralization. If the decentralization is to provide redundancy in analytical operations across all agencies, then that is a good reason for decentralization. Reasons for centralization vs. decentralization need to be part of an overall design of our collection and analysis capabilities.

The national recommendations for intelligence information sharing could more strongly support the concept of a national person identifier and legislation to protect our civil liberties. Such a person identifier is needed not only to support integrated information sharing for

intelligence, but also to track child abuse cases, and court cases for specific individuals across civil and criminal courts.

The regional systems that support cross-agency inquiry need to be combined with those that exchange data, so that workflow-oriented requirements such as intelligence analysis can be accomplished. For example, if a patrol officer needs to notify a local intelligence analyst that a victim on a domestic violence incident implicated the defendant as a terrorist, then a workflow process needs to be instituted to make sure that the information is passed on to the local intelligence analyst. Furthermore, if the data needs to be passed to an analyst with a broader perspective, then that handoff also needs to take place.

Most importantly, we need to have an overall model for intelligence analysis that incorporates the capabilities that law enforcement has for collection and analysis in with the federal capabilities for collection and analysis. There is no unified approach today across federal agencies, let alone between federal agencies and local/state agencies. Without this approach, any attempt to 'share' information will be being done from a bottom-up perspective, with sharing being focused on sharing available data elements, not on developing additional data elements necessary for supporting the national intelligence analysis processes.

The regional systems were each designed to solve a particular regional problem. There is a bigger picture to consider. Given the context of an overall model for intelligence information sharing, the regional information sharing models, whether vertical, horizontal, or reporting-oriented can be combined using the overall building block patterns for information sharing to create the desired integration and information sharing solution. This big-picture needs to be kept in mind when designing the intelligence analysis capability, and designing what can be done in a fusion center at each level (e.g. state vs. federal).

Are there any non-technical, human barriers to system development and implementation?

There are still many human barriers to overall system success. Law enforcement still believes in the concept of 'their' data – especially when it comes to intelligence and field investigative reports.

The processes that exist for gathering information relevant to intelligence analysis by law enforcement probably do not exist. Law enforcement's rightful focus is on reacting to specific problems that the citizens of this country and their jurisdiction encounter. This focus needs to be expanded to be able to collect the type of data that intelligence analysts in their agency, and in other agencies subscribing to their collected data (e.g. a federal analyst) need to do their job. Developing the capability for law enforcement to be directed intelligence collectors is appropriate. In addition, it is probably appropriate to suggest that mechanisms be developed for federal agencies to be able to "task" local law enforcement to gather information on specific physical targets or persons.

Alternatives to the SHARE Network

In this section, several alternatives to the Markle Foundation's information sharing network are developed. This is done to create a possible context for overall national intelligence information sharing.

Description of Alternatives

This section describes three alternatives to proceed with implementing information sharing for national security. The first alternative is to directly follow Baird & Barksdale's

(2004, ¶ 5) suggestion to build an information-sharing network based on keyword searches[25]. The second alternative is to put in place a mechanism to build a real-time dynamic model that represents our understanding of terrorist networks and the linkages between them. As either local analysts provided by local law enforcement, or national intelligence analysts detect the links, they would enter them into the overall dynamic model. The third alternative is to add the concept of knowledge management to the concept of data sharing. This section describes each alternative in more detail.

Watch List Sharing

The first alternative is to follow Baird & Barksdales' recommendations, but focus the information-sharing network on a data type that has a high probability of yielding short-term success and doesn't require extensive consensus building between agencies. The terrorist 'watch lists' are probably the best candidate for initial information sharing.

Real-Time Terrorist Network Monitor

The next alternative is to use the information-sharing network to build a real-time terrorist network monitor. This monitor would be built using both person information, and field investigative report information. The data facts, combined with the history of queries by investigators and analysts would be used to build a big-picture for decision makers. This could be referred to as a real-time terrorist network monitor.

[25] According to Vest, 2005, many police agencies do not have their records automated so that they are searchable. A 'readiness' assessment needs to be performed to survey the roughly 18,000 agencies involved to determine if they even have searchable records. If not, national grants may need to be directed to automate agencies with deficient systems if they are located in an area likely to learn information relevant to the national intelligence sharing initiatives.

Farley (2003, p. 404) discusses mathematical theory as it can be applied to probabilities of breaking up terrorist cells. His research indicates that terrorist networks, such as Al Qaeda, are organized somewhat hierarchically. Schultz & Margolies (2004, p. 69) describe how al-Qaeda is organized vertically with a "loose horizontal structure of compartmentalized cells." This enables their management to accomplish missions even when cells are partially crippled by combining or redeploying cells rapidly. Note that this is different than organized crime networks that are typically hierarchical. According to Gunaratna (2004, p. 93), although Al Qaeda's strength has been greatly diminished, it has been "instilling its mission and vision in associated groups and transferring its capabilities to them." It is probably a good assumption that their tactics and organization will model those of Al Qaeda, so our detection capabilities need to be able to track meaningful information about this type of organization.

So to create an efficient near-term information-sharing tactical plan, we need to bring together information about terrorist watch lists, mathematical concepts to model the terrorist networks, and our knowledge of Al Qaeda-like terrorist networks. This should provide a solid framework for framing a cohesive information sharing initiative that supports human detection and hindrance of terrorist efforts. Figure 2 presents a highly simplified view of what this might look like. In this view, information from the Department of Agriculture is assumed to be available even though there is no current legislation providing this capability[26].

[26] When data is needed for intelligence analysis (e.g. agriculture, person id) that is not available because of federal regulation, or local laws, the benefits of having the data available vs. the privacy concerns need to be addressed, and perhaps new or modified legislation needs to be proposed.

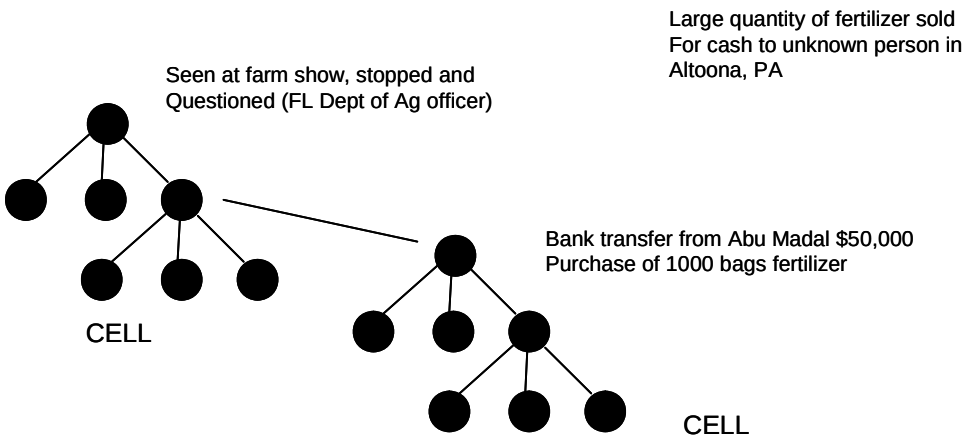


Figure 8 – Terrorist Network Monitor

The central core of this information sharing mechanism would be a computer program that would take information about specific terrorist node connections and aggregate it in real-time to one or more central authorities terrorist network monitors. The information would be stored as a data structure called ordered sets[27], with attributes of an off-the-shelf customer relationship management system that tracks details of each encounter with a customer. Each agency participating in the information sharing effort could determine what level of information would be shared. Additional features, such as contact history with each of the nodes could also be stored in effect creating a shared, dynamic 'terrorist information management system focused on terrorist nodes. Activity in the nodes could determine the keywords that would drive queries into the broader information-sharing network. The example in the figure would use the word, "fertilizer" In effect, instead of agents and analysts tracking data by case, they would track it by node and topic.

---

[27] According to Farley (2003), "A common way to represent visually a group of people and the relationships between them is by means of a *graph* or *network*." This is similar to how organized crime networks are modeled. Farley (2003) also states that "A graph inadequately represents a terrorist cell, however, because it fails to capture the fact that, in any cell, there will most likely be a hierarchy – leaders and followers – with orders passed down

Terrorist Threat Knowledge Management

Terrorist activities are comprised of a series of interrelated subsystems that individually and collectively create a threat to United States public safety. We seek to obtain knowledge about future terrorist activities by looking at vast quantities of intelligence data. In business, this process is known as knowledge management. "The problems of decision making in complex dynamic environments have also been examined by others, for example by Sterman (1989, 1994), whose key finding was that human performance in complex systems is poor relative to normative standards." (as cited in Yim, Kim, Kim, & Kwahk, 2004, p. 144). For data sharing to be successful, we need to consider how it will be used to further the overall goal of knowledge management. In addition, "the process of knowing, learning, and creating knowledge is the relevant aspect. This fact candidates them as milestones for CSCW[28] research, since they offer new conceptual categories for deepening our understanding of the intimate nature of cooperation, and challenge us to develop systems supporting cooperation beyond the surface of synchronous and/or asynchronous interaction." (Agostini, Albolino, Boselli, De Michelis, De Paoli, & Dondi, 2003, p. 248)

Where the terrorist network monitor is focused on providing the big picture to central authorities, the knowledge management solution allows local law enforcement to leverage the big picture, without needing to explicitly know what is on the big picture.

Using knowledge management techniques as guiding principles, we could extend the real-time terrorist network monitor to be able to learn from the collective experiences of the

---

from leaders to followers." This observation can also be applied to relationships between terrorist cells which serve other specialized functions such as supply, or implementation, and who are organized in a loose hierarchy.

[28] CSCW refers to Computer-Supported Cooperative Work.

intelligence community, the law enforcement community and other sources. This support for long-distance cooperation could make it possible for law enforcement agencies to become aware that others are recording incidents similar to theirs that fit a particular incident profile, and ultimately bring this to the attention to the JTTF's or to other intelligence community management.[29] For example, it would be useful to a law enforcement officer who is doing an investigation on stolen propane tanks to become aware of similar activities within a certain time span in another geography, particularly if that geography was recently frequented by a known terrorist cell member or members. This technique would achieve a knowledge-sharing goal without the hierarchical organizational filtering that has the potential to screen out patterns that need to be seen. The danger in hierarchical analysis processes is that information viewed in isolation seems irrelevant, but when viewed in a broader context becomes vital.

In this way, we would leverage knowledge of similar queries taking place that meet criterion for close distance, time, or tactic and gain overall knowledge of what is actually happening and combine this with knowledge of the political, social and economic factors likely to cause large-scale change in a region.

Comparison of Future Consequences

The three alternatives were listed from least complicated to most complicated. This section describe future consequences of each alternative in turn.

---

[29] This is a fundamentally different approach than the 'share and tear' lines referred to in the Markle report. Information on the share line could be shared. Information on the tear line wouldn't. The 'share and tear' lines represent automation of a manual process that is probably not the best process to solve the knowledge management problem.

Watch List Sharing

Our reference model for data sharing, the Florida data-sharing network was created initially to share pawn data. This was a particularly good choice since Florida State Statute 539.01(8) specifies the data fields that must be reported. As the data-sharing network expands into different types of data, building consensus on the semantic meaning of data fields being shared becomes more important. It is common, especially with packaged software products, for fields to be used differently in the database than they are on the screens that users see. For example, a database field may be named "drivers license", however, the computer programmers writing the program may store both passport numbers and drivers license numbers in that field, or they may embed special codes in the field that only a computer program can decipher. Unfortunately, this is a common occurrence in legacy information systems.

Watch list data sharing will suffer from some of these challenges. The General Accounting Office examined the 12 watch list systems in detail and found that there were many different types of information in the watch lists including biographic, criminal history, biometric, immigration, and financial data. *Name* and *birth date* were the only fields shared across all of the systems reviewed. (GAO, 2003, p. 16)

A further characteristic of this type of data sharing is its scalability. As the number of agencies' systems being queried increases, the speed of individual responses will be reduced. This solution gives analysts the ability to look at watch list data across agencies, but it does not provide us with the means to see patterns across agencies, or to learn when multiple investigators or analysts in different agencies are looking at similar people for related reasons. For that, we need to use a different model to frame our information sharing activities.

Terrorist Network Monitor

The terrorist network monitor concept depends on defining an overall reference model for the structure of terrorist networks, of the relationships between the actors in the networks, and what events are desired or possible to monitor. A hierarchical graph or network has been applicable to law enforcement efforts about organized crime for many years, so the knowledge of that particular way of working within the law enforcement community will require some un-learning for the new concept to be understood and accepted.

Knowledge Management

The knowledge management solution will require the most investigation by system designers into processes within the DOD, FBI, CIA, and other participants in the Intelligence Community. It will also draw on advanced techniques for information and process management, storage and retrieval. Pursuing this alternative will require strong leadership and patience.

Spillovers and externalities

Short-term information sharing initiatives can have a great benefit as long as they are successful. If, for some reason, the early efforts do not provide a success, then it has the possibility to derail future information sharing efforts. The human resistance goes up exponentially when an information-sharing initiative fails. Thus, the steps taken in information sharing need to be planned to provide benefits to stakeholders at each step along the way.

Constraints and Political Feasibility

The three alternatives have different constraints and political feasibility as described in this section.

Information Sharing

The basic information-sharing concept is the most palatable from a political perspective. Agencies are naturally anti-change, and any approach, which claims to work without any changes to the agencies' data systems, is likely to gain immediate acceptance without political fallout. The Markle foundation's recommendations will work as long as the data that is being shared is easily understood and defined. As the data that needs to be shared becomes more like knowledge, and less like facts, the willingness to share the data, and the ease with which the data can be shared will be reduced.

The Terrorist network monitor

The terrorist network monitor is also politically acceptable. It also minimizes the change to the agencies' operations. Its main purpose is to put an overall representation of the terrorist network into place for decision-makers, and to allow local law enforcement and other participants in the intelligence community to share analysis. One constraint will be that in any automated system; its value is only as good as the data put into it in the first place. Again, as the data being shared is more complex, the more the people gathering the data will need to be trained to contribute to it 'properly.' The people entering the information need to be trained to enter it effectively and consistently.

Knowledge Management

The knowledge management solution requires the most work politically. It is an interesting concept that could be grown incrementally. As the cooperating agencies got better at sharing analysts, and integrating their disciplines, the value of the knowledge management solution would grow. It would initially face political challenges, as agencies would not want to cooperate to share highly developed analysis.

The next section of this paper describes how these policy alternatives can be combined into a cohesive recommendation.

CHAPTER 5: CONCLUSIONS

Since the three alternatives are capable of being implemented in a stepwise manner, it isn't necessary to select between them if sufficient funding and resources are available for their implementation; however, the order in which they can be implemented is restricted.

Criteria for recommending alternatives

The three alternatives were reviewed and ranked for their ability to produce results in a relatively short amount of time, without requiring a large amount of consensus building. Successful results will lead to more cooperation for the more complex information-sharing alternatives. Unsuccessful results lead to non-cooperation and long-term project failure.

Description of preferred alternative(s)

The recommendation for policy implementation is to proceed in a stepwise manner through the three recommendations. Initially, creating the capability for law enforcement and intelligence agencies to search their collective watch lists for suspected terrorists would be beneficial to all stakeholders. In getting all of the organizations in the IC to work together, it will be best to prove that information sharing, on any scale, will lead to better defense against terrorists.

Once the initial watch list capability exists, the next step of building the terrorist network monitor could be taken. This would require expanding the initial data sharing initiative to several types of reports (FIR's, arrest reports) as well as people (watch lists). Finally, the knowledge management solution could build on both of the first two alternatives.

Outline of Implementation Strategy

Figure 3 shows the high-level phases that could guide an implementation strategy. The watch list sharing, and IC process analysis begin simultaneously. The watch list sharing will produce results. The results from the watch list sharing can drive implementation of a terrorist network monitor. This will provide input to the knowledge management solution. As data types are added to the information-sharing network, it can further enhance the terrorist network monitor.

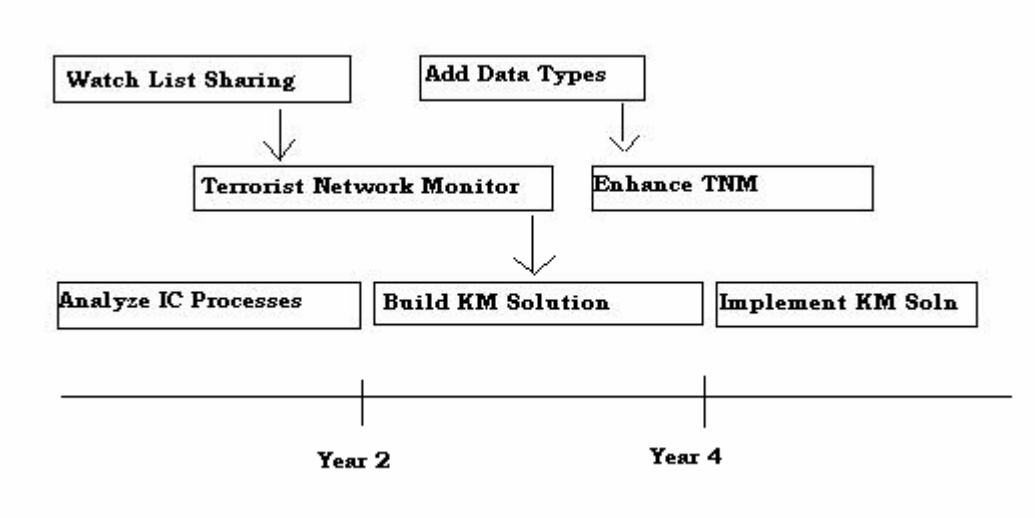


Figure 9 – High-level Implementation Strategy

Critical to the knowledge management solution is to document the specific means by which intelligence is collected, filtered, and deemed to be important. There may need to be some modifications to law enforcement procedures and training to accommodate the needed level of data and knowledge sharing, in effect, allowing them to tag something as other than 'locally' suspicious.

Finally, the terrorist threat knowledge management solution could be implemented. This would build on previous two recommendations and allow local law enforcement to act within the

framework of the big picture without actually seeing it. For example, they could run parameters of something they deemed to be suspicious (people walking by railroad yards) and the knowledge management solution would return a yes/no flag to tell the law enforcement officer to notify the JTTF or to proceed as usual. Essentially, the JTTF's could create event watch lists that would trigger when local law enforcement officers recorded one of those events.

Provisions for Monitoring and evaluation

Watch list sharing can be measured by building in the capability to count 'hits' when any user queries the information-sharing network. While this is a summary measure, it will provide the ability to track the quantity of usage, and usage that led to a successful query response.

The terrorist network monitor should also be able to be measured. As relationships between nodes on the network are created or destroyed, they can be counted. The numbers of known active cells, and the numbers and types of cells in a particular geography or sociopolitical sphere can be measured. Events averted and occurred can be counted. As events occur, they can be matched against the contents of the network to help discover new relationships between nodes in the network. A model of the network monitor can also be created and exercised by seeding it with fictitious data to see if the users of the system are able to predict events. This is the "red vs. blue" team mentioned earlier in this paper. This concept would work with the terrorist network monitor. The knowledge management solution can be evaluated the same way.

Limitations and unanticipated consequences

Information systems are limited by data quality, and limited by the people who know the data and how to 'enter' the data. The effects of poor report writers will have a great impact on the overall systems. If an officer writes a report that says, "Observed non-uniformed personnel in the subway doing something with the switching equipment" vs. one that says "Observed non-

uniformed personnel in the subway placing a small electronic device on the switching equipment and apprehended suspect. Suspect appeared to be of middle-eastern descent and was carrying an expired Egyptian visa" it is likely that one report will provide good information, and the other won't.

LIST OF REFERENCES

9-11 Commission Web Site (2004, August 21). Retrieved December 4, 2004, from http://www.9-11commission.gov/

9-11 Commission. (2004, August 21). *Final Report of the National Commission on Terrorist Attacks Upon the United States, Official Government Edition.* Retrieved December 4, 2004, from http://www.gpoaccess.gov/911/

9-11 Commission Staff Statement 12: Reforming Law Enforcement, Counterterrorism, and Intelligence Collection in the United States. (n.d.). Retrieved December 4, 2004, from http://www.9-11commission.gov/staff_statements/staff_statement_12.pdf

ACLU. (December 3, 2004). Remove National ID Provisions From S. 2845 & HR 10 Now. Retrieved March 31, 2005, from http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=17147&c=206

Adams. (1995). Bar Code History Page. Retrieved June 26, 2005, from http://www.adams1.com/pub/russadam/history.html

Agostini, A., Albolino, S., Boselli, R., De Michelis, G., De Paoli, F., & Dondi, R. (2003). Stimulating Knowledge Discovery and Sharing. Association for Computing Machinery Group 3 Conference Proceedings. 248-257. Retrieved November 29, 2004, from ACM Digital Library Database.

Baird, Zoe , & Barksdale, James. (2004, August 16). There is Security in Sharing: Information Would Aid Terror Fight. *San Jose Mercury News.* Retrieved November 28, 2004 from http://www.markle.org/downloadable_assets/mercury_news_op_ed_8.16.04.pdf

Baird, Zoe, & Barksdale, James (2004, August 31). *Letter to Senators Collins, Hollings, Lieberman and McCain.* Retrieved December 4, 2004, from http://www.markle.org/downloadable_assets/response_exec_orders_83104.pdf

Barger, Deborah G. (2005). Toward a Revolution in Intelligence Affairs. RAND Corporation. Retrieved June 26, 2005, from http://www.rand.org/publications/TR/TR242/

Carter, David. (2004). Office of Community Oriented Policing Services, U.S. Department of Justice Law Enforcement Intelligence Guide. Retrieved March 15, 2005, from http://www.cops.usdoj.gov/default.asp?Item=1404

Carter, Ashton B. (2002). The Architecture of Government in the Face of Terrorism. *International Security*. *26(3),* 5-23. Retrieved November 14, 2004, from PAIS International Database (2003-0503520).

Chabrow, Eric. (May 19, 2004). Effort to Build Enterprise Architecture at DoD Languishing – Report. *Information Week.* Retrieved December 3, 2004, from http://informationweek.com/story/showArticle.jhtml;jsessionid=Y4QVTPQSPVRJAQSNDBCCKHSCJUMEKJVN?articleID=20800064

Clark, Drew. (March 17, 2003). Intelligence Reorganization spotlights fabled FBI-CIA rift. GovExec.com. Retrieved December 3, 2004, from http://www.govexec.com/dailyfed/0303/031703cdam1.htm

Clark, Robert M. (2004). Intelligence Analysis: A target-centric approach. CQ Press, 2004.

Department of Justice. *28 CFR Part 23 – Guideline*. Retrieved February 13, 2005, from http://www.iir.com/28cfr/guideline1.htm

Department of Justice. *28 CFR Part 23 – Policy Clarification.* Retrieved February 13, 2005, from http://www.iir.com/Publications/28cfr23-clarification.htm

Department of Justice. Regional Information System Sharing Grants. Retrieved February 13, 2005 from http://assembler.law.cornell.edu/uscode/html/uscode42/usc_sec_42_00003796---h000-.html

DeRosa, Mary, & Lewis, James. (December 2003). Appendix B: A Primer on Homeland Security Players and Information. *Creating a Trusted Information Network for Homeland Security.* Retrieved March 15, 2005, from http://www.markle.org/downloadable_assets/nstf_report2_part_three.pdf

Eaglin, Ron, Flint, Michael, Reynolds, Michael. (2002). Establishing the Connectivity Infrastructure for the Central Florida Law Enforcement Data Sharing Consortium. Retrieved June 25, 2005, from http://druid.engr.ucf.edu/datasharing/programplan.html

FACC. (2003). Comprehensive Case Management System. Retrieved June 26, 2006, from http://www.flclerks.com/program.htm

Farley, Jonathan D. (2003). Breaking Al Qaeda Cells: A Mathematical Analysis of Counterterrorism Operations (A Guide for Risk Assessment and Decision Making). *Studies in Conflict and Terrorism*, 26(3). 399-411. Retrieved on 11/28/2004 from EBSCO Host Database.

FDLE. (2001). Assessing Florida's Anti-Terrorism Capabilities. Retrieved March 13, 2005, from http://www.fdle.state.fl.us/publications/anti-terrorism.pdf

Federation for American Immigration Reform. (January 27, 2005). Legislation Includes Immigration Reforms Recommended by 9/11 Commission Omitted from the Intelligence Reform Billz. Retrieved March 31, 2005, from http://www.fairus.org/news/NewsPrint.cfm?ID=2612&c=34

Fleishman, Joel (March 6, 2002). New Task Force Aims to Protect Nation With Better Information and Technology. Retrieved June 26, 2005, from http://www.markle.org/resources/press_center/press_releases/2002/press_release_03062002.php

General Accounting Office (GAO). (2003). Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing. GAO-03-322. Retrieved December 4, 2004, from http://www.gao.gov/new.items/d03322.pdf

Government Computer News. (2003, November 10). Alabama Links Data to Nab Bad Guys. Retrieved March 19, 2005, from http://www.gcn.com/22_32/statelocal/24077-1.html

Grabo, Cynthia M. (2004). Anticipating Surprise: Analysis for Strategic Warning. Lanham, MD. University Press of America.

Global Justice Information Sharing Initiative. (2003). Retrieved March 31, 2005, from http://it.ojp.gov/documents/ISWG-SOASMeetingSummary11-03.pdf

Greenemeier, Larry. (June 6, 2005). Tech vs. Terrorism. *Information Week.*, 1042*:* 37-46.

Harris, James W. (2002, May 16). Building Leverage in the Long War Ensuring Intelligence Community Creativity in the Fight Against Terrorism. Cato Institute. *Policy Analysis*. 1-14. Retrieved March 15, 2005, from http://www.cato.org/pub_display.php?pub_id=1298

Hollywood, John, Snyder, Diane, McKay, Kenneth, Boon, John. (2004). Out of the Ordinary: Finding Hidden Threats by Analyzing Unusual Behavior. RAND Corporation. Retrieved July 10, 2005, from http://www.rand.org/pubs/monographs/2004/RAND_MG126.pdf

IJIS Institute. (2004). *Integrated Justice Models.* Retrieved March 12, 2005, from http://www.icjia.state.il.us/IIJIS/public/word/TCH2/IJNmodels.doc

Intelligence Reform and Terrorism Prevention Act of 2004. Retrieved June 25, 2005, from http://www.senate.gov/~govt-aff/_files/IntelligenceReformconferencereportlegislativelanguage12704.pdf .

Lahneman, William J. (2003). Outsourcing the IC's Stovepipes?, *International Journal of Intelligence and CounterIntelligence*, 16: 573-593.

Kenney, Michael C. (2003). Intelligence Games: Comparing the Intelligence Capabilities of Law Enforcement Agencies and Drug Trafficking Enterprises, *International Journal of Intelligence and CounterIntelligence*, 16, 212-243.

Ross, Margy. (2003). To Be Or Not To Be Centralized, *Intelligent Enterprise.* Retrieved July 10, 2005 from http://www.intelligententerprise.com/030201/603warehouse1_1.jhtml?_requestid=166065

Markle Task Force., December, 2003, Creating a Trusted Information Network for Homeland Security, Retrieved June 25, 2005, from http://www.markle.org/downloadable_assets/nstf_report2_full_report.pdf

Microsoft, March 27, 2001. *Microsoft Helps Turn Britain's E-Government Vision Into Reality*. Retrieved July 10, 2005 from http://www.microsoft.com/presspass/press/2001/mar01/03-27britainpr.mspx

Microsoft, September 1, 2003, *State of Alabama: Alabama's LETS Portal Allows More Justice and Police Users to Get Information Faster"*. Retrieved March 19, 2005, from http://www.microsoft.com/resources/casestudies/CaseStudy.asp?casestudyid=15104&PF=yes

MSDN. (2003). Developing Service-Oriented Architectures. Retrieved March 31, 2005, from http://msdn.microsoft.com/architecture/application/default.aspx?pull=/library/en-us/dnvsent/html/FoodMovers3.asp#foodmovers3_topic2.

MSDN. (2004). Understanding Service-Oriented Architecture. Retrieved March 31, 2005, from http://msdn.microsoft.com/architecture/soa/default.aspx?pull=/library/en-us/dnmaj/html/aj1soa.asp.

Miller, Jason, June 21, 2004, After a Quick start, directorates prepare for the nitty gritty of IT consolidation and integration, Government Computer News, v 23, p. 44)

Menke, Susan M., November 8, 2004, Counterterror data sharing will rely on XML, Government Computer News. Retrieved November 11, 2004, from http://www.gcn.com/vol1_no1/homeland-security/27854-1.html

NGA.ORG. (2003). *Data Integration Problem*, Retrieved March 30, 2005, from http://www.nga.org/cda/files/1203JITPRITCHETT.ppt

NLETS. (2003). *Home Page*. Retrieved June 26, 2005 from http://www.nlets.org/general.html

Pinal County. (2003). *Pinal County Justice Integrated Systems (PCJIS).* Retrieved June 25, 2005, from http://co.pinal.az.us/IT/PCJIS/

PIU. (2002). *Privacy and Data Sharing.* Retrieved July 9, 2005 from http://www.number-10.gov.uk/su/privacy/downloads/piu-data.pdf

Real ID Act of 2005. H.R. 418.RFS. Retrieved June 26, 2005, from World Wide Web. http://thomas.loc.gov/cgi-bin/query/D?c109:3:./temp/~c109jhfOEB::

Schultz, Richard H. & Beitler, Ruth M. (2004), Tactical Deception and Strategic Surprise in Al-Qai'da's Operations. *Middle East Review of International Affairs*. 8(2), p. 56-79.

Solomon, Melissa. (2004), Improving the Odds. *StateTech*. Retrieved March 31, 2005,from http://statetech.texterity.com/archives/200407/.

Stonebraker, Michael. (1999). *Integrating Islands of Information.* EAI Journal. Retrieved July 10, 2005 from http://www.bijonline.com/PDF/stonebraker_1.pdf

Travers, Russ. (1997). A Blueprint For Survival: The Coming Intelligence Failure. Retrieved March 31, 2005, from http://www.cia.gov/csi/studies/97unclass/failure.html.

University of Central Florida. (2003). *Establishing the Connectivity Infrastructure for the Central Florida Law Enforcement Data Sharing Consortium*. Retrieved June 25, 2005, from http://druid.engr.ucf.edu/datasharing/programplan.html

U.S. Department of Justice. (2004). *Global Justice XML Data Model.* Retrieved March 31, 2005, from http://it.ojp.gov/jxdm/.

U.S. Senate. (2004). *9-11 Implementation Act Guide to Legislative Provisions.* Retrieved March 31, 2005, from http://govt-aff.senate.gov/_files/090704guide.pdf

Vest, Gary, June 2005. *Ohio Local Law Enforcement Information Sharing Network: Policy Issues in Data Exchange.* Retrieved July 9, 2005 from http://policechiefmagazine.org/magazine/index.cfm?fuseaction=display&article_id=612&issue_id=62005.

Wang, Li. (2004) Success Stories. Retrieved March 31, 2005, from http://druid.engr.ucf.edu/datasharing/SuccessStories.htm

Wermouth, Michael A., January 2005. Testimony presented to the Senate Committee on Homeland Security and Governmental Affairs on January 26, 2005. The RAND Corporation.

White House. August 27, 2004. *Executive Order Counterterrorism Center*. Retrieved June 26, 2005, from http://www.whitehouse.gov/news/releases/2004/08/20040827-5.html

Yim, Nam-Hong, Kim, Soung-Hie, Kim, Hee-Woong, Kwahk, Kee-Young, 2004, Knowledge Based Decision Making on Higher Level Strategic Concerns: System Dynamics Approach, *Expert Systems with Applications*, 27(1), 143-158