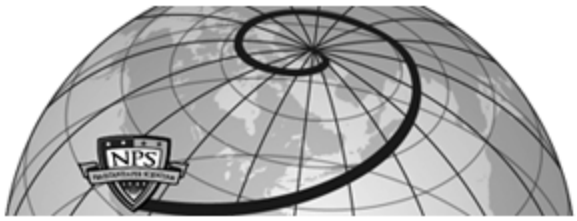

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

ARIZONA LAW ENFORCEMENT BIOMETRICS IDENTIFICATION AND INFORMATION SHARING TECHNOLOGY FRAMEWORK

by

William M. Kalaf

March 2010

Thesis Advisors: Richard Bergin
Robert Josefek

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2010	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Arizona Law Enforcement Biometrics Identification and Information Sharing Technology Framework		**5. FUNDING NUMBERS**	
6. AUTHOR(S) William M. Kalaf			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

Since 9/11, Arizona and federal law enforcement agencies understand the need to improve subject identification capabilities and integrate criminal information across jurisdictions. Agencies still collect information based on a subject's name and demographics for identification. Using a subject's name and demographics as keys to identifying information is a weakness. In 2012, Arizona will upgrade the state's strategic plan to allow law enforcement officers to use biometrics technology to verify a subjects' identity at first point of contact and implement information sharing capability across the state, border states, and federal agencies.

This thesis presents a technology framework for strategic planning that includes biometrics identification technology, information sharing capability, and a governance structure for oversight. Through researching implementations in Los Angeles County, California and the states Minnesota, Wisconsin, and Vermont a comparative analysis revealed similarities in each implementation that will be used in developing an Arizona technology framework.

Biometrics identification and information sharing is critical for supporting security along the U.S. border with Mexico. This thesis addresses expansion of the technology framework to align with the FBI's Repository for Individuals of Special Concern, initiatives to gain access to identification information from Central American countries and programs developed during the border governors' conferences with Mexico.

14. SUBJECT TERMS Arizona Criminal Justice Commission, biometrics technology, biometrics identification, facial recognition, fingerprint identification, law enforcement, information sharing, criminal information sharing, Arizona, Mexico, New Mexico, Texas, California, RISC, AFIS, IAFIS, NGI, governors border conferences, Central America, south west border initiative.	**15. NUMBER OF PAGES** 113
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

ARIZONA LAW ENFORCEMENT BIOMETRICS IDENTIFICATION AND INFORMATION SHARING TECHNOLOGY FRAMEWORK

William M. Kalaf
Program Manager, Arizona Criminal Justice Commission
B.S., Arizona State University, 1984

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
March 2010

Author: William M. Kalaf

Approved by: Richard Bergin
Thesis Co-advisor

Robert Josefek
Thesis Co-advisor

Harold A. Trinkunas, PhD
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Since 9/11, Arizona and federal law enforcement agencies understand the need to improve subject identification capabilities and integrate criminal information across jurisdictions. Agencies still collect information based on a subject's name and demographics for identification. Using a subject's name and demographics as keys to identifying information is a weakness. In 2012, Arizona will upgrade the state's strategic plan to allow law enforcement officers to use biometrics technology to verify a subjects' identity at first point of contact and implement information sharing capability across the state, border states, and federal agencies.

This thesis presents a technology framework for strategic planning that includes biometrics identification technology, information sharing capability, and a governance structure for oversight. Through researching implementations in Los Angeles County, California and the states Minnesota, Wisconsin, and Vermont a comparative analysis revealed similarities in each implementation that will be used in developing an Arizona technology framework.

Biometrics identification and information sharing is critical for supporting security along the U.S. border with Mexico. This thesis addresses expansion of the technology framework to align with the FBI's Repository for Individuals of Special Concern, initiatives to gain access to identification information from Central American countries and programs developed during the border governors' conferences with Mexico.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

10-Print	Ten fingerprint identification
2-FID	Two fingerprint identification
3D	Three Dimensional
ACJC	Arizona Criminal Justice Commission
AFIS	Automated Fingerprint Identification System
BCA	Minnesota Bureau of Criminal Apprehension
BioID	Minnesota's Identification Workflow Manager System
CAL-ID	California's Department of Justice State Biometrics Identification System
CIB	Crime Information Bureau
CID	County Subject Identifier
CJJIPC	Minnesota Criminal and Juvenile Justice Information Policy Group
CJJITF	Minnesota Criminal and Juvenile Justice Information Task Force
CJSIIP	Hennepin County's Criminal Justice System Information Integration Project
DLES	Wisconsin Division of Law Enforcement Services
DOJ	Department of Justice
DUI	Driving under the influence
EDL	Enhanced Driver Licensee
EPIC	Electronic Privacy Information Center
FAST ID	Wisconsin's biometrics mobile identification fingerprint system
FBI	Federal Bureau of Investigation
FBIID	FBI identification number
GID	Minnesota Global Identification Service Identifier
HJIP	Hennepin Justice Integration Program
IAFIS	FBI's Integrated Automated Fingerprint Identification System
ICE	Iris Challenge Evaluation
IRIS	Los Angeles County's Incident Reporting Information System
LACRIS	Los Angeles County's Regional Identification System
LAPD	Los Angeles Police Department
LASD	Los Angeles County Sherriff's Department

LEDSI	Vermont's Law Enforcement Data Information Sharing Initiative
LID	Local Person Identifier
MNCIS	Minnesota's Court Information System
MNJIS	Minnesota's Justice Information Services
MOU	Memorandums of Understanding
MRAP	Minnesota's Repository for Arrest Photos system
NCID	Non-Criminal Subject Identifier
NEIS	Minnesota's Name Event Index Service System
NGA	National Governors Association
NGI	FBI Next Generation Identification
NIST	National Institute of Standards and Technology
PDA	Personal Digital Assistant
PIA	Privacy Impact Assessment
RAN	Los Angeles County Remote Access Network Board
RFID	Radio Frequency Identification Chip
RISC	FBI Repository for Individuals of Special Concern
RTIIS	Los Angeles County's Regional Terrorism Information and Integration System
SAFE	Minnesota's Subject and File Enhancement System
SEARCH	National Consortium for Justice Information and Statistics
SFID	State Facial Identifier
SID	State Subject Identifier
SILS	Hennepin County Subject Identification and Locator Service
SILS-ID	Hennepin County Subject Identification and Locator Service Subject Identifier
TIME	Wisconsin's Transaction Information for Management of Enforcement System
VIP	Verify Identify Pyramid
VJISS	Vermont's Justice Information Sharing System
WDOJ	Wisconsin Department of Justice

ACKNOWLEDGMENTS

I want to express my heartfelt gratitude to my wife. Thank you, Barbara, for your support and believing in me and keeping me motivated for success. I appreciate the late nights spent reviewing papers even though you have your job activities that needed to be completed every evening.

I would like to thank my co-advisors, Richard Bergin and Robert Josefek, for their guidance and support. Their response to my efforts and our conference calls will remain with me forever. Keeping me focused on the topic and my proposal gave me momentum to complete my thesis on time.

I would also like to thank my fellow law enforcement partners for their documents and contributions to this thesis: Jerry Olson, Minnesota Bureau of Criminal Apprehension; Leila Tite, Hennepin County Sheriff's Office, Minnesota; Chris Cahhal and Leo Norton, Los Angeles County Sheriff's Department California; Phil Collins and Curt Bauer, Wisconsin Department of Justice; Francis (Paco) X. Aumand III, Division of Criminal Justice Services, Vermont Department of Public Safety; David Jones, Fred Jaco, Chad Rhoades, Gerg Voreh, and David Roth, Federal Bureau of Investigation, Criminal Justice Information Services Division, Next Generation Program; and Robert Fund, I2 Technologies. Their time and commitment to me and my thesis is greatly appreciated.

I would also like to thank John Blackburn Jr., the Director of the Arizona Criminal Justice Commission for his support, patience and latitude in allowing me to participate in this educational endeavor.

Finally I would like to thank my fellow students and the faculty and staff of the Naval Postgraduate School for your commitment and support during this academic journey as well as the personal growth and support you have all provided.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

1. Status Quo

Law enforcement agencies are the United States' front line of defense for protecting citizens against terrorism and crime. Officers make contact with the public every day, analyzing situations and gathering subject information. The common practice for officers is to collect information based on a subject's name and demographic characteristics such as age, height, weight, hair color, eye color, and any physical body markings. Using a subject's name and demographics as keys to identifying information is a weakness for automating information sharing. A name can be recorded and spelled many different ways and demographic information, such as age, height, and weight are subject to change over time.

Law enforcement agencies primarily rely on state drivers' licenses to verify subjects' identities. However, drivers' licenses can be forged and hard to verify across state lines. In many cases, officers rely on other forms of identification where the subjects' name may vary or in the worst case, officers rely on the subjects' verbal information. In addition, using subjects' demographic characteristics is subject to interpretation by an officer and varies each time a subject has been contacted.

Historical records are hard to change. A subject can legally change a name and no action is taken to change any information stored in law enforcement record systems. Also, when a subject is booked into jail, a fingerprint identification check against both the state and Federal Bureau of Investigation (FBI) identification systems may reveal a different name. Going back and correcting the initial information captured by the law enforcement agency may not occur.

Even with the advancements in using automation to store information, agencies still use the same subject identification techniques. Law enforcement agencies rely on

manual efforts such as phone calls and faxed pictures to make positive identification. In addition, courts, prosecutors and other criminal justice agencies follow the same process as law enforcement agencies to verify subject information.

In 2004, there were more than 17,000 law enforcement agencies with greater than 800,000 full-time sworn law enforcement officers in the United States (National Law, n.d.). Technology exists today that will provide law enforcement agencies global access to very detailed information in a secured environment. Massive amounts of information will be made available that will cross technology boundaries. Nevertheless, without a common standard for subject identification, law enforcement agencies will be forced to rely on the same manual techniques they use today.

2. Problem Statement

Information sharing is expanding in Arizona. Nevertheless, a technology framework for implementing identification technology, information sharing, and alignment[1] with federal, state, and local law enforcement systems have not been addressed. Further work needs to be done in these areas in order to improve information sharing and law enforcement decision making.

B. RESEARCH QUESTION

How does Arizona develop a technology framework that aligns with federal, state, and local law enforcement identification systems in order to improve decision making and support information sharing?

C. ARGUMENT: MAIN CLAIMS, WARRANTS, EVIDENCE AND CHALLENGES

The Arizona Strategic Plan identified the need to improve subject identification, implement an information sharing environment, and align with state, local and federal law enforcement agencies (ACJC, 2008). Agencies have started initiatives for evaluating

[1] For purposes of this thesis, alignment is defined as subject identification and law enforcement information sharing.

identification technologies independently of any information sharing plan. For example, the AZLink program provides tools used by Arizona law enforcement to share information. The program is being implemented without considering the expansion of biometric identification technology. The complexity of the systems and the introduction of new technologies involved will create waste and make rework inevitable without a technology framework for integration.

1. Arizona Identification Technologies

Two identification technologies are becoming the standard within Arizona, the two-fingerprint system (2-FID) being implemented by the Department of Public Safety and the facial recognition system being implemented by the Arizona Counter Terrorism Information Center. Each system is being evaluated independently with no consideration for integrating subject identification capabilities and storing accurate subject information within law enforcement records. A possible solution for Arizona is to create a multi-modal identification capability for each subject record as part of the *Arizona Strategic Plan.* In addition, the multi-modal systems will be expanded to use mobile wireless identification technologies by officers in the field. The challenge is to implement multi-modal identification capability into disparate local law enforcement record management systems and the central identification database maintained by the Department of Public Safety.

2. Arizona Information Sharing

The AZLink program provides the next step as part of the technology framework. The program's objective is to provide information sharing across disparate systems. The program depends on the information provide by local law enforcement record management systems. The challenge will be to upgrade the AZLink system to take advantage of multi-modal biometric identification technology provided by the local agencies.

3. Arizona Law Enforcement Information Systems Governance

A governance team that includes state, local, and federal agencies will need to be established to provide oversight and direction to both the Arizona Department of Public Safety for subject identification systems and the Arizona Criminal Justice Commission (ACJC) for criminal justice information sharing systems. The challenge will be to establish an organizational structure for governance, develop oversight responsibilities, and coordinate efforts with policy and technical teams.

4. Summary

This thesis will draw upon the successes of other states that have developed technology frameworks that include biometric identification systems, law enforcement information sharing systems, and have established a successful governance structures.

D. SIGNIFICANCE OF RESEARCH

The research for this thesis will serve to build a technology framework that will provide a common approach for integrating subject biometric identification capability into an information sharing environment. The objective of the framework will be to support three strategic trusts established by the *Arizona Strategic Plan*:

1. Implement a rapid identification capability to track information across systems
2. Provide visibility to criminal justice information across jurisdictional boundaries.
3. Extend federal initiatives for statewide records improvement and information Sharing. (ACJC, 2008, p. 14)

The research will also fill the gap between actual state implementations and literature information available on law enforcement biometric solutions and the integration of those solutions into an information sharing environment between state, local, and federal law enforcement agencies.

The research will serve as a starting point for future research efforts in the areas of public acceptance of biometric identification by field officers. In addition, further research will be needed in the areas of information security for mobile identification systems and data security for law enforcement information sharing systems.

This thesis will serve to renew the relationships between state, local and federal law enforcement agencies for collaborative information sharing. The consumers of this research will be Arizona law enforcement agencies, other state agencies, and agencies within the U.S. Department of Justice and the U.S. Department of Homeland Security.

THIS PAGE LEFT INTENTIONALLY BLANK

II. LITERATURE REVIEW

A. HIGH LEVEL SUMMARY

Arizona law enforcement agencies are planning to implement new identification technologies that will improve decision making and support information sharing for state, local, and federal agencies. Developing a technology framework involves the creation of a strategic plan, the selection of identification technologies, and implementation of an integrated information sharing environment.

This literature review was conducted to better understand what has been accomplished in each of these areas and explore what remains to be done in terms of creating an identification system for the state of Arizona. The following topical areas were explored.

- *The Arizona Integrated Criminal Justice Information System Strategic Plan*.
- Arizona identification technologies used by law enforcement agencies.
- Arizona law enforcement information sharing.

Alignment with the federal and state information sharing systems.

B. ARIZONA INTEGRATED CRIMINAL JUSTICE INFORMATION SYSTEM STRATEGIC PLAN

In 2008, Arizona published the *Arizona Integrated Criminal Justice Information System Strategic Plan* (ACJC, 2008) for improving law enforcement subject identification capability and implementing the capability for information sharing across jurisdictions. The following three strategic thrusts are part of the plan:

1. Implement a rapid identification capability to track information across systems;
2. Provide visibility to criminal justice information across jurisdictional boundaries; and

3. Extend federal initiatives for statewide records improvement and information sharing. (ACJC, 2008, p. 14)

In addition, three key goals are identified as part of the implementation of a rapid identification capability:

1. Utilize unique identification to link non-arrest events and formal arrest events with booking events;

2. Provide the capability for law enforcement to establish positive identification of individuals at the earliest authorized point; and

3. Provide unique identification for the exchange of justice information. (ACJC, 2008, p. 14)

The *Arizona Integrated Criminal Justice Information System Strategic Plan* was approved by state law enforcement leaders as a common direction for improving technology and information sharing. However, the plan did not define a framework that specified what identification technologies would be adopted as a state standard or how information sharing would be accomplished. Arizona has several programs underway piloting biometric identification technologies and information sharing within state and local law enforcement agencies.

C. STATE OF ARIZONA CRIMINAL JUSTICE GOVERNANCE

The *Arizona Integrated Criminal Justice Information System Strategic Plan* included improvements to both subject identification and information sharing capability. Subject identification systems are managed Arizona Department of Public Safety, Records Identification Bureau. Both policy and technology support is the responsibility of the Department of Public Safety (Arizona Department of Public Safety, n.d.).

The Arizona Criminal Justice Commission (ACJC) is authorized by state statutes to carry out various coordinating, monitoring and reporting functions. The Commission provides services for 480 criminal justice agencies (ACJC, n.d.). ACJC facilitates information sharing among statewide agencies by monitoring new and continuing legislation, researching and supporting criminal justice programs (ACJC, n.d.).

The Arizona Criminal Justice Commission oversees the AZLink program, the law enforcement information sharing system identified as part of the *Arizona Integrated Criminal Justice Information System Strategic Plan*. ACJC leads a consortium of regional law enforcement agencies that are responsible for establishing and implementing policies and technology for agencies within the state. ACJC is governed by an independent board of law enforcement leaders across the state. The board provides direction and support for all the ACJC programs (Arizona Integrated, n.d.).

D. ARIZONA IDENTIFICATION TECHNOLOGIES

Arizona law enforcement agencies have narrowed down the biometrics possibilities to fingerprint identification, facial recognition, and iris scanning. The introduction of one or more of these new technologies also introduces challenges in regards to public acceptance. Also, there is a growing concern that using multi-modal[2] biometric solutions within law enforcement will require additional federal and state policies.

1. Fingerprint Technology

Fingerprinting has been around longer than any other biometric identification system used in law enforcement. Standards have been developed for maintaining and securing information for fingerprinting that takes place at police department or jail facilities when a subject has been arrested. Policies and procedures have developed over time to address civil rights and privacy concerns.[3]

Mobile fingerprint capability is relatively new within law enforcement. Handheld identification units can process one, two or more fingers either from the right hand, left hand, or both hands. Using Bluetooth communications, or a hard wired connection, the

[2] Multi-modal biometrics uses more than one form of biometric identification to improve accuracy.

[3] A privacy and civil liberties policy is a written, published statement that articulates the policy position of an organization on how it handles the personally identifiable information that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, dissemination, access, expungement, and disposition (Department of Justice, 2008).

handheld devices can transfer fingerprint images to Personal Digital Assistant (PDA) and laptop. The PDA and laptop can also connect to the host server to process the image using wireless or cell phone connections.

In addition, some manufacturers provide handheld units with the capability to use wireless technology to directly communicate with a hosting server. Several vendors offer the capability to download database files directly to the handheld units. This allows direct search from the device against a database without a need to transmit information. Most devices offer a qualification check against the fingerprint on the handheld units. This makes sure the fingerprint meets a quality check before the image is transmitted to be processed. Policies and procedures vary across states for mobile units used by officers in the field.

a. Fingerprint Accuracy

The National Institute of Standards and Technology (NIST) conducted an accuracy study to fulfill requirements of the USA PATRIOT Act and the Enhanced Border Security and Visa Entry Reform Act (Bulman, 2004). The test used operational fingerprints from a variety of U.S. and state government sources. The most accurate systems were from NEC of Japan, SAGEM of France and Cogent, an American company (Bulman, 2004). The performance of these three systems was comparable. The best system was accurate 98.6 percent of the time on single-finger tests, 99.6 percent of the time on two-finger tests, and 99.9 percent of the time for tests involving four or more fingers (Bulman, 2004).

2. Facial Recognition Technology

Facial recognition systems use a standard camera to take a subject's picture. An officer in the field takes a picture and then transfers the information to a computer by placing the camera into a docking station attached to a laptop in a patrol car or a docking station attached to a PC at a remote location. The image can also be transmitted using Bluetooth communications to the laptop in the patrol car. Figure 1 illustrates how images are transmitted and information received by an officer in the field.

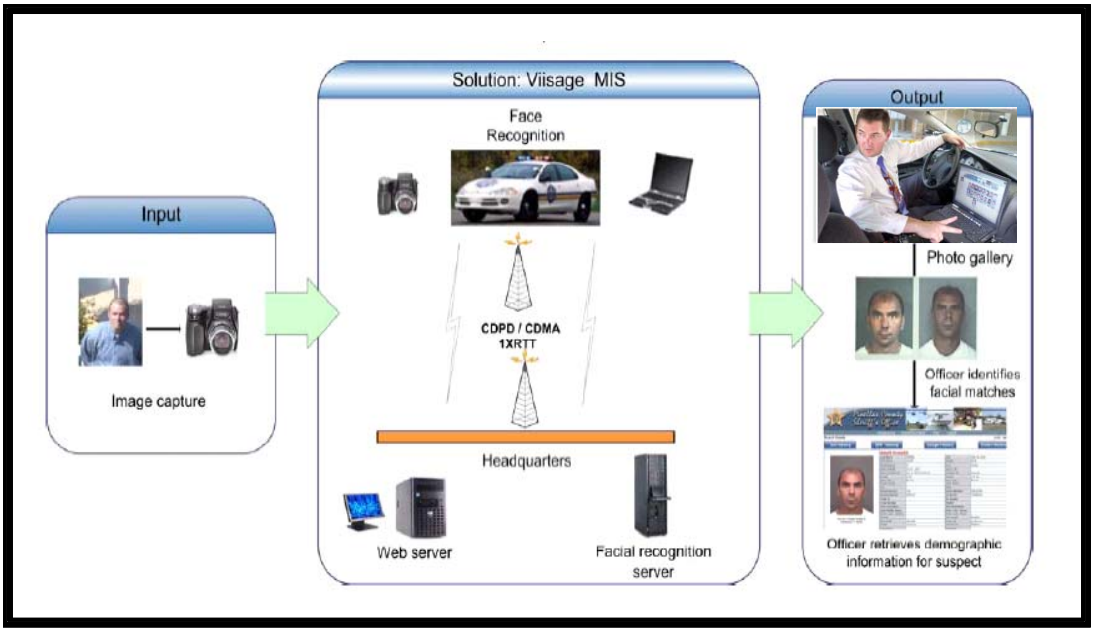

Figure 1. Mobile identification system (From Viisage Technology, 2005)

The image is then processed and sent to a central server to match against the image database. The system processes the image then returns one or more images back to the patrol car's laptop. The officer can then compare the results against the demographics of the subject to make a positive identification (Viisage Technology, 2005). Facial recognition can also be accomplished using a PDA to take a picture and then transmitting the image using Wi-Fi, Bluetooth, or cellular connections to a receiving facial recognition system. Facial recognition systems have drawn lots of attention in regards to privacy.

Advocates believe the Fourth Amendment of the Constitution restricts law enforcement's use of facial recognition systems. Law enforcement must have individualized, and reasonable suspicion of criminal activity before it can "search" someone's face to see if it matches that of an individual in a database. In the *United States v. Dionisio* (1973) court case, the U.S. Supreme Court ruled that a person does not have reasonable expectation of privacy for physical characteristics exposed in public. Therefore, physical characteristics collected in public can be used for image searches. Supporters believe using cameras to capture videos or pictures in public does not violate

the Fourth Amendment (Darryl, 2007, pp. 50–51). The road ahead is unclear for balancing the needs of citizen privacy rights against law enforcement's need to identify subjects and use facial recognition as an investigative tool.

a. Facial Recognition Accuracy

The National Institute of Science Technology completed a facial recognition accuracy vendor test in 2006. The results showed a 10 fold improvement over comparable tests conducted four years prior (Dizard, 2007). The test results rated performance by algorithms from 14 organizations, including vendors and universities (Dizard, 2007). The NIST study found that under the tests' conditions, the algorithms' recognition performance was about the same for very-high resolution still face images, three-dimensional (3D) face images and single-iris images. Facial recognition systems have reduced their error rates from about 0.73 percent in a 1993 to 0.01 in 2006 (Dizard, 2007).

3. Iris Scan Technology

Iris scanning systems can store iris image information on a handheld unit and then compare the image against a database residing on the device. The device can also be connected to a computer that can process the image against a database located on a remote computer. The computer can also transmit the image to a central server for processing. Identification analysis results can be returned to a computer or a handheld device to support decision making (L-1 Identity Solutions, n.d.). Therefore, the iris images can be processed against a database located on a handheld device, remote computer, or a central server.

a. Iris Scan Technology Accuracy

Iris scan accuracy is comparable to facial recognition. In 2006, the Iris Challenge Evaluation (ICE) was conducted by the National Institute of Standards and Technology. The test results indicated iris scans were more than 99 percent accurate (Newton & Phillips, 2006).

4. Multi-Biometric Identification Systems

In 2003, NIST recommended using a dual approach that employs both fingerprint and facial recognition technology as the best option for a biometric system that would make the nation's borders more secure. After studying biometric technologies, NIST, in conjunction with the Department of Justice, made the recommendation to use this multi-biometric combination in a system to Congress (Bulman, 2003).

Iris scan technology is used within law enforcement as part of the arresting and inmate process for identification purposes. Civil rights and privacy policies are not a concern in these areas. Nevertheless, iris scanning devices used by field officers to validate identification prior to an arrest has not gained acceptance in the public's view. The public is sensitive to this technology in that it is intrusive. Unlike facial recognition, iris scanning is similar to fingerprints. Each person has to submit to the biometric data capturing process (Iris Scan, n.d.).

a. Current State Within Arizona

Law enforcement agencies are evaluating a two-fingerprint rapid identification system provided by Sagem Morpho.[4] The system is being tested at the Phoenix, Mesa, and Glendale Police Departments. Currently, the only available biometrics data is for known criminals. The Department of Public Safety provides the standards and database technology for the law enforcement agencies. What remains to be done is to expand identification data collection, storage, and retrieval capabilities beyond that of known criminals within local law enforcement records systems and provide a secured environment for sharing information across agencies.

Facial recognition technology is being used by the Arizona Counter Terrorism Information Center (Hermann, 2006). Use of the technology is very limited. What remains to be done is to determine how facial recognition will be integrated into the state's strategic plan.

[4] Sagem Morpho provides biometric systems to federal and state law enforcement agencies across the U.S. For more information, see http://www.morpho.com/MorphoTrak/Morpho/Morpho_Prod/Crim_Just/rapID_1100.html.

Iris scanning is the least popular form of biometric identification. Currently, it is only used to identify prisoners within the Maricopa County Jail system. There is no interest in expanding this capability.

In addition to biometric identification, the Real-ID program introduced by the Real ID Act of 2005 has been evaluated by the Arizona governor and the state legislature. The program is considered a step in the right direction for improving the accuracy of drivers' licenses; however, the program has not been adopted within Arizona.

5. Real-ID Program Identification Technologies

The Real ID program is a nationwide effort to improve the integrity and security of state issued drivers' licenses and identification cards. The program calls for states to implement minimum standards for security and integrity of state-issued drivers' licenses. Each state must upgrade security features in each card, document and verify applicant's identity, and ensure the applicant does not have multiple drivers' licenses in other states (More Secure, 2009). The act mandated that states would need to comply by 2008. Nonetheless, many states are resisting implementing the federal Real-ID program based on concerns about the high cost of implementation and the concern about citizen privacy (Williams, 2008).

Along with states, many civil rights and privacy organizations are fighting implementing the REAL-ID program. The Electronic Privacy Information Center (EPIC) published an assessment of the REAL ID program in May 2008. Overall, the assessment recommends not adopting the program (Electronic Privacy, 2008). The assessment states the program increases the likelihood of uncontrolled linkage of records about people across government or government supported personal data systems (Electronic Privacy, 2008).

a. Current State Within Arizona

Arizona House Bill 2426 prohibits Arizona from participating in the implementation an Enhanced Driver Licensee (EDL) program recommend in the REAL ID Act of 2005 (Arizona State Legislature, 2008). An EDL contains a Radio Frequency

Identification Chip (RFID). The RIFD can be scanned by a machine from two to 15 feet away (Arizona State Legislature, 2008). This capability would allow law enforcement officers to scan a driver's license when stopped along side of the road or at the police station to facilitate identification verification. Privacy advocates have issues with vicinity scanning RFID technology and the possibility of identification theft (Arizona State Legislature, 2008). Arizona currently has no plans to implement the Real-ID program and is not considered within the technology framework to make such a program feasible. Further research will need to be done to determine if there are any acceptable conditions under which the Arizona State Legislature will change its view and adopt the program.

6. Arizona Information Sharing

With the acceptance of the strategic plan in 2008, the Arizona Criminal Justice Commission along with several law enforcement agencies began a program called AZlink. The program is currently developing the capability to align disparate law enforcement information systems to provide better continuity for law enforcement information sharing. AZLink uses Coplink as its foundation technology. Coplink provides a data warehouse capability for data collection and analysis. AZLink is developing four data center regions for consolidating law enforcement information. Each Coplink data center will be able to share information across Arizona, with the Department of Justice, and the Department of Homeland Security by 2010. By 2012, there will be 33 participating law enforcement agencies in Arizona.[5]

a. Current State Within Arizona

Coplink includes fingerprint and facial recognition technology and receives its information from local law enforcement record systems. Currently, these law enforcement systems do not store any biometric subject identification information. What remains to be done is to provide the capability for local law enforcement systems to

[5] The AZLink plan is part of an Arizona Department of Homeland Security Grant request submitted by B. Kalaf from the Arizona Criminal Justice Commission and the Maricopa Count Sheriff's Office. Grant information can be furnished upon request.

collect and store subject identification information. AZLink will also need to expand outside Arizona to share information with other states and federal systems.

7. FBI's Next Generation Identification Program

The FBI has initiated the Next Generation Identification (NGI) program. The NGI system will offer state-of-the-art biometric identification services. The program is a multi-million dollar effort (Next Generation, n.d.). Within the NGI program, the FBI is creating a Repository for Individuals of Special Concern (RISC). The system will provide law enforcement agencies with rapid/mobile identification services to quickly assess the level of threat that an encountered individual poses.

Currently RISC records include:

- Wanted Persons
- Sex Offender Registry Subjects
- Known or Suspected Terrorists
- (Next Generation, n.d.).

The RISC system will accept both the two fingerprint (2-FID) and ten fingerprint (10-Print) identifiers used in Arizona (Next Generation, n.d.). Combining the 2-FID system with the RISC rapid search capability will allow the appropriate authorities to search both the FBI and Arizona biometrics databases with a single request. Pilot state programs include the Ohio Bureau of Criminal Identification and Investigation, Florida Department of Law Enforcement, Texas Department of Public Safety, and the Minnesota Bureau of Criminal Apprehension (C. Rhoades, personal communication, February 19, 2010).

a. Current State Within Arizona

Arizona's strategic plan includes the integration with the federal identification systems and information sharing programs. What still needs to be done is integrate the state fingerprint system with the federal RISC system. Integration with the RISC system is not in the scope of this thesis.

E. SUMMARY

In 2008, Arizona published *the Arizona Integrated Criminal Justice Information System Strategic Plan* that addressed improving law enforcement subject identification technology and establishing an information sharing capability for state, local, and federal law enforcement agencies (ACJC, 2008). Since the approval of the plan, several agencies have been testing biometrics identification systems, the state has rejected the Real-ID program, and an information sharing program has been established.

Several agencies have started pilot programs for implementing biometric identification technology. Even so, the pilot programs are limited to police substations with identification capability limited to known criminals. Biometric identification information is stored in local law enforcement record management systems and information sharing is limited to a manual process. In order to move the technology out of the substations and into the field, law enforcement agencies are concerned about public acceptance.[6] Future research will be required to define privacy requirements for biometric identification for mobile fingerprint and facial recognition technologies.

The Arizona governor and the state legislature have reviewed the Real-ID program. The program has met with political resistance and has not yet been adopted. However, if the Real-ID program becomes reality in Arizona, it will only improve subject identification for those subjects who have drivers' licenses. Therefore, the technology framework for this thesis will not include the Real-ID capability.

The Arizona Criminal Justice Commission has established a program called AZLink that will implement a state and federal law enforcement information sharing capability. A pilot program is underway in southern Arizona and will soon expand across the state, link together other states, and share information with federal systems. This thesis only addresses law enforcement information sharing within Arizona.

[6] Acceptance meaning the act of favorably receiving new technology with approval (Dictionary.Com, 2010).

Although the literature presents elements of an approach that may be beneficial to achieving the strategy, it does not provide an integrated technology framework to achieve law enforcement subject identification and information sharing.

III. METHODOLOGY

Several states have implemented biometric identification capabilities. This methodology will examine existing implementations of biometric systems that are used to identify subjects at first point of authorized contact and information sharing systems used to organize and analyze law enforcement information housed in various incompatible databases. A comparative analysis methodology was used to understand and synthesize the best practices for designing and implementing biometrics identification systems that have been used within law enforcement and to describe how biometrics identification is used in an information sharing environment. The comparative analysis will examine three components within each state's technology framework. For the purposes of this thesis, there are three components that are included in the technology framework: biometric identification technology, information sharing technology, and governance models that support the technologies.

A. SAMPLE DATA

1. Minnesota's Biometric Identification and Regional Information Sharing

CriMNet is a framework of organization, processes, data, and technology focused on achieving integration of criminal justice processes and data (Macro Group & Labyrinth Consulting, 2000).

The program is not a single system but many systems located around the state working together according to common business rules, data definitions and technology standards.

The Minnesota Bureau of Criminal Apprehension (BCA) provided this researcher with the CriMNet Implementation Roadmap for biometric identification for Minnesota. The roadmap provides a strategic plan for implementing identification processes across the state. Hennepin County, Minnesota, provided this researcher with an overview of the

Hennepin Justice Integration Program.[7] This program is the county's information sharing initiative that is in the process of integrating with the state CriMNet program. In addition, the county provided the business rules, processes, and a context flow diagram of the county's Subject Identification and Locator Service program (SILS).

This researcher selected the Minnesota biometrics implementation roadmap because of the systems capabilities to link together subject identification across the state's law enforcement agencies as well as other criminal justice agencies. The Hennepin County Justice Integration Program and the Subject Identification and Locator Service program were selected as good examples of how regional law enforcement systems can maintain independence and still integrate information across other regional jurisdictions.

2. Los Angeles County Regional Terrorism Information and Integration System

The Los Angeles County Regional Terrorism Information and Integration System (RTIIS)[8] is an integrated law enforcement information sharing system that receives data from independent law enforcement systems and integrates the information into a data warehouse system that provides integrated information back to agencies using real-time access capabilities (Los Angeles Regional, 2005, p. 2). The Los Angeles County Sherriff's Department (LASD) developed the system architecture and supports the technology systems for participating law enforcement agencies.

LASD provided this researcher the RTIIS joint requirement document that was developed by various agencies in group work sessions, the RTIIS data repository architecture design document, the system data model document, and the RTIIS governance model. These documents established the foundation for information sharing in Los Angeles County. In addition, LASD has implemented the Los Angeles County Regional Identification System (LACRIS). The system provides subject biometric information to criminal justice agencies within the county. The county provided this

[7] In 2005, the Criminal Justice System Information Integration Project was renamed to the Hennepin Justice Integration Program.

[8] The RTIIS also includes law enforcement agencies in Las Vegas Nevada.

researcher with an information flow diagram, usage information, and success stories. The RTIIS was selected for research because the system uses a Coplink data warehouse approach. The same approach used within the Arizona AZLink program. The LACRIS system was selected to research integration capabilities with the RTIIS.

3. Wisconsin Department of Justice Fast ID

The Wisconsin Department of Justice provided this researcher a document that describes the system and how it is used in the field. The FAST ID system is Wisconsin's biometrics identification mobile fingerprint biometrics identification system. The research will compare the Fast ID capabilities to those biometric systems used in Minnesota and the Los Angeles County.

4. Vermont Law Enforcement Data Information Sharing Initiative

As part of the Vermont Justice Information Sharing System (VJISS), in 2007 Vermont initiated the Vermont Law Enforcement Data Information Sharing Initiative (LEDSI) program. The Vermont Department of Public Safety provide this researcher an overview of the VJISS strategic plan, privacy policy for law enforcement information sharing, and the technology services strategic plan that identifies the LEDSI technology needs. The Vermont LEDSI does not use Coplink and the data warehouse approach. Regardless, the information provided will allow research into privacy policies requirements for technology.

B. DATA COLLECTION

Many states do not publish technology documentation. Therefore, research was conducted by contacting practitioners and technologists across various states to retrieve existing documentation. Identifying contacts in each state and reviewing all possible combinations of technology frameworks and documentation would have been a massive effort. To narrow down the research, information collection for the technology framework focused on examining the use of existing biometric identification technologies

used in Arizona and the law enforcement information sharing technology that is being used in the AZLink program. The criteria for selecting initial contacts were based on recommendations made to this researcher by:

- Law enforcement professors at the Naval Postgraduate School
- The FBI's Next Generation Identification Program Office (NGI) [9]
- I2 Group [10]
- Sagem Morpho-Morpho Division [11]

Based on recommendations the following states, regions, and local law enforcement agencies were contacted:

- Massachusetts—Boston Police Department
- Colorado—Aurora Colorado Police Department
- Wisconsin—Department of Justice - Crime Information Bureau
- California—Los Angeles County Sheriff's Department
- Florida—Department of Law Enforcement
- Missouri—Criminal Justice Information Services Division
- Minnesota—Bureau of Criminal Apprehension
- Texas—Department of Public Safety Biometrics Identification Division
- Ohio—State Attorney Generals Office
- Vermont—Department of Public Safety

Research requests included calling each practitioner and technologist to discuss this thesis and the requested documentation. In addition, emails were sent out that

[9] The NGI Program Office's mission is to reduce terrorist and criminal activities by improving and expanding biometric identification. One objective is to share biometric identification information with state, regional, and local law enforcement agencies (Next generation, n.d.).

[10] I2 Group provides Coplink as the law enforcement information sharing solution to Arizona.

[11] Sagem Morpho-Morpho Division is the sole source for biometrics identification products for Arizona.

outlined the information requested for analysis. Additional phone calls where used for clarification when needed. The following information was requested:

- Strategies, plans, and design documents for implementing biometrics technologies.
- Listing of law enforcement or criminal justice agencies involved.
- Listing of technology products.
- Data and process flow diagrams.
- Strategies, plans, or design documents for implementing law enforcement information sharing.
- Governance documentation (organization structures, roles and responsibilities, and policies)
- Any statistics or success stories.

Out of the 10 states contacted, four states, Minnesota, Los Angeles County California, Wisconsin, and Vermont contributed information included in this thesis.

Many states, regional, county, and local law enforcement agencies do not publish technical documentation; however, information can be obtained through public requests. Information for this thesis was retrieved through direct contact with practitioners and technologists that work across various departments within state agencies or through documentation posted on the internet. Some states create extensive documentation and others have very limited documentation. The type of documentation retrieved came in many forms; formal documents, graphical charts, information and process flow documents and personal emails.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. ANALYSIS

A. MINNESOTA BIOMETRICS IDENTIFICATION AND INFORMATION SHARING

1. Minnesota's Technology Framework Components

Minnesota's biometrics identification program is the state's Automated Fingerprint Identification System (AFIS) used to identify subjects' during the jail booking process and the mobile field officer biometrics system used by law enforcement officers to identify subjects' in the field. In addition, Minnesota is now testing subject identification validation against the FBI's Repository for Individuals of Special Concern (RISC).

The state also provides a criminal justice subject event tracking system called the Name Event Index Service (NEIS). Through a database indexing capability, NEIS links together information stored in disparate criminal justice systems to subjects identifiers. In addition to the state's NEIS system, Hennepin County and other counties provide their own independent subject identification index systems. Hennepin County provides the Subject Identification and Locator Service (SILS) System. Independent criminal justice systems can retrieve information using the index systems at a state level or just within the county.

Minnesota's criminal justice agencies maintain and manage their own information. Information sharing capability is provided by the state NEIS system. The system provides access to disparate systems across agencies and consolidates the information for presentation and reporting.

The state's Department of Public Safety provides oversight for both biometric identification and information sharing capability through a program called CriMNet. Governance for the program is provided by the Criminal and Juvenile Justice Information Policy Group (CJJIPC) and the Criminal and Juvenile Justice Information Task Force

(CJJITF). The following diagram illustrates the Minnesota components in the state's technology framework. Figure 2 illustrates Minnesota's Technology Framework for subject identification and information sharing.

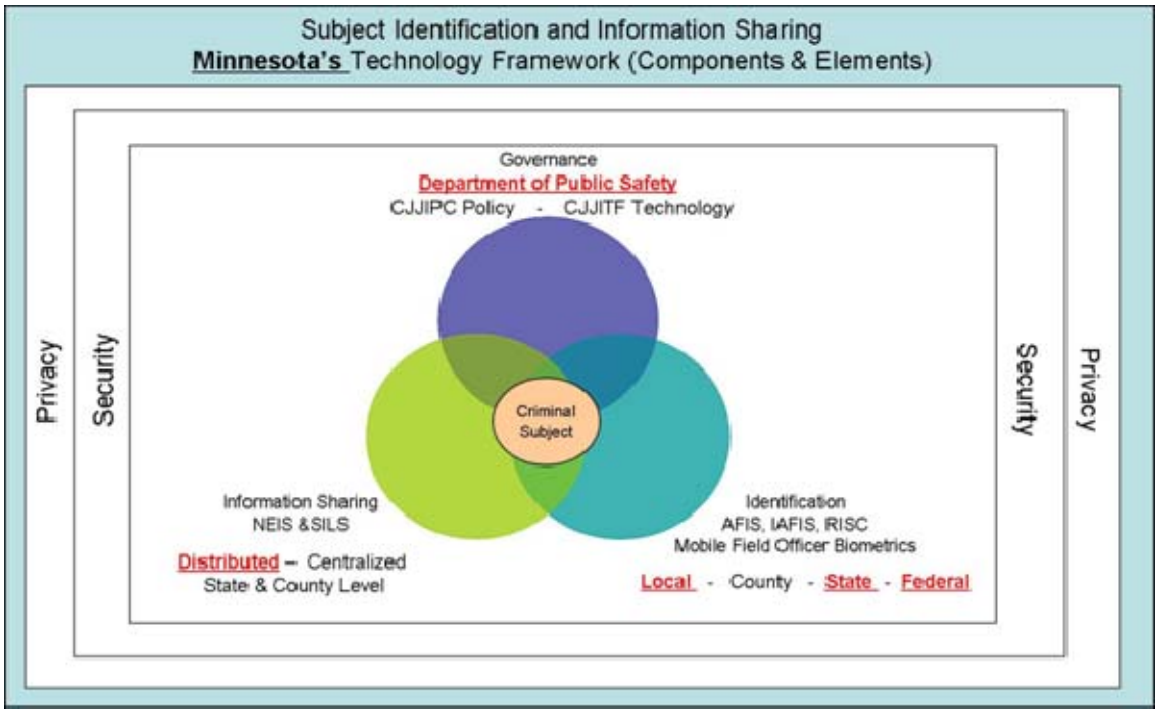

Figure 2. Minnesota's Technology Framework (Components and Elements)

2. What is CriMNet?

Minnesota has recognized the need to have accurate integrated criminal justice information available for decision making. Agencies depend on information provided by other organizations. Without information sharing, criminals and suspects can remain free because information from one state agency in a county may not be available to a judge in another county. CriMNet is Minnesota's solution for criminal justice information sharing across the state.

> CriMNet is a state-level program that works with Minnesota State and local agencies to make accurate and comprehensive criminal justice information available to criminal justice professionals in law enforcement, the courts and corrections. It is part of the Minnesota Bureau of Criminal Apprehension (BCA) (About CriMNet, n.d.).

The BCA was created by the State Legislature in 1927 to assist law enforcement agencies throughout Minnesota in solving local crimes and apprehending criminals. The BCA is part of the Minnesota Department of Public Safety (BCA History, n.d.).

CriMNet is not a single technology solution, but an effort that is shared between executive, legislative, and judicial branches of government with a focus on improving public safety (About CcriMNet, n.d.).

CriMNet is not a single database or technology solution. It exists to coordinate information sharing from a statewide and potentially nationwide viewpoint known as the "enterprise" view12 so that systems can work together. This requires the development of statewide standards for data, technology and business practices and methods for agencies to access and understand those standards. (About CriMNet, n.d.).

a. CriMNet Vision

CriMNet "provides for the safety of the public, victims, and criminal justice practitioners through delivery of accurate and timely information via efficient and effective processes and systems." (Macro Group & Labyrinth Consulting, 2000).

b. CriMNet Goals

- To accurately identify individuals.
- To make sure that criminal justice records are complete, accurate, and readily available.
- To ensure the availability of an individual's current status in the criminal justice system.
- To provide standards for data sharing and analysis.
- To maintain the security of information.
- To accomplish our tasks in an efficient and effective manner. (About CriMNet, n.d.)

[12] The enterprise view is sometimes referred to as the CriMNet Enterprise Architecture.

3. The Story of Two Identical Twins

The Minnesota Identification Roadmap has an excellent example of how two subjects with very similar names can be mistaken when faced by an officer and human error can create inaccurate information with law enforcement records (Integration Architects, 2005, p. 5). John and Jonathon Echols are identical twins with criminal records in Minnesota. When an officer confronted John with a warrant for arrest, John claimed innocence. The officer assumed John's real name was Jonathon and to took him to jail. Once the officer had John printed at the jail and the biometrics were compared to his records on file, it was learned that John had a twin brother named Jonathon. John was then released.

Human error occurred when a court clerk compared two sets of records, one set for John and one set for Jonathon. The clerk investigated the subjects' demographics and dates of birth and assumed the two sets of records contained information about the same subject. The clerk merged the records together. During a jail booking process for Jonathon, the merge was discovered and it took considerable time to untangle the electronic records (Integration Architects, 2005, p. 5). The above example is only one case out of many with identity and record accuracy issues found in Minnesota.

4. Identification Roadmap Initiative

The expansion of the integrated Minnesota Court Information System (MNCIS) across 87 counties demonstrated the complexity of information sharing on a state wide basis. Many court systems had records of the same subject and in many cases; the records had inaccurate information (Integration Architects, 2005, p. 3). In 2004, an Identification Steering Committee was formed to address identification and record accuracy issues. In 2005, the steering committee held several workshops that examined the criminal justice system from a subject identification perspective and the impact to the criminal justice business (Integration Architects, 2005, p. 7). The outcome of the workshops yielded six areas that needed dramatic improvements in identification:

- Return comprehensive identity information to law enforcement agencies and detention facilities.
- To accurately identify individuals.
- To ensure the availability of an individual's current status in the criminal justice system.
- To make sure that criminal justice records are complete, accurate, and readily available.
- To provide standards for data sharing and analysis.
- To maintain the security of information. (Integration Architects, 2005, pp. 7–8)

This researcher focused on improvements one through three to address the biometric identification section of the technology framework. The standards for data sharing, analysis, and maintaining the security of information is specific to Minnesota. There are three sections in the identification roadmap that are specific to Minnesota's biometric identification technology framework, the identification protocol standard, the Biometric Identification Workflow Manager (BioID) and the Subject and File Enhancement System (SAFE). BioID is a system that retrieves identity information from multiple justice systems and monitors the status of a subject as they move through the justice process. SAFE is a system that captures a person's identify and event information (Integration Architects, 2005, p. 11).

The SAFE program has been renamed to the Name Event Index Service (NEIS) (J. Olson, personal communication, February 16, 2010). For the purposes of this thesis, future references to SAFE or NEIS are interchangeable (SAFE/NEIS).

5. Identification Protocol Standard

The identification protocol is the Minnesota standard for biometric identification of a subject. The standard determines who can be identified and under what conditions. The standard also defines who is authorized to make the identification, the appropriate method for the given situation, and the procedure for managing the biometric information. Minnesota has defined the identification protocol standard as a state statute

299C.10 (Integration Architects, 2005, p. 1). Having the standard defined by state law establishes a baseline for possible challenges in court and also gives the public the right to change the law.

The state statute defines the type of felony and misdemeanor crimes that require biometric identification. The crimes apply to both adults and juveniles. The statute extends beyond those subjects arrested and covers officer judgment. If an officer believes a subject is a fugitive from justice, the officer has the right to request fingerprint biometric identification (Integration Architects, 2005, p. 2).

The Minnesota law calls for biometric identification at the earliest authorized point in the justice system (officer contact in the field), during jail booking, court hearings, and in correctional facilities. The identification procedure is to be performed by sheriffs, peace officers, and community corrections agencies (Integration Architects, 2005, p. 2).

In many states, the first time subject electronic fingerprints are taken happens at a jail facility during the booking process. The standard process for booking a subject into jail is to capture an electronic image of all 10 fingers (10-Print) within the Automated Fingerprint Identification System (AFIS) and compare the images against the AFIS identification database. In addition, the images are sent to the FBI's Integrated Automated Fingerprint Identification System (IAFIS)[13] to compare against the federal identification system.

If the set of fingerprints submitted to the FBI's IAFIS system are unique (no match) a new FBI record will be created. The master record will contain the name and demographics of the information submitted by the requesting agency and a unique FBI identification number (FBIID) will be assigned. The FBI does not perform any verification against the subject's name or demographics. If the subject is arrested again (from any state), any new names and demographics will be recorded as alias information and attached to the master record. If a new record is created or there is a match to an

[13] IAFIS, is a national fingerprint and criminal history system maintained by the Federal Bureau of Investigation. For more information on the IAFIS, see http://www.fbi.gov/hq/cjisd/iafis.htm.

existing record, the FBI will respond to the requesting agency with the master record of identification information and all associated alias information. Changing the subjects name and demographic information can be done, but it is a lengthy, formal process (F. Jaco, personal communication, February 16, 2010).

The only accurate information returned by the FBI's IAFIS system is the FBIID associated with the subject's biometrics. There is no guarantee the subject information is accurate. The FBI associates all federal criminal information with the FBIID, not a subject's name or demographics. However, the FBI does allow searching against the subject's information. Law enforcement agencies understand the results may not yield the appropriate information.

In addition, the fingerprints submitted to the FBI IAFIS system may not meet the quality standards established by the bureau. In this situation, a state record will be created without creating a link between the State's Identification Number (SID)[14] and the (FBIID).

Minnesota will either create a new record or match against an existing record through its AFIS system based on the biometrics submitted at booking time. Information will be sent back to the jail facility during the booking process. The information sent includes the SID, subject's name and demographics associated with the state record and the FBIID if available.

New technology allows the integration of smaller mobile biometric identification devices using two fingers (2-FID)[15] with the existing state AFIS system. The identification protocol modified the existing state AFIS identification process to take advantage of the new technology. The protocol allows a 2-FID be taken prior to booking by field officers. The 2-FID system validates the subjects identify against the existing AFIS database. If a match is found, the subject's identification information (along with

[14] Each state creates a unique subject identifier called a SID. The SID is based on a subjects fingerprint biometrics. The SID is unique only within the state.

[15] New mobile technology also allows the use of two fingers, four fingers or a palm print. Some vendors refer to this type of technology as flat prints or patterns. For the purposes of this thesis the researcher references only two fingerprint units (2-FID).

additional information provided by the SAFE/NEIS system) is returned to the requesting officer. The state SID is used to link together the information from the state AFIS system and the SAFE/NEIS system. If no match is found, a "no hit" status code is returned by the SAFE/NEIS system. If warranted, the subject will be brought into the jail for fingerprinting (Integration Architects, 2005, p. 3).

The following diagram depicts a field identification scenario where the identification is completed by a filed officer and the information is passed on to the jail management system for booking and the police department's record management system. Figure 3 illustrates the process law enforcement officers use in Minnesota for a typical subject field identification.

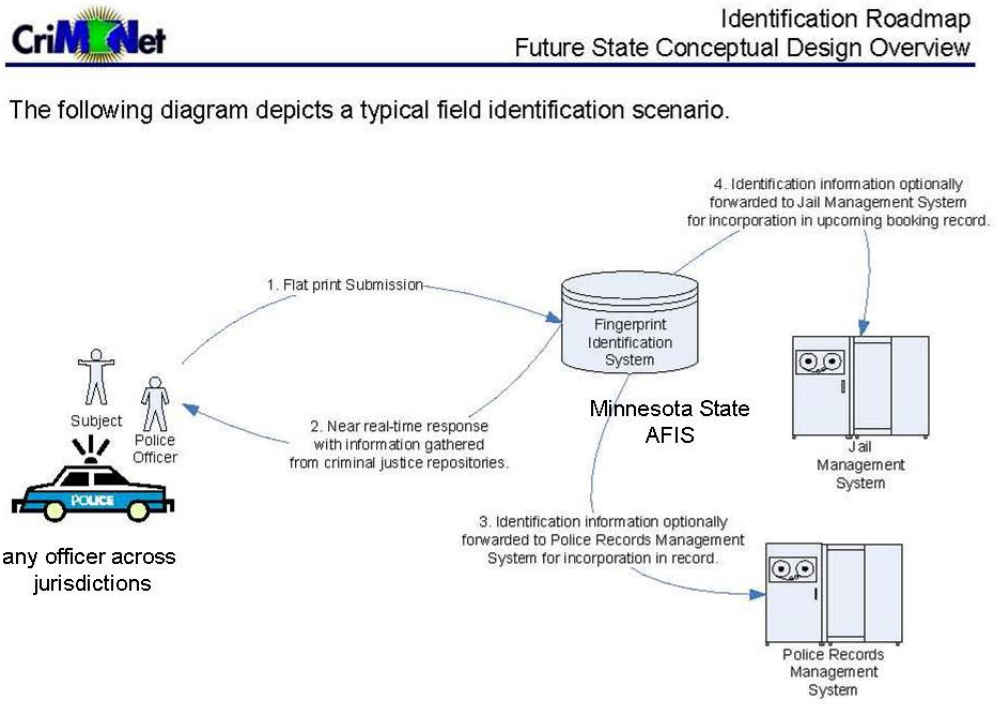

Figure 3. CriMNet Field Officer Identification scenario (From Integration Architects, 2005, p. 2)

The identification protocol also identifies management procedures that will be followed to maintain data accuracy and personal privacy protection:

- Systems and processes will adhere to the Minnesota Government Data Practices Act; [16]
- Subject identification keys will be maintained, exchanged, and accessed electronically;
- Fingerprint quality will be maintained (quality standards must be defined and enforced). (Integration Architects, 2005, p. 3).

Finally, the identification protocol does not define what information should be contained in criminal information records. The process of who should be identified, under what conditions, who is authorized to make identifications, methods used, and the procedures for managing identification information is completely independent from any other criminal justice process or system (Integration Architects, 2005, p. 1).

6. Name Event Index Service (SAFE/NEIS)

A subject can move through the criminal justice system many different ways and multiple times across police departments, court systems, correction systems, and jurisdictional boundaries. Subject criminal events are captured in various independent record management systems. Since CriMNet is not a single system but a program that exists to coordinate information sharing, criminal justice agencies create independent identification systems. The SAFE/NEIS system was created to track subject criminal events, various agency subject identification keys and link them together. A series of events and identification keys are linked together through a thread (Integration Architects, 2005, p. 2).

A thread can be considered as a criminal case.[17] For example, a subject was arrested for burglary by the Hennepin County Sheriff's Office, and at a different time the subject was arrested for driving under the influence of alcohol (DUI) by the Ramsey County Sheriff's office. The events associated with the Hennepin County Sheriff's

[16] The Minnesota Government Practices Act is found in Minnesota Statutes, chapter 13. The statues are created on the presumption that state and local government records are accessible to the public, unless a statute or rule provides otherwise. The Act contains many of the statutory provisions that classify various types of government data as other than public, and thus restricts access to the data in some way. The features of the Act can be found at http://www.house.leg.state.mn.us/hrd/pubs/dataprac.pdf

[17] A case can have multiple criminal charges.

Office arrest, jail booking, court process, and adjudication is considered a thread. The events associated with the Ramsey County Sheriff's Office arrest, jail booking, court process and adjudication is considered a different thread. Each thread tracks the subject through the criminal justice process.

The SAFE/NEIS system captures the subject identification[18] information along with the event information from each agency as the event occurs. The system will build a subject profile across all events using the agency's subject identification information linked together with the Global Identification Service Identifier (GID) created by the SAFE/NEIS system. The GID is used to uniquely identify a person within the SAFE/NEIS system. Associated with a GID are one or more Local Person Identifiers (LIDs). The LIDs used by agencies as person identifiers (Integration Architects, 2005, p. 32). Figure 4 illustrates the integration of threads into the SAFE/NEIS system.

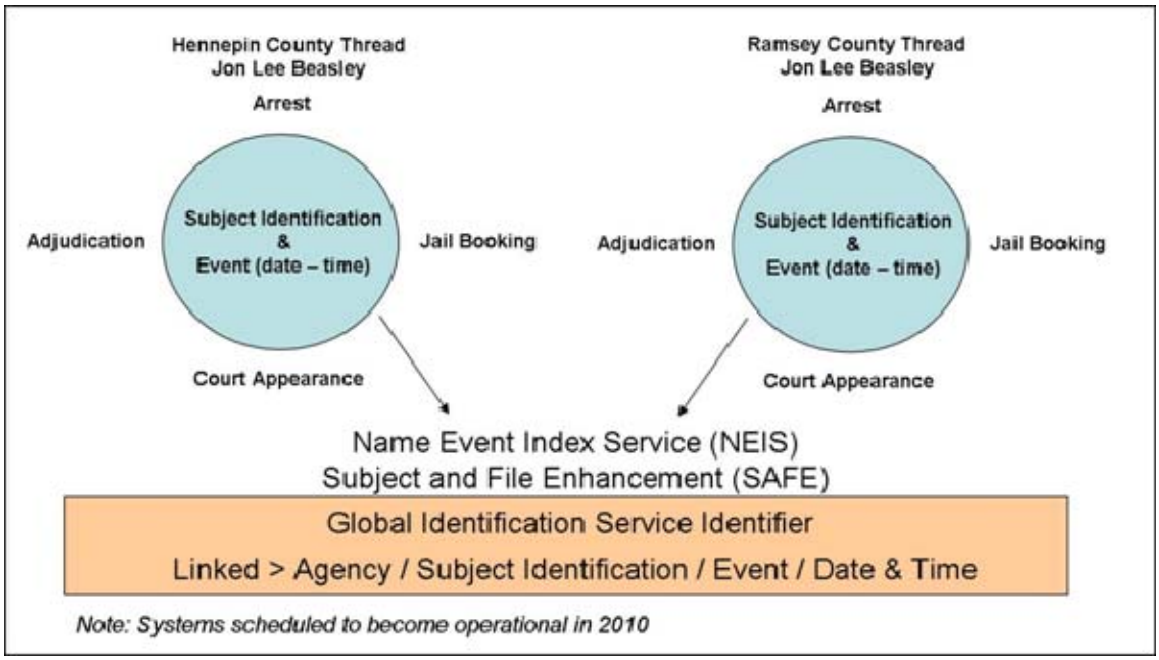

Figure 4. CriMNet SAFE/NEIS Integrated Agency and State Biometric Identification

[18] Counties have independent identification systems. The subject identification identifier is unique to the subject within the county.

The SAFE/NEIS system is a centralized identification service provided by the state; however, larger counties such as Hennepin and Ramsey counties provide their own identification services for their respective criminal justice agencies. These systems are known as regional complex identification systems. The SAFE/NEIS system interacts with both complex identification services and simple identification systems unique to a single agency. This researcher will examine the Hennepin County complex Subject Identification and Locator Service (SILS) later on. Figure 5 illustrates the relationship between the SAFE/NEIS identification system, a complex county system, and a simple system used by a single agency.

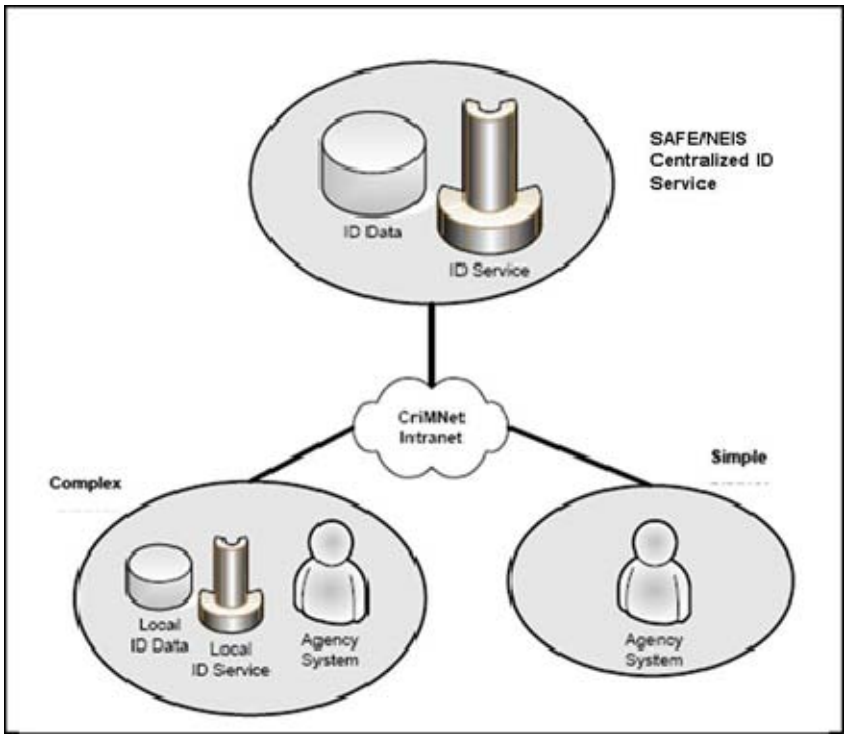

Figure 5. Distributed option (From Integration Architects, 2004, p. 9)

The subject identification and event profile within SAFE/NEIS will allow a "Subject Identification Viewer"[19] to access information across state and local agencies. In addition, by using the date and time stamps the current status of a subject can be

[19] The research did not identify if the Identification Viewer had been created after the document was published.

determined in any thread (Integration Architects, 2005, p. 4). Figure 6 illustrates the vertical and horizontal subject identification information available to the viewer.

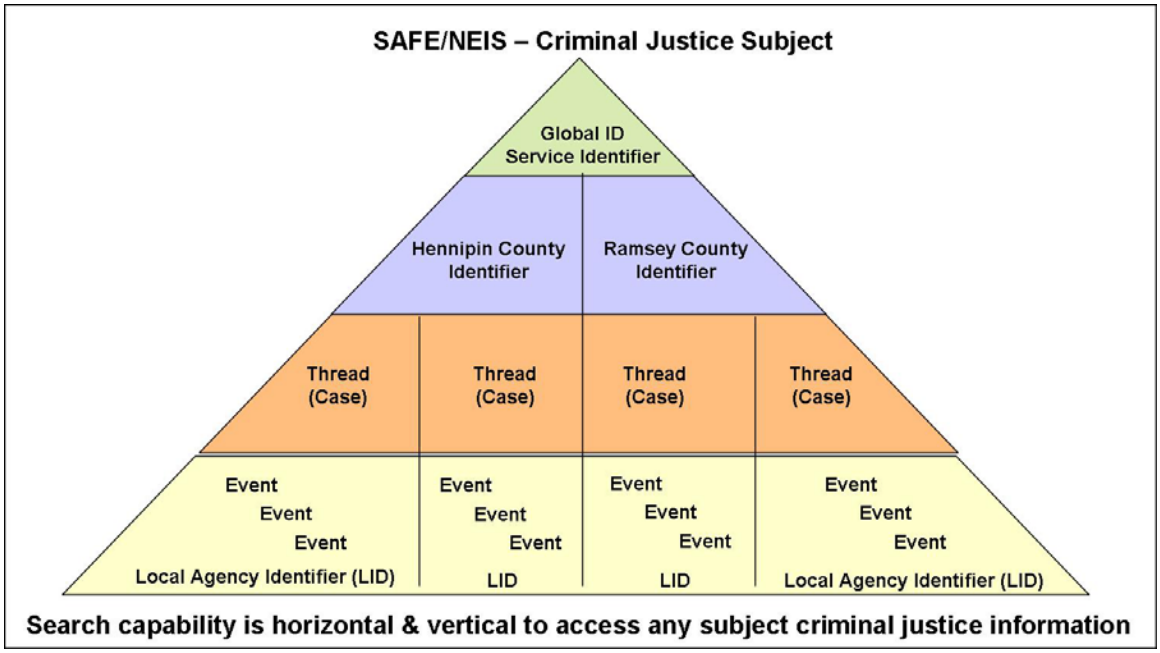

Figure 6. CriMNet SAFE/NEIS Subject Identification Viewer (operational 2010)

7. Biometric Identification Workflow Manager and the Conceptual Model

The biometric identification workflow manager handles retrieval of identify information from multiple justice applications and monitors events (Integration Architects, 2005, p. 11). The primary functionality is managing the transaction flow, data processing rules, and the routing of identification transactions. In addition to the SAFE/NEIS system, the Biometric Identification Workflow Manager manages the information exchanges between two other identification systems used by criminal justice agencies, the Automated Fingerprint Identification System (including 2-FID) and the Minnesota Repository for Arrest Photos (MRAP) system. The above systems are packaged as the CriMNet identification system that supports the state's criminal justice applications and the events that occur to subjects traversing through the criminal justice process (Integration Architects, 2005, p. 3). Figure 7 illustrates the identification roadmap conceptual model.

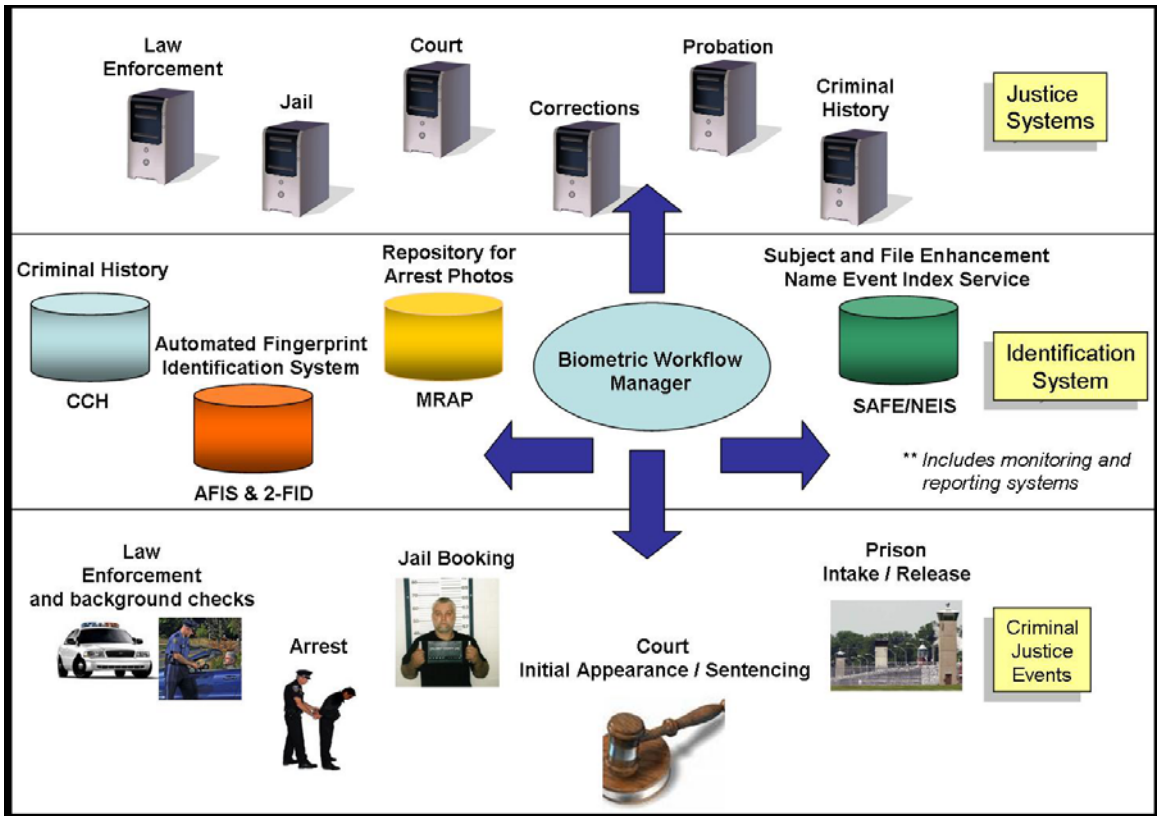

Figure 7. CriMNet Implementation Roadmap Conceptual Model (operational 2010) (After Integration Architects, 2005, p. 3)

The CriMNet identification system includes the Implementation Protocol, SAFE/NEIS system, and the Biometric Identification Workflow Manager. The identification system has far reaching impacts for linking together subject information across systems and events as shown in the conceptual model. The implementation roadmap goes into further detail about integration between justice systems and events. The roadmap identified seven categories and 157 system integration opportunities for subject information across the criminal justice lifecycle. The following table (Table 1) summarizes the possible connections for linking together information using the SAFE/NEIS system and the Biometric Workflow Manager events (Integration Architects, 2005, pp. 5–65).

Table 1. CriMNet Justice Lifecycle Event Model Summary

CriMNet Justice Lifecycle Event Model Summary		
Event Category	**Definition**	**System Integration Opportunities**
Applicant Services	background checks, identity theft, mistaken identity requests	5
Investigations	subject identification Investigations	11
Charged with an Offense	arrest, booking, citations, prosecution, release, transfer	43
Court Processing	warrant, appearance, case, disposition, orders, sentencing, summons	49
Supervision	sex offender and criminal registration, probation, check-in	18
Incarceration	prison intake and release, workhouse intake and release	25
Post Release Supervision	offender on probation encounters law enforcement or probation officer	6
Criminal Justice Categories = 7		
Subject information integration opportunities = 157		

8. Identification Roadmap Enablers

The Implementation Roadmap identified five key enablers that were required to be successful at creating an integrated biometric subject identification capability across Minnesota's criminal justice agencies.

- Executive long term focus and commitment that included funding, resources, and sponsorship.
- Legislative champions that support changes and additions to statutes and also funding requests.
- Adherence to State and Federal data privacy laws.
- Completion of a Privacy Impact Assessment (PIA)[20] for the SAFE/NEIS system.
- Cross agency program oversight. (Integration Architects, 2005, p.9–10)

9. Hennepin County Justice Integration Program

Hennepin County is the largest population county of the 87 counties in Minnesota. The county ranks sixteenth in population size across the metropolitan areas

[20] Privacy Impact Assessment is a series of questions that evaluate the processes through which personally identifiable information is collected, stored, protected, shared, and managed by an electronic information system or online collection application (U.S. Department of Justice, 2008, p. 1).

within the nation. The county houses a quarter of the state's population and includes the city of Minneapolis (Fast Facts, n.d.). Hennepin County has 47 law enforcement jurisdictions (About HCSO, n.d.).

The Hennepin County Criminal Justice System Information Integration Project (CJSIIP) began in 1999 as Minnesota's efforts to create an information sharing environment that allowed all criminal justice agencies to share information. The initial scope for integration covered the county's law enforcement agencies, city and county prosecutors, courts, probation and parole, jails, and the county's incarceration facility. The CJSIIP efforts enticed other counties to establish similar integration efforts (Gil-García, Schneider, & Pardo, 2004, p. 12). In 2005, the CJSIIP program was renamed to the Hennepin Justice Integration Program (HJIP) (L.Tite, personal communication, February 19, 2010). For the purposes of this thesis, future references to CJSIIP or HJIP are interchangeable (CJSIIP/HJIP).

The county effort gained legislature support and funding for the development of a state wide integration effort leveraging the best practices from the CJSIIP/HJIP. With the interest across other counties, success of CJSIIP/HJIP, and the support from the State legislature, CriMNet was created to orchestrate the integration efforts and provide services across the counties. Hennepin County serves in an advisory capacity on various state-level boards created to guide the CriMNet initiative **(**Gil-García et al., 2004, p. 12). The Hennepin County Identification and Locator Service System is part of the HJIP.

a. Hennepin County Subject Identification and Locator Service

As mentioned earlier, some Minnesota counties maintain their own identification services for their respective criminal justice agencies. The Hennepin County Subject Identification and Locator Service (SILS) provides a regional identification service to agencies in the county.

Historically, law enforcement agencies, County and City Attorney's offices, courts, and correctional facilities created independent identification systems. The SILS system identifies links and cross references various subject identifiers associated with independent criminal justice record management systems. Agencies are responsible

for managing their own criminal justice information and providing identification and event information to the State's SAFE/NEIS system. SILS was created to provide a county subject identifier and compliment other county identification initiatives and the State CriMNet SAFE/NEIS system (Hennepin County, 2005, p. 3). The HJIP SILS system went into production July 16, 2007 (L. Tite, personal communication, February 19, 2010).

The SILS system accepts various forms of subject identification from county agencies. Biometric identification verified against the state AFIS system and retrieval of the SID is preferred. The SILS system does not communicate directly with SAFE/NEIS (L. Tite, personal communication, January 26, 2010). However, agencies that have not implemented biometric identification can use other identification methods such as driver's licenses, social security numbers, and subject demographics.

SILS stores the method [21] used for identification by each agency. Regardless of the forms of identification used, each agency creates its own unique subject identifier that SILS will accept and link together with the Hennepin County Identifier (SILS ID) (Hennepin County, 2005, pp. 8–12). A SILS ID begins usually at an arrest or a warrant request (Hoch, 2007, p. 6). Figure 8 illustrates the flow of the SILS identification information across various criminal justice agencies.

[21] Identification method is an indicator of how the agency determined the subject's identification. Possible methods are biometric, driver's license, subject number submitted by another agency, and a subject's demographics.

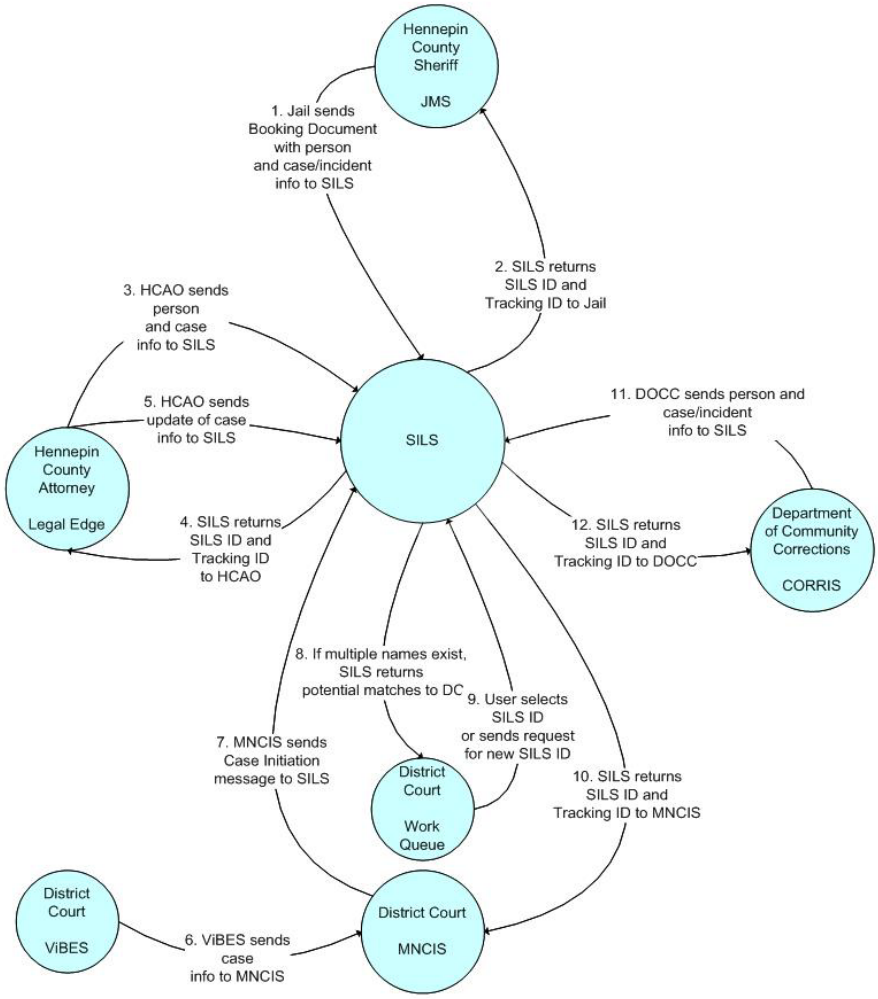

Figure 8. High Level Business Context Overview Diagram (From Hoch, 2007, p. 11)

SILS offers a county search capability similar to SAFE/NEIS. Agencies can search the SILS system using their agency subject identification key, the SILS ID, driver's license number or subject demographics information. SILS returns cross reference link information that identifies agencies within the county that have subject information within their record management systems (Hennepin County, 2005, p. 13–22).

10. Minnesota Information Sharing

Each criminal justice agency is responsible for maintaining its criminal justice information. The SAFE/NEIS subject identification system in Minnesota only provides linkage to agency systems. The SAFE/NEIS will provide access to information across disparate criminal justice agency systems, and a comprehensive view of a subject's criminal activity. The SAFE/NEIS pilot program began in 2008 (Name Event Index, 2008). The system is expected to be operational in 2010 with a limited number of statewide systems providing information (J. Olson, personal communication, February 16, 2010).

11. Minnesota CriMNet Program Office Governance

Governance of CriMNet is the responsibility of the Criminal and Juvenile Justice Information Policy Group (CJJIPC) and the Criminal and Juvenile Justice Information Task Force (CJJITF). Both groups were established by the Minnesota legislature, [22] to over see criminal justice information policy (CriMNet Program Office, n.d.).

The policy group has responsibility for budgets, program priorities, direct hiring of the CriMNet program director, and tracking criminal justice information sharing issues. The policy group has responsibility for completing statewide criminal justice information integration and makes recommendations to the governor, legislature and the Supreme Court for decision making (Criminal and Justice, n.d.). Group membership is made up commissioners from the executive branch and judicial branch of government. In addition, the chairman and vice-chairman of the task force participate in the group. The policy group also appoints members to the task force[23] (CriMNet Program Office, n.d.).

The Criminal and Juvenile Justice Information Task Force is made up of criminal justice and state agency professionals, local municipal representatives and state citizens (CriMNet Program Office, n.d.). The task force provides oversight and monitors

[22] Minnesota Statutes 299C.65.

[23] As defined by Minnesota state law.

CriMNet related projects as directed by the policy group. The task force also reviews funding requests, appoints project delivery teams, seeks resources for issues through the policy group (Task Force, n.d.).

The Minnesota Bureau of Criminal Apprehension (BCA) provides oversight and state administrations services for the CriMNet Program Office. The BCA is a division of the Minnesota Department of Public Safety (CriMNet Program Office, n.d.).

The Minnesota Justice Information Services (MNJIS) provides the technology support for the biometrics' and information sharing systems. MNJIS was formed in October 2008 and took on the responsibility of the criminal justice information systems from CriMNet. MNJIS is now a division directly at BCA (MNJIS Programs, n.d.). Figure 9 illustrates the BCA organizational structure and the influence the policy group and the task group have on the CriMNet program.

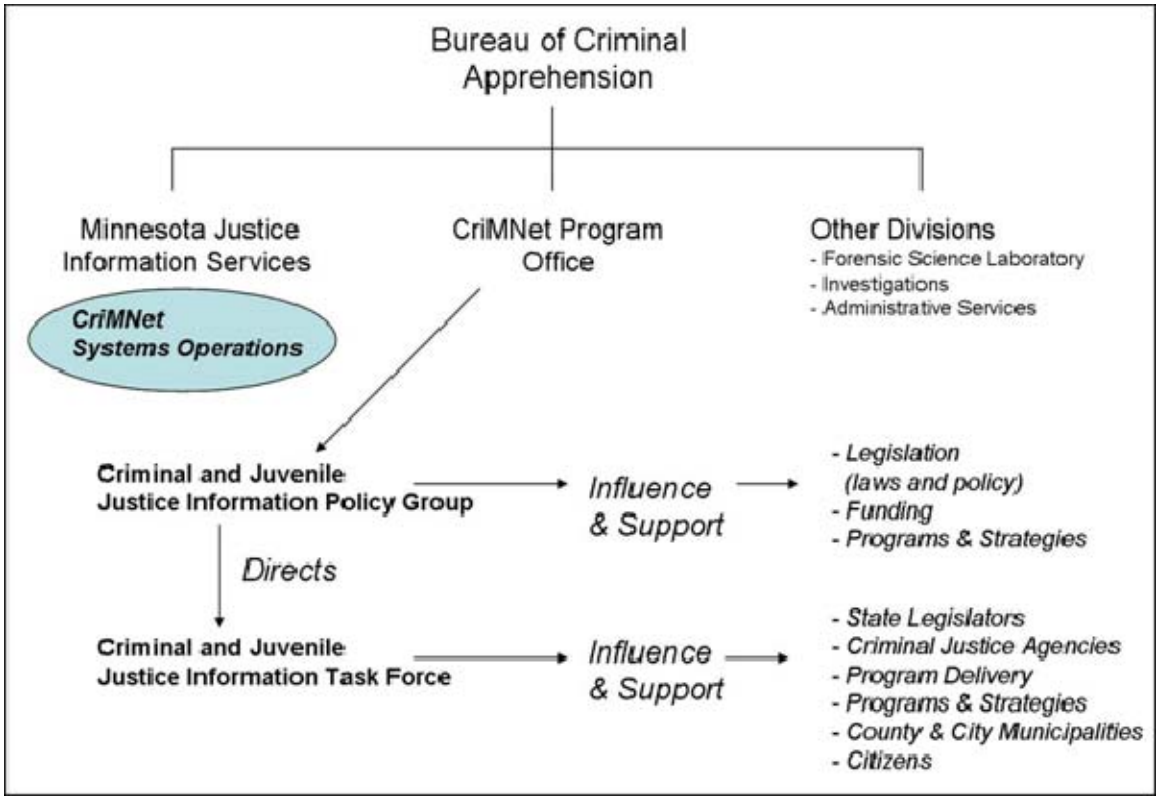

Figure 9. CriMNet Governance and Influence

12. Minnesota Best Practices

Hennepin County provided the foundation for best practices for the state CriMNet effort. The county, in coordination with the state, implemented the Criminal Justice System Information Integration Project (CJSIIP/HJIP). The project identified best practices that became instrumental in other CriMNet projects. The purpose of researching the CJSIIP/HJIP is to look at the key elements used within the project as they relate to information sharing and governance.

a. CJSIIP/HJIP Business Case Foundation Points for Sharing Information

The business case for gaining legislative support, funding, and sponsorship of CJISIIP/HJIP rested on the following foundation points.

- Shared information is more accurate.
- Collect the same information multiple times across many different systems. This leads to incomplete records, conflicting data, and inaccurate information. The objective is to collect information once and share many times.
- Shared information is timelier.
- Shared information is more readily available.
- Shared information is more complete.
- Information from many sources can be assembled into a complete record. [This researcher also notes from experience that time is critical when initiating an investigation to a crime. Having a complete record of a subject's information can be critical to an arrest.]
- Shared information is less expensive.
- Information stored once and shared is less expensive than collecting the information many times. (Macro Group & Labyrinth Consulting, 2000, p. 2)

b. CJSIIP/HJIP Business and Technology Framework

Hennepin County developed a framework that included elements for success. The project's success was highly dependent on cross functional and highly interdependent business and technical staff, criminal justice processes, data, standards, and shared technology. Key elements include:

- Organizational model
- The organizational model is made up of members across criminal justice agencies. The model also includes roles and responsibilities to effectively support, fund, and manage information sharing.
- Process model
- The process model includes the business processes and the information flows across the various processes.
- Data model
- The data model includes the data definition and standards required for sharing information between criminal justice agencies.
- Technology model
- Technology includes the functionality, guidelines and standards that enable information sharing in an integrated environment.
- Motivational model
- The motivation model provides each organization the will to succeed in adding value to the state as well as each organization. CJSIIP/HJIP recognizes that the vision of information integration has to include shared values. (Macro Group & Labyrinth Consulting, 2000, p. 2)

c. CJSIIP/HJIP Critical Success Factors

CJSIIP/HJIP consists of individual projects across criminal justice agencies. The projects all share several aspects that were critical to information integration and information sharing. Program governance has the responsibility to address each critical aspect required for success. In order to be successful, the follow aspects are addressed:

- Cultural change

- Thinking and behavior needed to shift from an agency centric view to a CJSIIP/HJIP enterprise view. Agencies and teams must work cooperatively to insure the success of all individual projects. Even if an agency needs to allocate funding and resources to a critical project that may only indirectly benefit the agency.

- CriMNet compliance

- Since CriMNet exits to coordinate information sharing form a statewide and potentially a nationwide viewpoint (enterprise view), CJSIIP/HJIP projects must comply with CriMNet statewide standards for data, technology, business practices and methods.

- CriMNet vision

- The vision is the standard by which integration decisions and efforts are judged. As stated earlier, the vision "provides for the safety of the public, victims, and criminal justice practitioners through delivery of accurate and timely information via efficient and effective processes and systems."

- Stable funding

- CJSIIP/HJIP funding is required for new projects and ongoing support for the new systems. The critical aspect of funding was that funding could not come from current agencies budgets. New funding sources had to be addressed from the state budget. Governance and legislative efforts hand to address this critical aspect.

- Training and communications

- The critical aspect was to expand training and communications to provide a broad CriMNet integrated approach to county and state goals and objectives. Shared training, information, and communication were critical to understand difference in data, technology, business practices and methods used across agencies.

- Dedicated staff

- All the CJSIIP/HJIP projects involved more than one agency. The critical aspect was that the resources allocated by each agency had to have the project as a top priority over local agency efforts. In addition, the mind set of the staff had to accept new technologies,

willing to accept cultural changes, and work towards providing deliverables acceptable to CriMNet and shared solutions acceptable to all agencies.

- State initiatives
- The governance body must play and active roll at the state legislature, to implement policies, deliver funding, or implement state initiatives. (Macro Group & Labyrinth Consulting, 2000, p. 3)

13. Summary

Both the SAFE/NEIS and SILS systems are examples of using subject identification methods to create links between disparate criminal justice agency systems. Agencies have the option to search for subject information relationships at both the county and state level. Biometric identification that creates the State Subject Identifier (SID) happens when the subject is booked at the jail. Booking time is where the state verifies information with the FBI's IAFIS system. Minnesota supports a two-tier biometric identification process, one at the state level and one at the federal level. Hennepin County does not include an AFIS system and relies on subject identification information from law enforcement record management systems (FBIID, SID, name, and demographics). Subject criminal records are dependent on both the state and federal biometrics identifiers. Searching on a subjects name and demographics is available but may not return the right results.

Law enforcement agencies have the capability to use 2-FID biometrics identification using mobile devices in the field. The 2-FID systems do not store any information and do not create criminal records based the 2-FID. The units are used to verify identity and retrieve limited information from SAFE/NEIS. SAFE/NEIS also creates pointers to other potential sources of information that resides in independent criminal justice agency disparate systems.

Not all criminal information is linked together by biometrics identification keys. Information can still be dependent on subjects' names and demographics. CriMNet and county systems still provide search capability to criminal justice records based on subjects' names and demographics. CriMNet and the county systems only provide and

index capability to disparate systems. Criminal justice agencies have the responsibility to provide information for updating these index systems with the most accurate information possible. Agencies understand the only unique way to link a subject to their records is through biometric identification used to establish local agency, state, and county identifiers.

Minnesota is participating in the FBI's Repository for Individuals of Special Concern (RISC). This system is part of the FBI's Next Generation Identification (NGI) program. The system allows 2-FID mobile systems to rapidly access an FBI system that houses information for individuals the pose a threat to public safety. RISC houses a subset of the FBI's IAFIS system and includes wanted person information, the Sex Offender Registry, and known suspected terrorists (Advanced Fingerprint, n.d.).

Minnesota maintains criminal justice information in disparate systems and uses a federated [24] query approach to accessing information. In addition, the state and counties have developed and Indexing capability that allows searching across the disparate systems.

B. LOS ANGELES COUNTY BIOMETRICS IDENTIFICATION AND INFORMATION SHARING

1. Los Angeles County Technology Framework Components and Elements

Los Angeles County supports two biometric identification capabilities. First, Los Angeles County provides the Regional Identification System (LACRIS). The system provides subject biometric information to criminal justice agencies within the county. The LACRIS system is integrated with the California State Automated Fingerprint Identification System (CAL-ID). Second, the LACRIS system provides mobile identification capability to officers in the field. The mobile units provide both fingerprint and facial image verification to insure accuracy.

[24] This type of search is sometimes called a federated query. Federation enables end users to issue a query that searches multiple sources and displays results in separate Web parts on a single search results page. For more information, see Microsoft Tech Notes Website http://technet.microsoft.com/en-us/library/bb905377.aspx.

Similar to Minnesota, each agency within the county has the responsibility to maintain its own criminal justice information. However, information sharing within Los Angeles County (and other counties within the state) uses a centralized approach. Information is provided by participating agencies to a central repository system called the Incident Reporting Information System (IRIS). Agencies can use the information for searching, analysis and reporting.

The Los Angeles County Sheriff's Department provides oversight for the LACRIS biometric systems and the Los Angeles Regional Integrated Law and Justice Governance Committee provides oversight for the IRIS system. Policy and technology teams are created and shared between agencies. In addition, the Los Angeles County IRIS system is integrated with the Los Angeles Police Department's (LAPD) centralized repository system and the Regional Terrorism Information and Integration System (RTIIS). Oversight for the information sharing effort between the three systems is managed by a consortium of 45 municipal law enforcement agencies within the county. Figure 10 illustrates the Los Angeles County's Technology Framework for subject identification and information sharing.

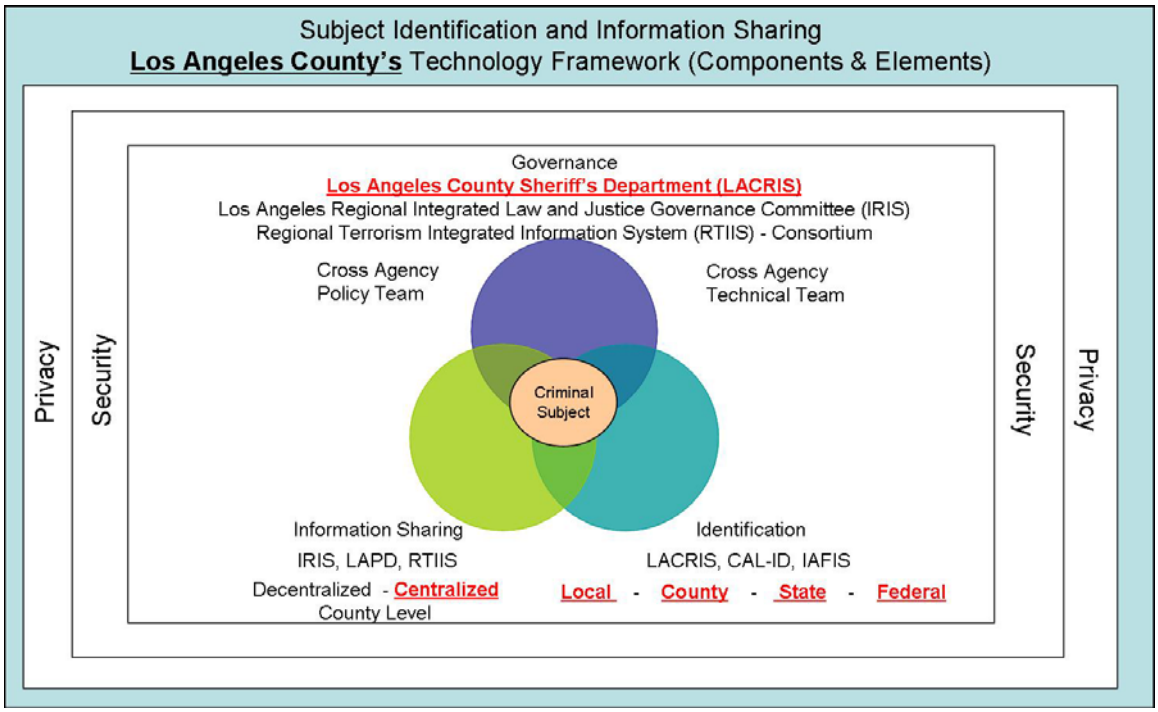

Figure 10. Los Angeles County's Technology Framework (Components and Elements)

2. Los Angeles County Regional Identification System

Los Angeles County covers 4,000 square miles and supports a population of over 10 million residents (Norton, 2009). The county has over 80 cities and unincorporated areas. Law enforcement agencies include the Los Angeles County Sheriff's Department, California Highway Patrol, and over 40 municipal agencies (Norton, 2009). Los Angeles County Regional Identification System (LACRIS) is managed by the Los Angeles County Sheriff's Department (LASD).

This researcher analyzed the LACRIS and its relationship to the California Department of Justice State system (CAL-ID). It should be noted that many counties maintain independent AFIS systems. During the county booking process, the Los Angeles Regional Identification System (LACRIS) AFIS first checks the submitted fingerprints against its own database and then sends a request to CAL-ID to check fingerprints and determine if there is a state record that matches. In addition, CAL-ID sends a request to the FBI's IAFIS system. The process is the same as in Minnesota for checking and creating state and FBI IAFIS records. Again, it should be noted that the FBIID and the state SID [25] are the key identifiers to the subject's records. Names and demographics may not be accurate and are considered aliases. LACRIS receives a response from CAL-ID and from the FBI IAFIS system if available. The LACRIS AFIS system will create a new record if the state does not show a match to a LACRIS record and a County Subject Identifier (CID). The available identifiers and associated subject information is sent back to the jail during booking.

3. Los Angeles County Sheriff's Department Mobile Identification System

The Los Angeles County Sheriff's Department (LASD) is the largest Sheriff's Department in the world and supports nine community colleges, 48 Superior Courts, 19,000 inmates housed in correctional facilities and the residents of the county. The

[25] Minnesota, California, and many other states use the same SID acronym to represent the state subject identifier. It should be noted that the identifier is unique within the state. The identifier does not match across states.

department has 9,500 sworn officers and 7,200 non-sworn personnel (SEARCH, 2009, p. 2). LACRIS has implemented mobile 2-FID identification capability using Cogent "Bluecheck" devices provided to field officers (of any agency in the county) and has documented success cases.

a. The Story of Changing Appearance to Avoid Arrest

The following is an example of how mobile identification technology was used to determine the true identity of a homicide suspect using false identification.

> March 20, 2008—An LASD Homicide Detective reported that he had been investigating a murder in Palmdale and identified three suspects. He had arrested two of them and was actively searching for the third. After about three weeks, the detective got a call from an LAPD officer informing him that the third suspect was in custody. The LAPD officer working near downtown had stopped the suspect for possible narcotics activity. The suspect (who had changed his appearance dramatically) gave a false name. The LAPD officer made use of a Bluecheck device and within minutes took the suspect into custody after acquiring a positive identification and conducting a warrant check. (Norton, 2009)

b. The Story of Leaving and Re-entering the Country Using a Different Name to Avoid Arrest

The following is an example of a suspect who fled the country and returned with new identification documents. The suspect's true identity was determined using mobile biometrics technology.

> January 29, 2008—Huntington Park PD stopped an individual who gave a false name and date of birth. After using the Bluecheck device to positively identify the individual it was determined that he had a felony domestic violence warrant. The suspect had fled the country after the warrant was issued and re-entered after several years with a different name and date of birth to avoid arrest. (Norton, 2009)

c. Multi-Modal Identification Implementation

Currently, the system only accesses the LACRIS AFIS system. However, a pilot project in several small counties is underway with the California Department of

Justice that will provide search capability into the state's CAL-ID system. A typical hit will occur within five minutes (LASD) and six to eight minutes through the CAL-ID system (McCombs, 2009). The LACRIS AFIS system houses approximately 10 million records. The CAL-ID system houses 19-plus million persons records (McCombs, 2009).

The LACRIS program has deployed over 2,300 multimodal devices throughout the law enforcement agencies of the county that include facial recognition and fingerprint identification capability. The devices include Blackberry PDA's and biometric software running on Mobile Data Computers located in patrol cars (L. Norton, personal communication, November 3, 2009). Units have been deployed to homicide detectives, coroner staff, and officers riding public transportation systems (Norton, 2009).

Within the county, officers only use the devices when an arrest is underway or probable cause may lead to an arrest. In addition, officers are restricted to using the devices only when a subject has no government issued identification or the officer believes the documents are fraudulent (Norton, 2009). When the mobile identification device accesses the LASD AFIS system, if a record is found the system returns the subject's name, photograph, and the latest arrest information. If no record is found, a "no hit" indicator is returned to the requesting officer (LASD Technical Services Division, 2007). If the situation warrants an arrest, the officer will take the subject in for booking.

The multimodal system can transmit a subject's facial image to the DataWorks mugshot system. The facial recognition software on the system can search through the seven million images and return a response in fifteen seconds. The system returns several possible matches from the highest possible match to the lowest. Final verification using facial images rests with the officer. The system also provides image recognition capability against the two million scars, marks, and tattoos stored within the system. Using fingerprints, facial image, and body marking photos can all be used to insure verification of the subject. Once verification is complete, the same information is returned as with the AFIS system (Dataworks, 2008). Both the AFIS and DataWorks mugshot systems receive their information during the booking process.

The LACRIS booking system sends the county's subject identifier, name, and demographics stored in the AFIS system to the arresting agency's record management system. Each police department sends their respective subject information records to the Incident Reporting Information System (IRIS), discussed in the next section. The quality of identification information is critical to the county's information sharing program.

Future plans include expanding LACRIS to access the county wide warrant system, other county AFIS systems, the California State Department of Justice AFIS system, the FBI's IAFIS biometrics system, and the FBI's Repository for Individuals of Special Concern system. The expectation is that each system will be contacted during a single transaction request from an officer. Figure 11 illustrates the flow of information for an officer identification request within LACRIS. In addition, the red circle identifies the link into the LASD County IRIS law enforcement information sharing environment.

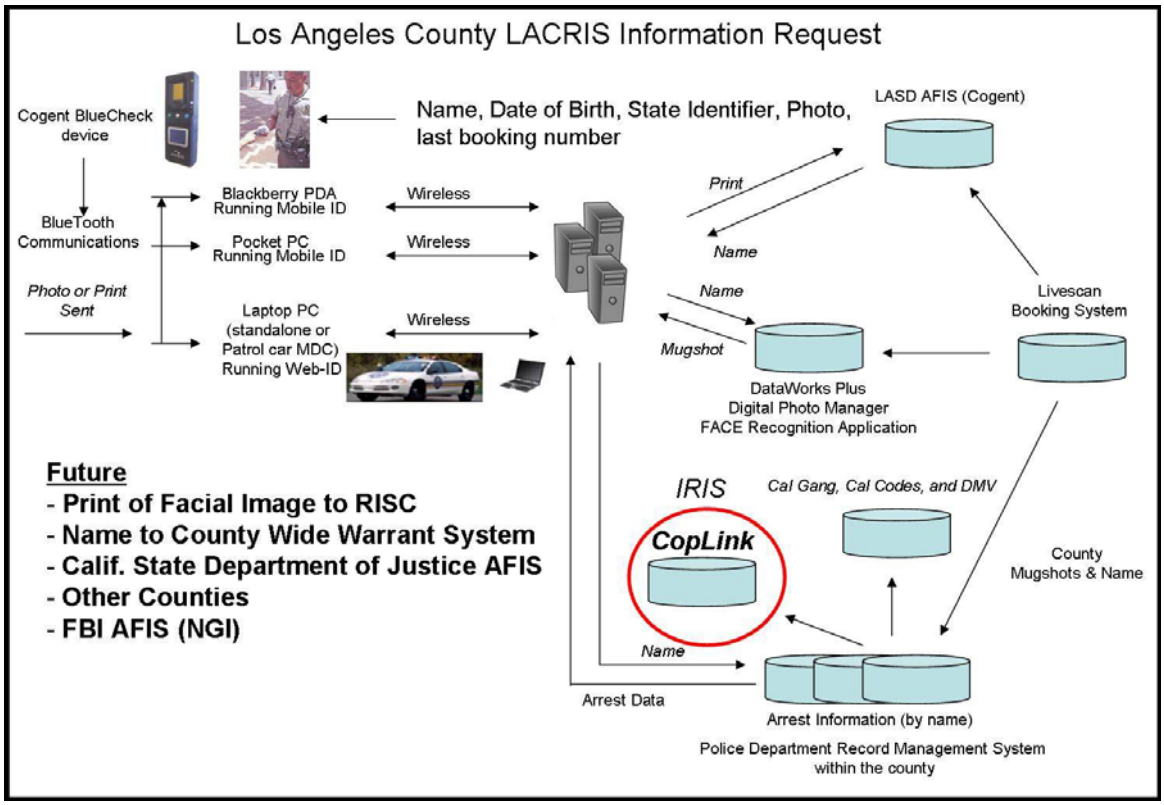

Figure 11. LACRIS Information Context Flow Diagram

The LACRIS mobile identification usage report for 2009 showed PDA devices were used by officers 35,772 times with a 44 percent positive hit rate for identifying subjects (LACRIS Mobile ID, 2009). Units used in patrol car laptops were used 63,146 times with a 40 percent positive hit rate for identifying subjects (LACRIS Mobile ID, 2009). Officers being able to verify a subject's identification four out of 10 times where a subject's identification is in question, is a significant improvement (LACRIS Mobile ID, 2009). In addition, a positive hit means the subject had a prior record on file from a previous arrest. Prior to using the devices, these subjects might not have been identified.

4. Los Angeles County Regional Information Sharing

In 2006, the Los Angles County Sheriff's Office implemented the Incident Reporting Information System (IRIS) using the Coplink data warehouse capability. The Coplink data warehouse takes information from disparate data sources, converts the information into a common language that can be integrated into a central repository. Searches are conducted against the central repository, thereby eliminating the need to log into multiple systems.

The system was the first county's data warehouse for gathering criminal justice agency information from disparate systems. IRIS contains over 43 million records (SEARCH, 2009, p. 4). The data warehouse capability extends beyond accessing subject records. The data warehouse can also store information about criminal justice events, vehicle information, locations, and more. The data warehouse technology is capable of building relationships between informational records based on specific key information located in documents. The system can build relationships to arrest documents, incident reports, citations, warrants, drivers' licenses, motor vehicle registrations, firearm permits and more. Coplink data warehouses can be linked together making it possible to search data from other jurisdictions (SEARCH, 2009, p. 8).

IRIS was implemented during the same time period that the Los Angeles Police Department (LAPD), San Diego County, Orange County, and Imperial County were implementing the same data warehouse solution with their respective law enforcement

agencies. The Los Angeles County Police Chiefs Association recognized the need to tie together the LASD and LAPD efforts and expand the information sharing opportunity to regional municipal law enforcement agencies. The Los Angeles County Police Chief's Association established the Regional Terrorism Information and Integration System (RTIIS). A consortium of 45 municipal law enforcement agencies participates in the RTIIS data warehouse system (SEARCH, 2009, p. 2). Each law enforcement agency participates and contributes information from their respective record management systems into one of the data warehouse repositories. RTIIS was also formed to coordinate information sharing across other regions, states, and eventually with federal law enforcement systems.[26]

Relating information in a data warehouse allows analysis of information from all participating agencies in one database. Law enforcement can collaborate on cases and analyze information without jurisdictional boundaries. In addition, to information analysis, data warehouse systems nurture cross jurisdiction collaboration on solving cases (SEARCH, 2009, p. 5). Figure 12 illustrates the data warehouse sources connected (or planned for the future) to RTIIS.

[26] Law enforcement agencies with the Department of Homeland Security and the Department of Justice are working on a program for information sharing between federal, state, local, and tribal agencies. Discussion about information sharing initiatives with other states and federal agencies is outside the scope of this thesis.

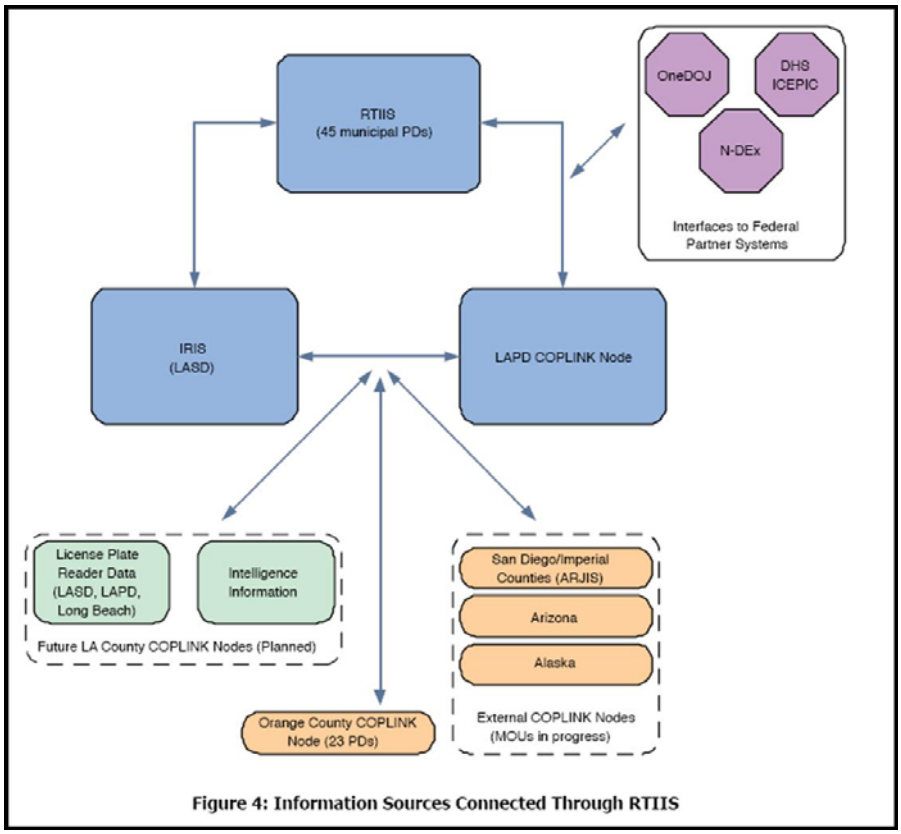

Figure 12. Information resources connected through RTIIS (From SEARCH, 2009, p. 11)

5. Los Angeles County Governance

Figure 13 illustrates the Los Angeles County Sheriff's Department Organization.

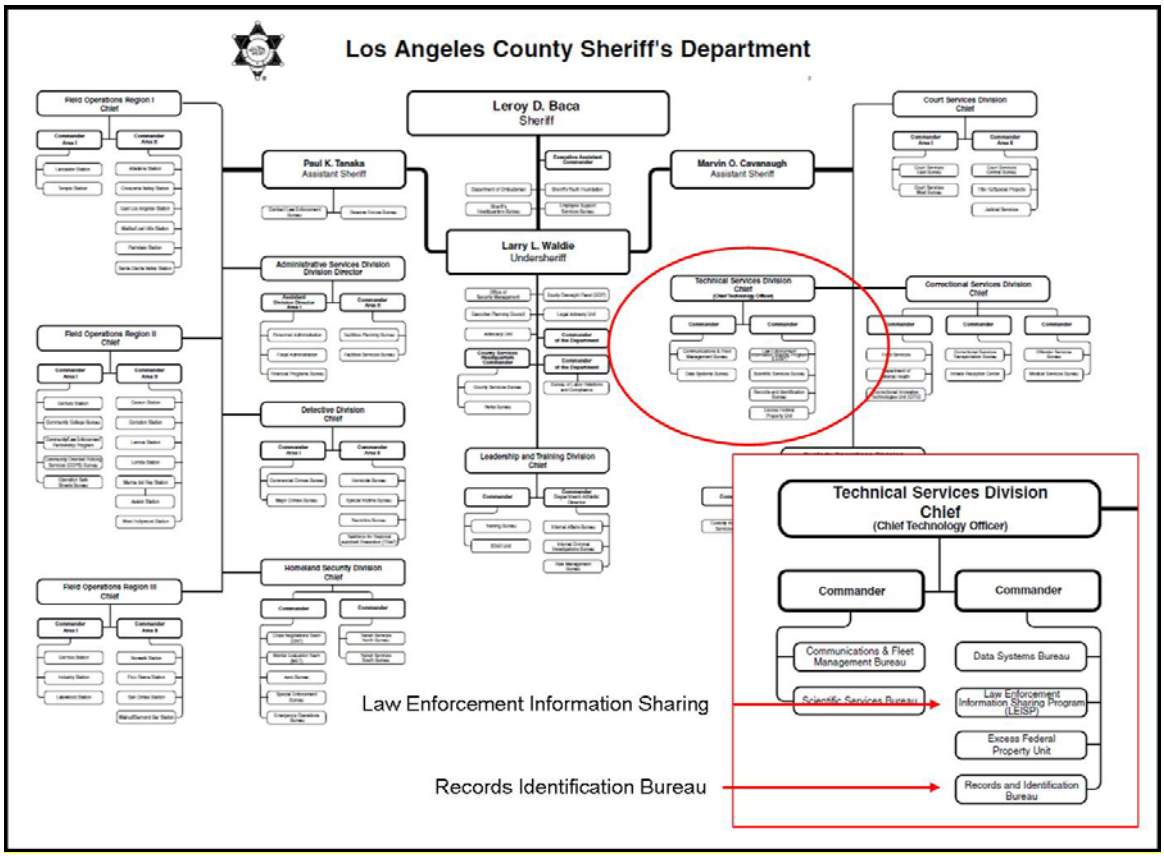

Figure 13. Los Angeles County Sheriff's Department Organization Chart (From Los Angeles County Sherriff's Department, 2008)

The Los Angeles County Regional Identification System (LACRIS) and the Incident Reporting Information System (IRIS) is managed by the Los Angeles County Sheriff's Department (LASD). Oversight and funding for LACRIS is authorized by the Remote Access Network Board (RAN) (LACRIS, n.d.). The RAN Board is chaired by a member of the County Board of Supervisors. The remaining board members include law enforcement executives. The board seeks and authorizes funding along with establishing the direction for the LACRIS systems. The RAN Board also supports a technical subcommittee that provides technology needs and recommends hardware and software. The Technical Subcommittee is chaired by the Sheriff's CAL-ID representative (Los Angeles County Records, n.d.).

Information sharing is managed by the Los Angeles Regional Integrated Law and Justice Governance Committee that includes LASD, LAPD, and three municipal police departments participating in the RTIIS. The function of the governance committee is to oversee law enforcement participation in information sharing. The principle method for participation includes memorandums of understanding (MOUs) between agencies and the process to monitor compliance. The purpose of the agreements is to define participation guidelines and address issues such as data ownership and usage, confidentiality and liability, and indemnification (SEARCH, 2009, p. 8). The Governance Committee provides oversight to policies and use of technology through the MOU agreements.

The California Department of Justice is leading a coordinating an effort to develop a statewide information sharing initiative. Both the LACRIS biometrics system and the IRIS information sharing system are included in the effort. The goal is to produce a strategic plan for the state (NGA Center, 2009, p. 11).

Within Los Angeles County, the IRIS law enforcement information sharing program is leading the effort in regards to information sharing across all criminal justice agencies. Currently, many independent systems exist across the courts, prosecutors, Department of Corrections, probation, and other agencies. The only access is through the independent legacy systems. There is no effort under way for data sharing. However, IRIS is being considered for expanding information sharing across these agencies (C. Cahhal, personal communication, February 7, 2010).

6. Los Angeles County Best Practices

An assessment of lessons learned from the RTIIS information effort was conducted by SEARCH, the National Consortium of Justice Information and Statistics in 2009. The lessons learned identified some key best practices. Establishing representative governance and partnerships from participating agencies is critical for any multiagency information sharing programs to succeed. An acceptable governance model must be put in place along with implementing formal information sharing agreements (SEARCH, 2009, p. 16).

Leadership plays a significant part in implementing, funding, and gaining acceptance. Leadership at the program level requires one agency to take a leading role. The agency must have the technical expertise, business knowledge, and management experience required for a multiagency program. Leaders must facilitate decision making across agencies and advocate the use of new systems and technologies at the highest levels of government (SEARCH, 2009, pp. 16–17).

Success is dependent on developing a culture for information sharing by users of the system. Agencies have different processes and systems and users need to be positive about adapting to new ways of doing business. Officers and deputies must recognize that they are part of a regional effort that benefits their agencies as well as law enforcement across the region. Participating in training, round table discussions, and contributing success stories that support the adoption of the program was successful in building relationship networks across agencies. In addition, using real cases for marketing efforts gained support from both government officials as well as the public (SEARCH, 2009, pp. 16–17).

The Los Angeles Regional Integrated Law and Justice Governance Committee conducted Joint Application Requirements meetings with 13 law enforcement agencies (Los Angeles Regional, 2005, p. 2). Early on in the process, the team identified that defining a phased approach for deliverables was a requirement. The best practice was to break the project up into meaningful and manageable phases. Each phase must be long enough to provide business value and support acceptance of the program but short enough to deliver quick wins and build support for the program. Each phase required managing user expectations by developing a centralized communications plan. Information was provided that was concise, concrete, and focused on the "wins" (Los Angeles Regional, 2005, pp. 30–32). In addition, the requirements called for establishing technology standards for information sharing that are compatible with federal government standards (Los Angeles Regional, 2005, p. 20).

7. Summary

Los Angeles County Sheriffs Department supports a large community that required the development of the LACRIS identification system to support the county's law enforcement agencies. For subjects being booked into the county jail system, the process is similar to Minnesota with the exception that Los Angeles County has implemented an AFIS system. At booking time, verification or creation of biometric identifiers occurs at the county level, state level, and the FBI level (FBIID). The county supports a three-tier biometric identification process. Los Angeles County, also similar to Minnesota, relies on subject identification information provided by law enforcement record management systems (FBIID, SID, CID, name, and demographics) for information sharing. Subject criminal records are dependent on the county, state, and federal biometric identifiers.

Los Angeles County provides search capability across disparate law enforcement record management systems using the FBIID, SID, CID, name, and demographics. In contrast, unlike Minnesota, the county does not provide a separate indexing and pointer system based on subject identification keys to the information. Searching on a subject's name and demographics is available but may not return the right results.

Los Angeles County also provides law enforcement agencies the capability to use 2-FID and facial image biometric identification using mobile devices in the field. Similar to Minnesota, the multi-modal devices do not store any information or create records. The units are used to verify identity and retrieve limited identification information. The subject's FBIID, SID, CID, name, and demographics can be used to search through independent systems or used to search the IRIS data warehouse system. The IRIS system uses the subject's biometric identification keys, name and demographics to link together subject criminal justice information across jurisdictions. Coplink does not currently provide any biometrics capability in the LASD system (L. Norton, personal communication, December 30, 2009). IRIS is dependent of the information provided by criminal justice agencies.

The multi-modal identification systems are limited to accessing the LASD identification system. Future plans will allow additional access to CAL-ID and the FBI's Repository for Individuals of Special Concern System (L. Norton, personal communication, February 17, 2010).

Criminal justice agencies have the responsibility to provide information to the IRIS system with the most accurate information possible. Agencies understand the only unique way to link a subjects to their records is through biometric identification used to establish local agency, county, state, and federal identifiers. Los Angeles County maintains criminal justice information in disparate systems, but is moving forward with a centralized data warehouse capability.

C. WISCONSIN DEPARTMENT OF JUSTICE BIOMETRICS IDENTIFICATION AND INFORMATION SHARING

1. Wisconsin Technology Framework Components and Elements

Wisconsin's biometrics identification program is the state's Automated Fingerprint Identification System (AFIS) and the mobile fingerprint biometrics identification system (FAST-ID). Both systems provide subject identification capability to all agencies across the state.

Similar to Minnesota, Wisconsin criminal justice agencies maintain and manage their own information. Information sharing capability is provided by the state's Transaction Information for Management of Enforcement (TIME) system. The TIME system provides access to disparate systems across agencies and consolidates the information for presentation and reporting (Transaction Information, 2009).

The Department of Justice, managed by the State Attorney General, provides oversight for both the biometric identification and information sharing capability. The Crime Information Bureau within the Department of Justice provides policy and technology support. Figure 14 illustrates the Wisconsin's Technology Framework for subject identification and information sharing.

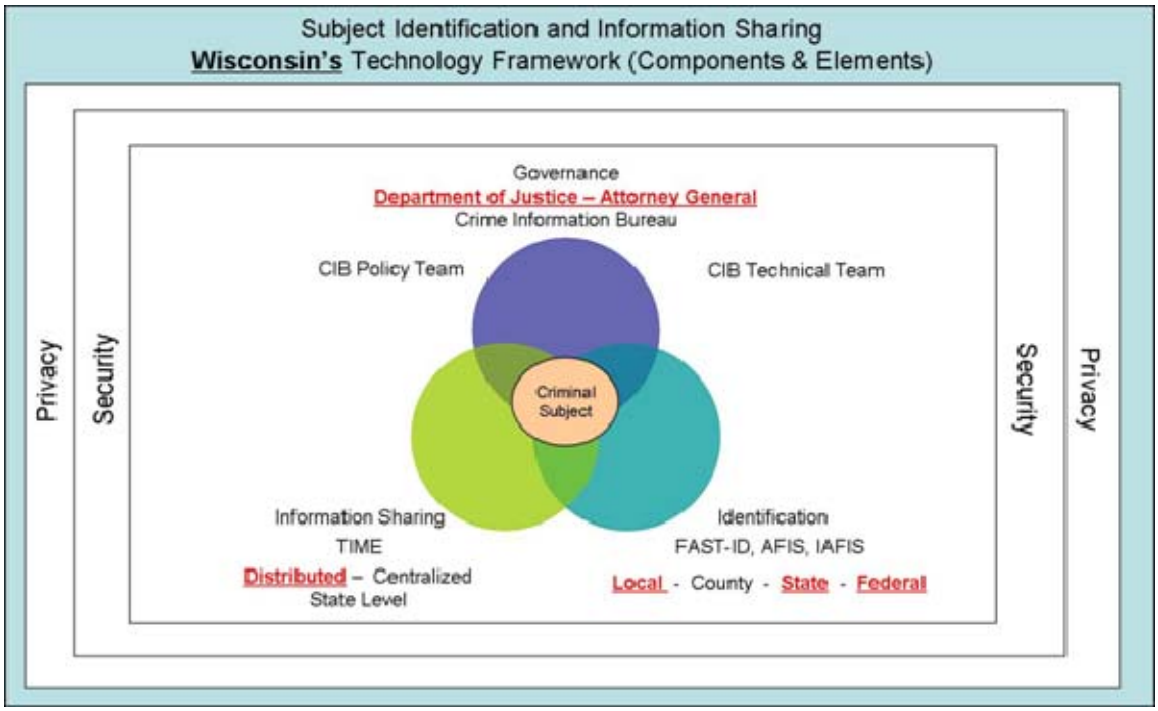

Figure 14. Wisconsin's Technology Framework (Components and Elements)

2. Wisconsin Department of Justice Fast ID

Wisconsin has a population of 5.3 million residences living in 72 counties that cover 65,000 square miles (Wisconsin Department, 2002). The State Transaction Information for Management of Enforcement (TIME) system is being used by 625 agencies that includes 580 traditional law enforcement agencies (two tribal), 16 federal agencies, 15 state agencies, and six other agencies associated with criminal justice support or technology services (Crime Information Bureau, 2008, p. 7). There are approximate 17,300 sworn officers providing public services (P. Collins, personal communication, February 22, 2010).[27]

The Wisconsin AFIS system operates similar to the Minnesota and Los Angeles County. Fingerprints of a subject are taken at the time of booking and checked against the state AFIS system and the FBI's IAFIS system. Like other states, the Wisconsin state

[27] Officer count as per system billing information.

AFIS system may submit a request to the FBI's IAFIS system for print verification; however, the FBI's system may reject the request based on the quality of the fingerprints and data submitted. Between January 1, 2009 and July 31, 2009 the FBI rejected 3.56 percent of the submissions from the Wisconsin AFIS system (Wisconsin criminal, 2009, p. 23). Wisconsin is similar to Minnesota in that the state supports a two-tier biometric identification process, one at the state level and one at the federal level.

Wisconsin has implemented a 2-FID mobile biometrics identification capability called "Fast ID." The system captures the index finger prints of a subject and searches the state AFIS system. If a match in found, the state identifier (SID), subject's demographics, and the local person identifier (LID) is returned to the requester. If no match is found, the system sends a "no match found" indicator. Fast ID does not store any biometric information (WDOJ, 2004, p. 2). This is similar to both the Los Angeles County Regional Identification System and the Minnesota CriMNet field officer identification system; however, there is an important difference; the Wisconsin AFIS system does not store names. Therefore, the Fast ID system does not return the subjects name (WDOJ, 2004, p. 3). However, a project is underway to upgrade the state AFIS system to include a subject's name. When the project becomes operational, AFIS will return the subject's AFIS master file record name back to the 2-FID requester (P. Collins, personal communication, February 22, 2010).

If the Fast ID system returns the state identifier, the requestor will need to access the Wisconsin Transaction Information for Management of Enforcement (TIME) System using the state identifier to retrieve additional information. There is no relationship between the Fast ID system and the TIME system (P. Collins, personal communication, January 12, 2010).

3. Wisconsin Transaction Information for Management of Enforcement System

The TIME [28] system provides information sharing capability across law enforcement agencies. The system is similar to Minnesota's system in that information is maintained by the agencies and the TIME system provides visibility across the disparate systems. However, the TIME system differs in that it does not use an index database to consolidate keys and create pointers to subject records (P. Collins, personal communication, January 12, 2010).

In addition to serving the state and local law enforcement agencies with information sharing, the TIME system provides information from other data sources. The system accesses information from the Department of Transportation, Department of Corrections, and the Department of Resources. TIME also provides Minnesota with access into federal criminal information systems (C. Bauer, personal communication, December 7, 2009). In 2008, the TIME system processed over 74.5 million transactions (not include outside internet system access). In addition, 28 million of those transitions were subject searches (Crime Information Bureau, 2008, p. 52). The TIME system connects to approximately 9,600 criminal justice computers in Wisconsin and over 400,000 computers located nationwide and in Canada. The system contains over 1.2 million subjects arrest and disposition records (Crime Information Bureau, 2008, p. 2).

4. Wisconsin Governance Model

Governance for the AFIS, Fast ID, and the TIME systems are the responsibility of the Crime Information Bureau (CIB). The Bureau is part of the Wisconsin Department of Justice (DOJ) that is managed by the State Attorney General. Figure 15 illustrates the Wisconsin Department of Justice Organization.

[28] Minnesota is implementing a replacement system for TIME called eTIME. For more information, see http://www.doj.state.wi.us/les/TIME/eTIME.htm for more information.

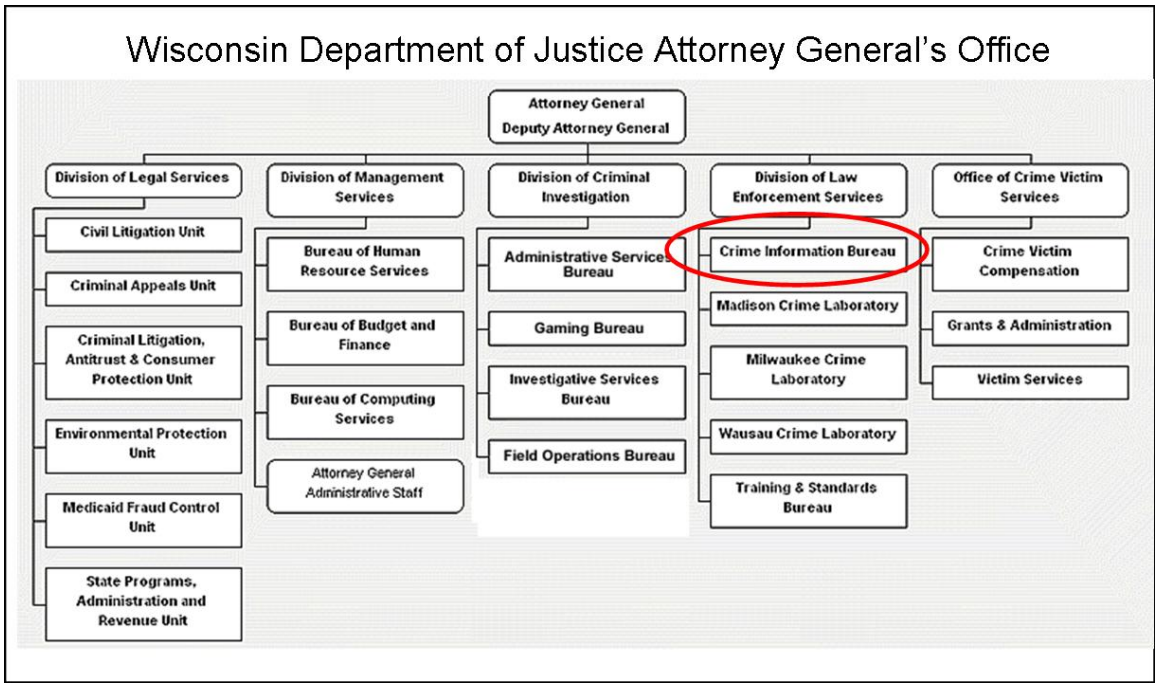

Figure 15. Wisconsin Department of Justice Organization Chart (From DOJ Organization Chart, n.d.)

The Department of Justice provides the legal advice and support for agencies across the state. The department oversees the operations of the state's legal services, criminal investigations, law enforcement systems and services, and crime victim services. Within the DOJ, the Division of Law Enforcement Services (DLES) provides the technology and services required by law enforcement agencies across the state. DLES is responsible for all systems central to state operations. In addition, DLES is responsible for law enforcement training and establishing operational standards (Agency Division, n.d.).

The Crime Information Bureau (CIB) is a Division of Law Enforcement Services.

CIB is responsible for the operation and management of the TIME system, the state's Criminal History System, the Automated Identification Fingerprint System, and other state law enforcement systems (Law Enforcement Services, n.d.).

State statutes 165.83(2)(a) and 165.84(1) determine when fingerprints are required for subjects contacted by law enforcement and taken into custody. The statues also give

the option to the Attorney General to define addition offenses that require fingerprinting. In addition, the statues finger-printable offenses exist for subjects who have been issued summons or citations. For any offenses requiring fingerprinting, statute 970.02(7) mandates fingerprinting must be completed before a subject appears before a judge (Wisconsin Crime Information Bureau, 2010). Using the Fast-ID system is used by officers in the field when an arrested person with an unknown or questioned proof of identification exists. Also, the system can be used prior to entering errant arrest information into an agency's record management system (WDOJ, 2004, p.3).

D. VERMONT DEPARTMENT OF PUBLIC SAFETY BIOMETRICS IDENTIFICATION AND INFORMATION SHARING

1. Vermont Technology Framework Components and Elements

Vermont's biometrics identification program is the state's Automated Fingerprint Identification System (AFIS). The state does not have a mobile biometrics identification capability.

Vermont is similar to Minnesota and Wisconsin. The state criminal justice agencies maintain and manage their own information. Information sharing capability is provided by the Vermont Justice Information Sharing System (VJISS). Within the VJISS system, there is a Law Enforcement Data Sharing Initiative (LEDSI) specific to law enforcement information sharing. Both the VJISS and LEDSI systems provide access to disparate systems across agencies and consolidate the information for presentation and reporting.

VJISS is managed and governed by the Department of Public Safety with support from other state agencies. Governance includes both policy and technology. The Department of Public Safety facilitates meetings between the agencies for decision making. Figure 16 illustrates Vermont's Technology Framework for subject identification and information sharing.

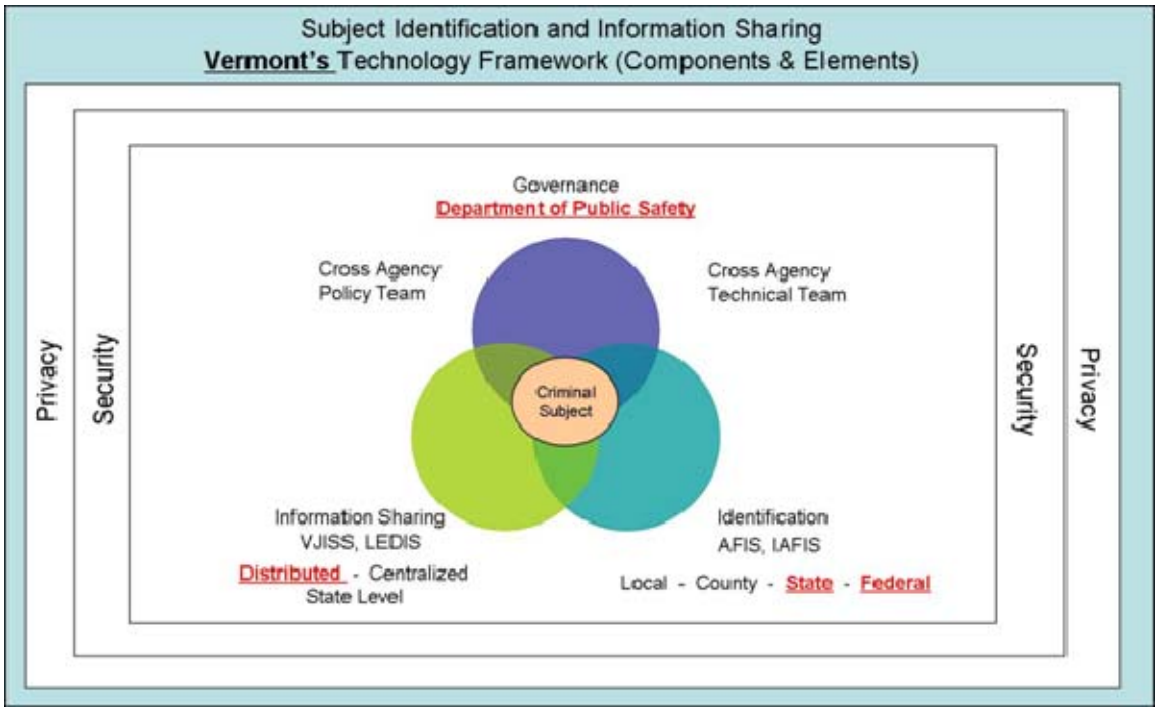

Figure 16. Vermont's Technology Framework (Components and Elements)

2. Vermont Justice Information Sharing System

Vermont serves a population of 621,000 over 2,000 square miles (U.S. Census Bureau, 2008). The state has 51 municipal law enforcement agencies, 14 Sherriff's Departments, and the Vermont State Police (Vermont Department, 2008). The state has a unified court system, statewide corrections system, police record management systems,[29] centralized states attorneys, and a common shared network (VJISS Strategic Plan, 2009, p. 1).

The Vermont Justice Information Sharing System (VJISS) is an ongoing program to provide information sharing capability across criminal justice agencies in Vermont.

VJISS is managed and governed by the Department of Public Safety, State Attorneys and Sheriff's, Department of Motor Vehicle, Department of Corrections, Court

[29] Ninety-three percent of the police record management systems are provided by the same vendor (Aumand, 2008a p. 1).

Administrators Office, and the Defender General Office. Governance includes both policy and technology. The Department of Public Safety facilitates meetings and activities (VJISS Strategic Plan, 2009, p. 1).

Vermont law enforcement agency officers do not have the capability to use biometrics identification in the field. Subject biometric identification only occurs during the subject booking process. However, law enforcement agencies participate in the VJISS information sharing program (F. Aumand III, personal communication, February 11, 2010).

The Law Enforcement Data Sharing Initiative (LEDSI) is a program within the VJISS program. Representatives from law enforcement agencies are responsible for implementing information sharing between law enforcement systems. In addition, the LEDSI representatives work with other agencies within VJISS to develop information sharing capability between other criminal justice agencies. (VJISS Strategic Plan, 2009, p. 1).

The VJISS system provides two capabilities for law enforcement agencies. First the system will allow searching police agency systems based on a subjects name, vehicle information, and agency incidents (including incident number). The system searches through the disparate systems based on the user request and returns consolidated information.[30] The system does not store any information. Second, there is a separate server and database that captures subjects' names, vehicle identification information, and agency incidents (including incident number). The system delivers analysis capability for information provided by the law enforcement disparate systems. This system will have restricted role based usage, limited access, and regularly audited (Privacy Policy, 2008, p. 3).

[30] This type of search is sometimes called a federated query.

3. Vermont Best Practices

a. Privacy Impact Assessment and Privacy Policy

The Vermont LEDSI program completed a public impact assessment in 2008. The impact assessment is an excellent example analyzing information from a questionnaire to establish guidelines for developing policies that meet privacy concerns. Every state will have similar questions, but answers will vary. For the purpose of this thesis, this researcher examined the Vermont VJISS Privacy Impact Assessment and the established Vermont VJISS Privacy Policy.[31] The intent is to show the importance of an assessment and policy necessary for the technology framework, not to develop a deep understanding of privacy issues and policies. The impact assessment included the following questions that the VJISS program had to address:

- Information
  - What information will be collected and stored?
  - From whom is the information collected?
  - What privacy risks exist and how will they be mitigated?
- Purpose
  - Why is the information being collected?
  - What legal authorities, arrangements, agreements authorize the collection and use of the information?
  - What privacy risks exist and how will the risks be mitigated?
- System use
  - How, when, and by whom will the system be used?
  - Will the system analyze the information?
  - How will the results be used and distributed?
  - Who has responsibility for information accuracy?
  - How long will the information be retained?
- Information sharing and disclosure

[31] Privacy policy is a legally binding notice of how an agency handles an information contributor's personal data. The privacy policy should contain details about collecting information and secondary uses of data, including how information is shared with third parties and who those third parties are (U.S. Department of Justice, 2008, p.1).

- What agencies will be authorized to share information?
- What information will be made available within each agency?
- How will the information be transmitted or disclosed?
- What privacy risks exist and how will they be mitigated?

- Technical access and security
  - What user groups will have access to the system?
  - Will contractors be allowed to have access?
  - Does the system use "roles" to assign access privileges?
  - How and who will provide access administration?
  - How will access assignments be verified?
  - What security policies, audit measures, and technical safeguards be implemented?
  - What privacy risks exist and how will they be mitigated? (Aumand, 2008a, pp. 3–8).

The privacy assessment was used to develop the VJISS privacy policy. The Vermont Privacy policy details specific requirements that address privacy concerns. The following outlines information included in the Vermont VJISS Privacy Policy:

- VJISS purpose and benefits
- Compliance with privacy and civil rights laws (state and federal)
- Agency transparency and accountability
- Definition of the system
- Operational policies
- Seeking and retaining information
- Information usage, validity, reliability
- Information classification based on limitations, access and disclosure restrictions
- Information collation and analysis
- Public access to information, usage, and change management
- Accountability of activities
- Enforcement of policies
- Agency agreements
- Training (Aumand, 2008b, pp. 2–17).

V. FINDINGS

A. ARIZONA PROPOSED TECHNOLOGY FRAMEWORK FOR LAW ENFORCEMENT IDENTIFICATION AND INFORMATION SHARING

This researcher found similarities in the technology framework across the states researched. In each state, success depended on three primary components, subject identification and linkage to criminal justice records, information sharing with visibility across jurisdictions, and governance to support policy and technology requirements. Each component recognizes the important in maintaining information security and establishing privacy policies. Figure 17 illustrates the proposed Arizona technology framework for subject identification and information sharing based on leveraging current programs within the state and similarities across the researched states.

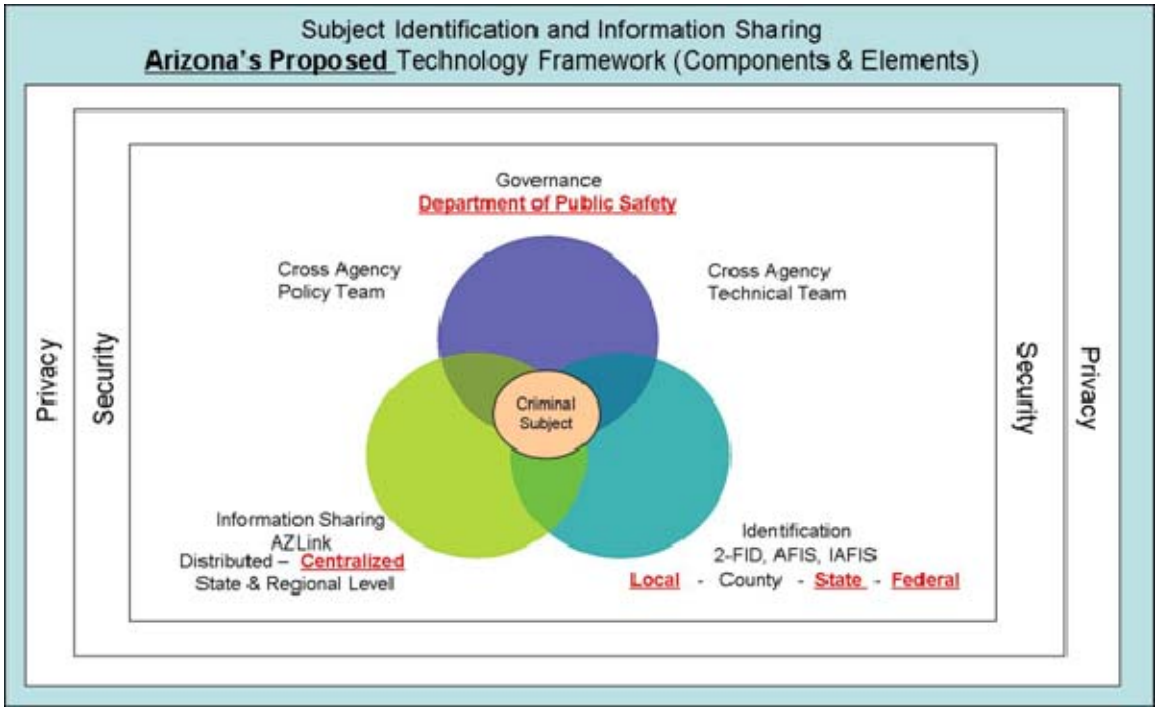

Figure 17. Arizona's Proposed Technology Framework (Components and Elements)

1. Subject Identification Comparative Analysis

This researcher found that each state follows the same guidelines for creating subject biometric identifiers. The only time subject biometric identifiers are created is during the jail booking process. In addition, during the booking process is the only time a state can request the FBI to create a federal subject identifier (FBIID). Arizona follows the same processes as the states researched. The only variation to this process is in Los Angeles County. The Los Angeles County Sheriff's Department creates a county subject biometric identifier (CID) in addition to a SID and an FBIID.

Minnesota and Wisconsin law enforcement and criminal justice agencies use wireless mobile biometric identification systems to validate a subject's identity against the state's biometric identification system. Wireless mobile identification systems are under review in Arizona, but not currently being deployed. Los Angeles County has also deployed mobile wireless capability within the county. The system validates a subject's identity against the county biometric identification system. The county has plans to integrate with the state's biometric identification system in the near future. Vermont has not deployed a mobile identification capability. Minnesota is the only state (as part of this research) that is the process of extending the mobile identification capability to validate subjects against the federal RISC system (currently, the results only go back to the state AFIS system and not to the field mobile units (C. Rhoades, personal communication, February 19, 2010). These systems do not store or create biometric identifiers; the systems are only used to validate identity.

2. Information Sharing Comparative Analysis

In each of the states researched, there is a struggle between maintaining agency independence and the need to integrate information for the good of the states and the nation. Some states believe information should be maintained and managed at the local agency level with controlled access for information sharing at the primary source; information is provided through a distributed access capability. Other states believe

maintaining and managing information is also the responsibility of the local agency, but information can be contributed to a repository for other agencies to use under a controlled data usage agreement.

Minnesota supports a county and state approach to indexing subject identifiers that point to distributed disparate criminal justice information systems. The indexing system is unique in that it also supports tracking subject events as the criminal moves through the justice system. A state system is used to access the primary sources of information that remain under the control of each agency.

The Los Angeles County Sheriff's Department supports information sharing using a centralized data warehouse approach. Each agency contributes criminal justice information to a central repository for the benefit of other organizations. This is a shift in cultural thinking. Primary agency information still resides with the local agency, but the information is now released to be used by other agencies. Agreements are critical to controlling how the information will be used in order to protect the agencies interests.

Wisconsin and Vermont use a distributed information sharing approach similar to Minnesota; however, Wisconsin and Vermont do not provide an integrated indexing pointer system. Both states provide a system to their respective agencies to access information from disparate agency systems. Wisconsin and Vermont support agency control of their own information.

Arizona supports a centralized information sharing approach similar to Los Angeles County. However, some counties have deployed new systems that access disparate agency systems. Integrating the two concepts will be a challenge for information sharing across the state.

Regardless if a state uses a distributed or centralized approach to information sharing, access to the right information and accurate information at the right time is critical for law enforcement and criminal justice agencies.[32] With the availability of

[32] The National Consortium for Justice Information and Statistics compared the advantages and disadvantages to information sharing using centralized, distributed, or indexed approaches (SEARCH, 2008, p.27).

larger sets of subject information, accurate retrieval of all pertinent subject information becomes a necessity. Visibility to the right information is dependent on validated biometric subject identifiers. As stated earlier, using a subject's name and demographics are not acceptable in a large information sharing environment. The Verify Identify Pyramid (VIP) in Figure 18 illustrates how combining biometric identification keys (federal, state, county, and local) can yield accurate access for subject information across a vast amount of available information.

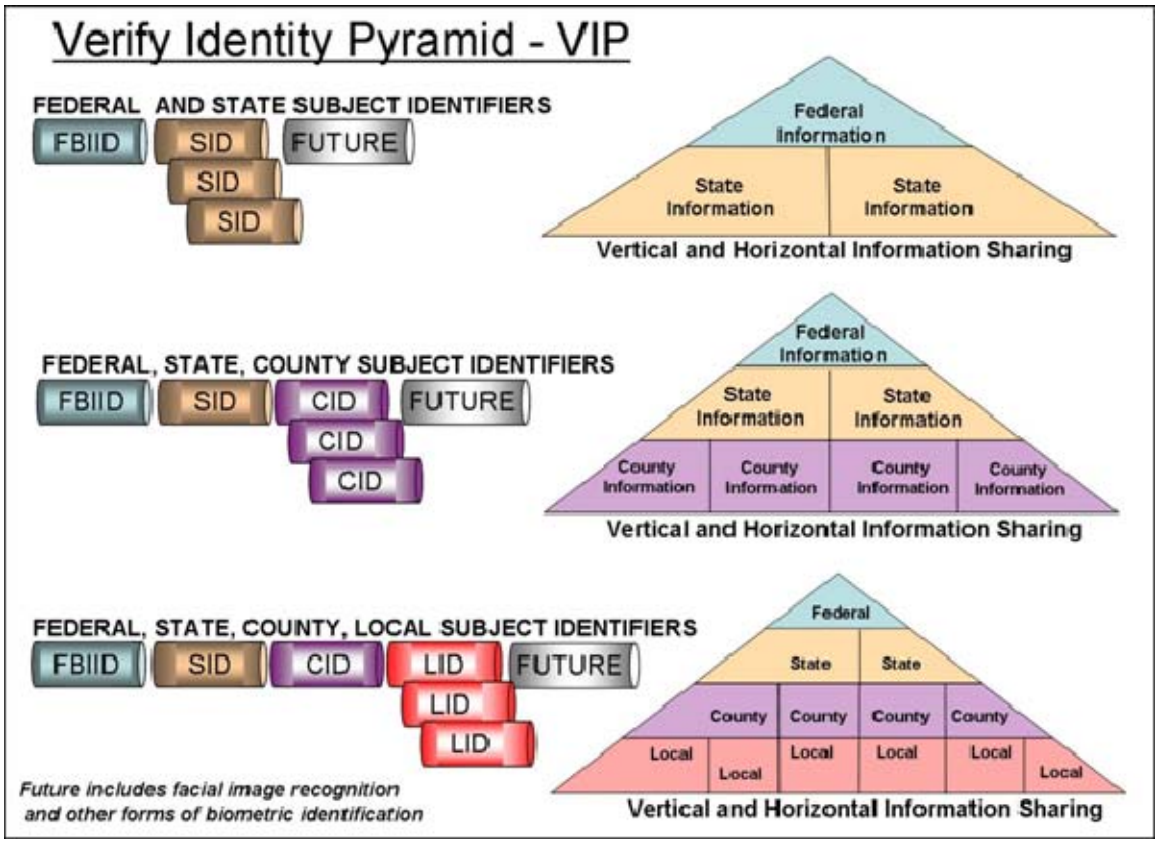

Figure 18. Verify Identity Pyramid—VIP

3. Governance Comparative Analysis

This researcher analyzed the governance structures in Minnesota, Wisconsin, Vermont, and Los Angeles County. The focus was to identify the organizational structure along with roles and responsibilities necessary to support both policy and technology requirements.

Minnesota and Wisconsin have a governance structure at a high level within each state. Both states established governance structures in three areas. First, leadership at the highest level necessary to establish direction, create or change polices that impact statutes, and deliver funding sources through legislative action. Both states created state policy groups and technology groups required to implement systems. Minnesota differs from Wisconsin in that governance ultimately falls under the responsibility of the Department of Public Safety and then to the governor. Governance in Wisconsin is the responsibility of the Department of Justice headed by the Attorney General. This researcher believes the reporting structure has disadvantages and advantages in both scenarios. Governance under the Department of Public Safety leans towards the influence of the Governor and the State political structure. Governance under the Department of Justice and the Attorney General leans towards the influence of federal and state law enforcement along with the judicial systems. However, further research would need to be conducted to validate advantages and disadvantages.

Vermont governance consists of a consortium of members from the Department of Public Safety, State Attorneys and Sheriff's, Department of Motor Vehicle, Department of Corrections, Court Administrators Office, and the Defender General Office. The consortium provides policy and technical resources when requested. The Department of Public Safety facilitates meeting and activities. The state identification system is funded as part of the Department of Public Safety budget. Vermont is seeking funding for the Justice information sharing system.

Los Angels County identification and information sharing systems are governed at the county level. Leadership is provided by county executives and law enforcement leaders. It should be noted that approximately 27 percent of California residents reside in

the county. If the county were to be considered as a state, it would have the nineteenth largest economy in the world (About L.A. County, n.d.). The county works with state to lead many criminal justice programs. The Los Angeles County Sheriff's Department oversees both the biometric identification systems and the information sharing programs. Funding for the biometrics identification program is supported by the state through fines, penalties, and a dollar fee on all registered vehicles in the county (L. Norton, personal communication, November 3, 2010). Funding for the county information sharing program is funded by the Los Angeles County Sheriff's Department and the Los Angeles Police Department. The expectation is that a distributed cost model will be put in place for participating agencies (C. Cahhal, personal communication, February 7, 2010).

Arizona identification systems are managed by the Department of Public Safety. Funding is supported by the department's budget as part of the state's revenue plan (Department of Public Safety, 2009, p. 354). The AZLink information sharing program is managed by the Arizona Criminal Justice Commission. Governance is provided by law enforcement regional representatives. The commission facilitates sessions for decision making with both a state policy team and technology team.[33] Direction and support is provided the commissioners (ACJC, 2010).

The following matrix illustrates the relationship between the state technology framework components (Table 2).

Table 2. Technology Framework Component Comparison

State	Biometric Identification			Information Sharing	Governance
	Creation	Verification	Mobile Identification Systems Available		Reporting Structure
Minnesota	State Level (1)	State Level	Yes (3)	Distributed & Indexed	Department of Public Safety
Los Angeles County Sheriff's Departmer	State (1) and County Leve	County Level (2)	Yes	Centralized	Los Angeles County Sheriff's Department
Wisconsin	State Level (1)	State Level	Yes	Distributed	Department of Justice, Attorney General
Vermont	State Level (1)	State Level	No	Distributed	Department of Public Safety
Arizona	State Level	State Level	No	Centralized & Distributed	Department of Public Safety - Identification Arizona Criminal Justice Commission - Information Sharing
Notes:					
(1) State Biometric Systems link to the FBI's Identification system and request federal biometrics identifiers					
(2) Los Angeles County Sheriff's Department verifies mobile identification requests against the County system. Plans are under way to extend verification to the State system					
(3) Minnesota has also extended mobile biometrics identification verification to the federal Repository for Individuals of Special Concern (RISC)					

[33] The AZLink program is the responsibility of the author of this thesis.

4. Technology Framework Best Practice

The following best practices were derived from the research information provided by Minnesota, Los Angeles County Sheriff's Department, Wisconsin, and Vermont and are captured in the information found in this thesis.

Technology Framework Identification Best Practices:

- Subject identifiers should be based on biometric identification technology.
- Verification of identity is based on biometrics not subjects names and demographics.
- All subjects' names are considered aliases.
- Criminal justice agencies should use biometric identification to verify identities and establish local record system identifiers.
- Identification protocol for mobile biometrics identification should be defined by state statutes.
- Integrated biometrics identification verification should include the FBI's RISC system.
- Federal, state, county, and local identifiers should be accurate, stored within local criminal justice systems and verified using biometric technology.

a. Technology Framework Information Sharing Best Practices

- Criminal justice information is stored, shared, and retrieved by biometric generated subject identifiers.
- Agencies must adherence to state and federal privacy laws.
- Collect information once and share many times.
- Local agency information must be accurate to support information sharing across agencies.
- Development of organizational, process, data, technology, and motivational models must use a cross discipline approach.
- Establish an environment for cultural change.
- Establish round table discussions at the lowest level to build relationship networks across agencies.
- Build partnerships across jurisdictions.

- Create a shared training and communications capability across jurisdictions.
- Implement technology standards that align with federal initiatives.
- Establish memorandums of understanding between local, state, and federal partners.
- Information should be accessible without jurisdictional boundaries.

b. Technology Framework Governance Best Practices

- State statutes should define organizations and their responsibilities.
- Executive commitment is required for setting direction, establishing funding, and allocating resources.
- Governance should include legislative champions.
- Leadership plays a significant part in implementing, funding and gaining acceptance.
- Leadership must facilitate decision making, across agencies and be advocates at the highest levels of government.
- Use real case success stories for marketing.
- Data practices for usage of criminal justice information should be defined by state statutes.
- Complete a privacy impact assessment and a privacy policy.
- Governance membership must have cross agency participation.
- Governance includes oversight and support for both policy and technology.
- Programs and projects should be defined in a phased approach. The best practice is to break the project up into meaningful and manageable phases. Each phase must be long enough to provide business value and support acceptance of the program, but short enough to deliver quick wins and build support for the program.

VI. CONCLUSIONS

A. THE TRAGIC LOSS OF A LAW ENFORCEMENT OFFICER

In 2006, Officer Nick Erfle of the Phoenix Police Department was shot and killed by a subject stopped and questioned by the officer for jaywalking. If information sharing had been available between Arizona law enforcement agencies and federal agencies this tragedy most likely would have been avoided.

The subject was an illegal immigrant who had a lengthy criminal history record. In 2006, the subject was deported based on a felony conviction for theft. The subject was issued an outstanding deportation order [34] and would face criminal charges if he re-entered the country. The subject re-entered the country and was arrested again two months later.

The Scottsdale Police Department arrested the subject in May of 2006 for grabbing his girlfriend's arm twice during a quarrel. Scottsdale officers only had local information and released the subject when he posted bond. If the Scottsdale Police Department had known the subject had an outstanding deportation order, he would have been jailed and federal criminal charges filed. A conviction could have earned him up to 20 years in prison; however, more importantly the subject would have not been released to commit the tragic shooting of Officer Nick Erfle (Villa, 2007). Although there is no guarantee the Scottsdale Police would have checked information through an integrated system, the opportunity would have presented itself based on the ease of use versus the manual efforts used today to find the information.

B. ARIZONA STRATEGIC PLAN 2012 RECOMMENDATIONS

The Arizona Criminal Justice Commission will be updating the 2008 *Arizona Integrated Criminal Justice Information System Strategic Plan* in 2012. This researcher

[34] Subjects who re-enter the county with an outstanding deportation order face federal criminal charges and are subject have penalties and jail time when convicted.

recommends using the technology framework discussed in this thesis as a guideline for taking the next steps. The technology framework offers suggestions for improvement based on other states efforts in the areas of implementation of biometric identification for criminal justice agencies, integration of identification capability with law enforcement information sharing systems, and establishing a governance structure necessary to support policy requirements and new technology solutions.

C. TECHNOLOGY FRAMEWORK LIMITATIONS

The technology framework provided in this thesis was founded on practical implementations in Minnesota; Los Angeles County, California; Wisconsin; and Vermont. Even though each implementation was designed to meet state requirements, there were similarities in regards to how technology is being used, governance oversight, and recommended best practices. Many states and regions are currently implementing law enforcement biometric identification systems and cross jurisdictional criminal justice information sharing programs. There is no one solution that fits all implementations. This researcher would like to see the technology framework enhanced by exploring additional states and their solutions.

D. ARIZONA STRATEGIC PLAN—BIOMETRIC IDENTIFICATION LIMITATIONS AND POSSIBILITIES

The 2008 *Arizona Strategic Plan* calls for utilizing unique identification to link together non-arrest events and formal arrest events with jail booking events. In addition, law enforcement agencies need to expand identification capabilities beyond known criminals.

The analysis in this thesis indicates that prior to booking a subject, law enforcement agencies only use biometric identification systems to verify identification against existing criminal records located in the state AFIS system. Law enforcement agencies do not create biometric identifiers. The only time a new biometric record is created is when a subject is booked into the jail system (creating a criminal record). Law enforcement agencies are dependent on the state to provide subject identifiers (SID,

FBIID) for their record management systems. For non-criminal identification, law enforcement agencies continue to create records and use information based on a subject's name and demographics. In addition, the systems are independent and require manual efforts to link subject information together for investigations and processing court cases. The information in this thesis shows using a subject's name and demographics as identifiers for criminal justice records is unreliable. The only true subject identification is based on biometric identification.

The possibility exists to use mobile biometric technology to generate a Non-Criminal Subject Identifier (NCID) at first point of authorized contact. The new identifier would be used as a subject identifier in all law enforcement record management systems across the state. The NCID would be maintained by the state (similar to the current state AFIS system) and distribute the NCID to law enforcement officers during the subject's biometric validation process. Having a NCID capability would provide a link between independent systems to retrieve information using automated solutions for non-criminal offenders. In addition, if a subject is booked into jail, a link between a State Identifier (SID), the FBI's Identifier (FBIID) and the NCID could provide a complete picture of a subject's involvement with the criminal justice system. This would include being able to automatically retrieve subject information stored in law enforcement systems prior to arrest and booking.

In addition to biometric fingerprint identifiers, possibilities exist to include facial image identifiers. Facial recognition systems are being implemented by the Arizona Counter Terrorism Information Center. Using facial recognition technology would follow the same process that creates a SID. A facial image would generate a State Facial Identifier (SFID). The SFID would be created from jail booking mugshot photos, law enforcement photos, and state driver's license photos for subjects with a criminal record. The additional SFID along with the SID will add an optional way to retrieve criminal record information and provide another validation capability to insure subject verification accuracy.

1. Future Research—Biometric Identification

Creating biometric identification capability used to store non-criminal subject information is a sensitive issue for the American public. This thesis has shown Arizona, along with other states, has rejected the National REAL-ID program. Concern exists in regards to how the information will be used, possibility of identity theft, and the security of personal information. For Arizona, further research will need to be done to determine if there are any acceptable conditions in which the Arizona state legislature will change their view in using and maintaining biometric identification information for non-criminal offenders. Restricting the use of the information to law enforcement does offer some possibilities. This researcher believes facial image recognition for non-criminal subjects will be unacceptable for the foreseeable future.

E. ARIZONA STRATEGIC PLAN—LAW ENFORCEMENT INFORMATION SHARING

Arizona is moving away from a centralized access capability across disparate law enforcement systems. The AZLink program using Coplink will provide integrated analysis and data access capability across the state. The information sharing environment will be similar to Los Angeles County, California.

The analysis of Minnesota, Los Angeles County, California, and Wisconsin showed there is no relationship between biometric identification systems and the information sharing systems. The Arizona Tucson Police Department is now piloting a program using new facial recognition technology included in the Coplink system (R. Fund, personal communication, August 18, 2009). The software allows input of images and creates biometric identification keys integrated into a pointer system. The system points to subject records located in the central repository. A requester can use a scanned image to request subject information.

This researcher would like to note that Arizona is participating with other states (including Los Angeles County, California) in information sharing across state borders. In addition, pilot programs are underway to share information with the U.S. Department of Justice and the U.S. Department of Homeland Security. However, information sharing

outside the state and with federal agencies is not included in this thesis. An excellent thesis would expand on the materials presented here and research information sharing across state borders and with federal agencies.

1. Future Research—Biometric Identification Integrated with Information Sharing Systems

The integration of facial recognition technology with information sharing systems links together two different law enforcement business practices. The capability is new and requires additional research in governance, policies, and procedures. The recommendation is to analyze other states using the same capability. In addition, the analysis would provide benefit to the technology framework developed in this thesis.

F. ARIZONA STRATEGIC PLAN—ALIGNMENT WITH FEDERAL AND STATE SYSTEMS LIMITATIONS AND POSSIBILITIES

The 2008 *Arizona Integrated Criminal Justice Information System Strategic Plan* identified a requirement to integrate with federal information sharing capabilities. The 2012 strategic planning process will consider integration with the FBI's program that delivers fast biometric identification capability against a Repository for Individuals of Special Concern. The RISC system is under development with pilot programs located at the Ohio Bureau of Criminal Identification and Investigation, Florida Department of Law Enforcement, Texas Department of Public Safety, and the Minnesota Bureau of Criminal Apprehension (as noted in the analysis) (C. Rhoades, personal communication, February 19, 2010).

1. Future Research—Biometric Identification Integrated with Federal and Border State Initiatives

The FBI is working with Central American countries to collect and store biometric information. The FBI plans to deliver information sharing capability to both federal and state law enforcement agencies. No single system exists that delivers both federal and state information to law enforcement officers in the field. The goal is to stop criminals at the first point of contact, regardless if it is along the border or within cities.

In parallel, Arizona, California, New Mexico, and Texas governors have been holding border conferences with Mexico since 2006. The objective of the conferences is to develop partnership programs to improve border security and reduce crime. Several programs support criminal information sharing. Table 3 illustrates the automated identification systems in Central America.

Table 3. Central American Countries Identification Systems Comparative Matrix (From McNicholas, 2009)

Comparative Matrix Central American Countries Automated Identification Systems				
	National ID System	**Criminal History & Prison System**	**Driver's License System**	**Firearms Permit System**
Panama	A-V	A-V	A-V	A-V
Honduras	A-V		A-V	A-V
El Salvador	A-V	A-V	A	A
Guatemala	A (2011)			
Mexico	A (2012)			
A	Automated System (includes prints and facial Images)			
V	Identification verified against a national identification system			
	Paper based system (may contain prints or facial images)			

The comparative matrix summarized from the Biometrics Baseline for Central America Final Report 2009 [35]

Further research will be necessary to determine the feasibility of integrating identification capability. The benefit would be enormous for the states that border with Mexico (Arizona, California, New Mexico, and Texas).[36]

G. ARIZONA STRATEGIC PLAN—EXPAND AND INTEGRATE GOVERNANCE

The Arizona Department of Public Safety governs the biometrics identification systems. The Arizona Criminal Justice Commission provides oversight to the state law enforcement information sharing program (AZLink). Since the adoption of the *Arizona*

[35] Central American countries include El Salvador, Honduras, Guatemala, Panama, and Mexico.

[36] Further information on this can be found in the unpublished paper *Central America Identification Information Sharing with Local Law Enforcement Agencies* (Kalaf, 2009).

Integrated Criminal Justice Information System Strategic Plan in 2008, four regional information centers have been established that support the Coplink central repository. A governance committee has been established to provide guidance to both the commission's policy and technical teams.

The recommendation will be to create a formal governance team that includes both a policy board and a technical board at the highest level within Arizona. This thesis provided two possible alternatives. First, create a formal governance program under the direction of the Arizona Department of Public Safety, similar to Minnesota. Second, create a formal governance program under the direction of the Arizona Attorney General, similar to Wisconsin. Both options have positive and negative impact to the state.

However, the technology framework outlines the responsibilities of the governance team. The 2012 strategic planning effort should include the recommendations and determine the best solution. This researcher recommends the state legislature create statues that formalize a governance structure, responsibilities, and funding.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

About CriMNet. (n.d.). Retrieved January 18, 2010, from http://www.crimnet.state.mn.us/About/aboutcrimnet.htm

About HCSO. (n.d.). Retrieved January 28, 2010, from http://www.Hennepinsheriff.org/content/about-hcso

About L.A. county. (n.d.). Retrieved February 21, 2010, from http://portal.lacounty.gov/wps/portal/!ut/p/c1/04_SB8K8xLLM9MSSzPy8xBz9CP0os3gLAwgwsjAJdDMw8nG1CPU0NTYy8DUEykfilg80I6A7HGQfHv2mBOTNIPIGOICjgb6fR35uqn5BboRBZkC6IgB6KXqV/dl2/d1/L2dJQSEvUUt3QS9ZQnB3LzZfODAwMDAwMDAyOExUMzAyTFE5TlVQQTBHSTU!/

Advanced fingerprint identification technology. (n.d.). Retrieved February 17, 2010, from http://www.fbi.gov/hq/cjisd/ngi.htm

Agency division/bureau descriptions. (n.d.). Retrieved February 13, 2010, from http://www.doj.state.wi.us/site/divs.asp#dles

Arizona Criminal Justice Commission. (n.d.). *Overview.* Retrieved February 22, 2010, from http://72.32.210.188/about/overview.asp

Arizona Criminal Justice Commission. (2008). *Arizona records improvement and information sharing plan*. Retrieved December 12, 2008, from http://azcjc.gov/pubs/home/RcdsImpandInfoSharingPlan2008.pdf

Arizona Criminal Justice Commission. (2010). *Commissioners.* Retrieved February 21, 2010, from http://72.32.210.188/about/commissioners.asp

Arizona Department of Public Safety. (n.d.). *Records and Identification*. Retrieved February 22, 2010, from http://www.azdps.gov/About/Organization/Criminal_Justice_Support/Records_Identification

Arizona State Legislature. (2008). *HB2426 Enhanced driver licenses; prohibition.* Retrieved March 22, 2009, from http://www.azleg.gov/FormatDocument.asp?inDoc=/legtext/49leg/1r/summary/h.hb2426_02-12-09_gov(3).doc.htm

Arizona integrated criminal justice information system. (n.d.). Retrieved February 22, 2010, from http://72.32.210.188/cjrip/AZICJIS.asp

Aumand F. (2008a). *Privacy Impact Assessment for the Vermont Justice Information Sharing System*. Internal document, Division of Criminal Justice Services. Vermont Department of Public Safety, provided by Director Francis X. Aumand III on November 4, 2009.

Aumand F. (2008b). *Privacy Policy*. Internal document, Division of Criminal Justice Services. Vermont Department of Public Safety, provided by Director Francis X. Aumand III on November 5, 2009.

Dataworks. (2008). *Digital mugshot system county of Los Angeles.* Retrieved February 2, 2009, from http://www.dataworksplus.com/press.htm#losangelesdpm

BCA history (n.d.). Retrieved November 7, 2009, from http://www.bca.state.mn.us/HomePageLinks/Documents/BCA-Hist.html

Bulman, P. (2003, February 11). *NIST: Both fingerprints, facial recognition needed to protect U.S. borders* [NIST news release]. Retrieved January 10, 2009, from http://www.nist.gov/public_affairs/releases/n03-01.htm

Bulman, P. (2004, July 6). *NIST study shows computerized fingerprint matching is highly accurate* [NIST news release]. Retrieved January 9, 2009, from http://www.nist.gov/public_affairs/releases/computer_fingerprint.htm

Crime Information Bureau. (2008). *2008 Annual Report*. Internal document, Wisconsin Department of Justice. Internal document provided by Phil Collins, Crime Information Bureau, Wisconsin. Department of Public Safety.

Criminal and juvenile justice information policy group. (n.d.). Retrieved January 31, 2010, from http://www.CriMNet.state.mn.us/Governance/PolicyGroupInformation.htm

CriMNet program office governance. (n.d.). Retrieved January 31, 2010, from http://www.CriMNet.state.mn.us/Governance/governance.htm

Darryl M., (2007). Law enforcement turns to face-recognition technology. *Information Today, 24*(5), pp. 50-51. Retrieved February 12, 2009, from ABI/INFORM Global database. (Document ID: 1268770751).

Department of Public Safety. (2009). *FY2009 appropriations report.* Retrieved February 21, 2010, from http://www.azleg.gov/jlbc/09app/dps.pdf

Dizard W.P. (2007, April 3). That face! Those eyes! How recognizable? *Government computer news*. Retrieved January 9, 2009, from http://gcn.com/Articles/2007/04/03/That-face-Those-eyes-How-recognizable.aspx

DOJ organization chart. (n.d.). Retrieved February 13, 2010, from http://www.doj.state.wi.us/site/doj_orgchart.asp

Electronic Privacy Information Center. (2008). *Real ID Implementation Review: Few benefits, staggering costs. Analysis of the Homeland Security's national id program*. (2008). Washington, DC: author. Retrieved March 22, 2009, from http://epic.org/privacy/id-cards/epic_realid_0508.pdf

Fast facts about Hennepin. (n.d.). Retrieved January 28, 2010, from http://www.co.Hennepin.mn.us/portal/site/HennepinUS/menuitem.b1ab75471750e40fa01dfb47ccf06498/?vgnextoid=9888822a9fe23210VgnVCM10000049114689RCRD

Gil-García, J., Schneider, C., & Pardo, T. (2004, July). *Effective strategies in justice information integration: A brief current practices review.* Retrieved January 28, 2010, from http://www.ctg.albany.edu/publications/reports/effective_strategies/effective_strategies.pdf

Hennepin County. (2005). *SILS Business Rules and Processes* (Version 2). Internal document, Hennepin County Sheriffs Office, Information Technology Services.

Hermann, W., *Facial recognition latest tool for state law enforcement.* (2006, October 12). Retrieved February 22, 2010, from http://www.janet2006.com/news/view_article.cfmid=69

Hoch J., (2007). *SILS Business Requirements* (Version 1.4). Internal document, Hennepin County Sheriffs Office, Information Technology Services, provided by Leila Tite, Consulting Information Technology Specialist on December 12, 2009.

Integration Architects. (2004). *Technical Specifications-CriMNet ID Service.* Internal document, Minnesota Bureau of Criminal Apprehension.

Integration Architects. (2005). *Identification Roadmap Initiative (Draft Final Report).*

Internal document, Minnesota Bureau of Criminal Apprehension, provided by Mr. Jerry Olson Project Manager, Minnesota Bureau of Criminal Apprehension on November 19, 2010.

Iris Scan. (n.d.). Retrieved February 11, 2009, from http://ctl.ncsc.dni.us/biomet%20web/BMIris.html

LACRIS—Los Angeles County Regional Identification System.(n.d.). Retrieved January 9, 2009, from http://www.lasd.org/divisions/tsdiv/record_id/ri_ovrview.html#lacris

LACRIS Mobile ID Usage Report. (2009). Internal document, Los Angeles County Sheriff's Department

LASD Technical Services Division. (2007). Field Based Biometric Identification. Internal document, Los Angeles County Sheriff's Department, Technical Services Division, provided by Commander Daryl Evans

Los Angeles County Records and Identification Bureau. (n.d.). *Los Angeles County regional identification system*. Retrieved February 19, 2010, from http://la-sheriff.org/sites/YIR/2002/visuals/3841.pdf

Law Enforcement Services. (n.d.). Retrieved February 13, 2010, from http://www.doj.state.wi.us/dles/cib

Los Angeles County Sherriff's Department. (2008). *Organization chart*. Retrieved January 5, 2010, from http://www.lasd.org/aboutlasd/OrgChart/images/chart.pdf

Los Angeles Regional Integrated Law Enforcement and Justice Governance Committee. (2005). *Consolidated Joint Application Requirements Session Results* (Draft 1.0). Internal document, Los Angeles County Sheriff's Department, provided by Lieutenant Chris Cahhal. Law Enforcement Information Sharing Program on October 20, 2009.

L-1 Identity Solutions. (n.d.). *Fast and accurate field identification with iris technology*. Retrieved January 9, 2009 from http://www.l1id.com/files/246-PIER2.4_0908_final.pdf

Macro Group & Labyrinth Consulting. (2000). *CJSIIP phase III deliverable.* Internal document, Hennepin County Sheriffs Office, Information Technology Services.

McCombs W. *Integrated biometrics identification system.* (2009). Retrieved February 18, 2010, from http://www.police-technology.net/integrated_biometrics_identification_system.html

McNicholas M. (2009) *Biometrics baseline for Central America final report 2009*. Internal document, Phoenix Group and Pathfinder Consulting LLC.

MNJIS programs and information. (n.d.). Retrieved January 31, 2010, from http://www.bca.state.mn.us/CJIS/Documents/cjis-intro.html

More Secure Driver's Licenses. (2009). Retrieved March 22, 2009, from http://www.dhs.gov/xprevprot/programs/gc_1200062053842.shtm

Name event index service project (NEIS). (2008). Retrieved February 22, 2009, from http://www.CriMNet.state.mn.us/Projects/NEIS.htm

National Law Enforcement Recruiters Association. (n.d.) *BJS Law Enforcement Summary Findings.* Retrieved February 14, 2010, from http://www.nlera.org/?page_id=116

Newton, E., & Phillips, P. (2006). *Meta-analysis of third-party evaluations of iris recognition.* Gaithersburg, MD: National Institute of Standards and Technology. Retrieved January 9, 2009, from http://iris.nist.gov/ice/IrisComparisonY070820_NISTIR.pdf

Next generation identification. (n.d.). Retrieved February 22, 2010, from http://www.fbi.gov/hq/cjisd/ngi.htm

NGA Center for Best Practices. (2009). *Overview of state justice information sharing governance structures.* Retrieved November 12, 2009, from http://www.nga.org/Files/pdf/0907JUSTICEINFOSHARING.PDF

Norton, L. (2009). Who goes there? Mobile fingerprint readers in Los Angles County. *The Police Chief, 76*(6). Retrieved February 2, 2010, from http://policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=1824&issue_id=62009

SEARCH. (2009). *Information Case Study – Los Angeles County California*. (2009). Internal document, Los Angeles County Sheriff's Department, provided by Lieutenant Chris Cahhal, Law Enforcement Information Sharing Program on October 20, 2009.

Task Force - Criminal and Juvenile Justice Information Task Force. (n.d.). Retrieved January 31, 2010, from http://www.CriMNet.state.mn.us/Governance/TaskForceInformation.htm

Transaction Information for the Management Enforcement (TIME). (2009). Retrieved December 23, 2009, from http://www.doj.state.wi.us/dles/time

U.S. Census Bureau. (2008). *State and County Quick Facts*. Retrieved February 10, 2010, from http://quickfacts.census.gov/qfd/states/50000.html

U.S. Department of Justice. *Guide to Conduct Privacy Impact Assessments for State, Local, and Tribal Information Sharing Initiatives*. (2008). Washington, DC: Office of Justice Programs, the National Consortium for Justice Information and Statistics, U.S. Department of Justice. Retrieved February 6, 2010, from http://www.ojp.usdoj.gov/BJA/pdf/PIAGuide-Feb09.pdf

Vermont Department of Public Safety. (2008). *Vermont Crime - Full Time Vermont Law Enforcement Offices*. Retrieved February 10, 2010, from http://www.dps.state.vt.us/cjs/crime_08/police_full.htm

Villa, Judy (2007, September 20). After deportation, shooter was caught, freed again. *New Nations News Reporters Newsroom* [Reprint from *Arizona Republic*]. Retrieved February 6, 2010, from http://www.newnation.vg/forums/showthread.php?t=110755&highlight=Nick+Erfle

Viisage Technology Inc. (2005). *Mobile identification system for law enforcement* [solution sheet]. Retrieved January 8, 2009, from http://www.l1id.com/files/88-missolutionsheet_20051212.e.r.pdf

VJISS Strategic Plan. (2009, March). Internal document, Vermont Department of Public Safety, Division of Criminal Justice Services, provided by Director Francis X. Aumand III on November 5, 2009.

WDOJ. (2004). *Wisconsin Fast ID Information*. Retrieved February 12, 2010, from http://www.doj.state.wi.us/dles/cib/forms/time/fast_id.pdf

Williams W. (2008). State lawmakers challenge REAL ID Act. *The State Journal*. http://www.statejournal.com/story.cfm?func=viewstory&storyid=33938

Wisconsin Crime Information Bureau. (2007). *Identification Training* (rev.). Retrieved February 13, 2010, from http://www.doj.state.wi.us/dles/cib/forms/time/ident_handout.pdf

Wisconsin criminal history records: From arrest to sentence. (2009). Retrieved December 23, 2009, from http://www.doj.wi.gov/dles/cib/conference/2009Handouts/CriminalHistory.pdf

Wisconsin Department of Administration. (2002). *Census 2000 data.* Retrieved February 12, 2010, from http://www.doa.state.wi.us/demographic/rcounty_view.asp?locid=9

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California