NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

CONNECTING LAW ENFORCEMENT RECORDS MANAGEMENT SYSTEMS

by

Martin L. Birkenfeld Jr.

March 2021

Co-Advisors: Patrick E. Miller (contractor)
Erik J. Dahl

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2021	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE
CONNECTING LAW ENFORCEMENT RECORDS MANAGEMENT SYSTEMS

5. FUNDING NUMBERS

6. AUTHOR(S) Martin L. Birkenfeld Jr.

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	**12b. DISTRIBUTION CODE**
Approved for public release. Distribution is unlimited.	A

13. ABSTRACT (maximum 200 words)

Every law enforcement agency uses records management systems (RMS) that contain a wealth of information essential for investigations or intelligence. This information includes crime reports, arrest reports, name records, and property records. The ability to share this information between law enforcement agencies, especially those with bordering jurisdictions, would appear beneficial to the homeland security enterprise; however, this thesis reveals that sharing RMS data is not occurring as often as expected. Direct RMS connections are uncommon, and law enforcement agencies possess valuable information hemmed off in seclusion.

This thesis examines a research-based RMS model and other systems that attempt to solve the data-sharing problem. One case study reveals the costly failure of a records system commissioned by the FBI. A survey and interviews of Texas police agencies reveal gaps in information sharing, including many not furnishing data to exchange networks. Although fusion centers and regional information-sharing systems (RISS) provide valuable intelligence and investigative products, many police agencies do not use these resources.

How can law enforcement improve information sharing? The answer requires agency leaders to become educated on the many resources available and break down bureaucratic or political barriers that prevent the automated sharing of law enforcement RMS data.

14. SUBJECT TERMS	**15. NUMBER OF PAGES**
police records management, RMS, records management systems, law enforcement records management systems, law enforcement information sharing, national data exchange, N-DEx	93
	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.

CONNECTING LAW ENFORCEMENT RECORDS MANAGEMENT SYSTEMS

Martin L. Birkenfeld Jr.
Chief of Police, City of Amarillo
BS, Mountain State University, 2009
MBA, West Texas A & M University, 2017

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 2021

Approved by: Patrick E. Miller
Co-Advisor

Erik J. Dahl
Co-Advisor

Erik J. Dahl
Associate Professor, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Every law enforcement agency uses records management systems (RMS) that contain a wealth of information essential for investigations or intelligence. This information includes crime reports, arrest reports, name records, and property records. The ability to share this information between law enforcement agencies, especially those with bordering jurisdictions, would appear beneficial to the homeland security enterprise; however, this thesis reveals that sharing RMS data is not occurring as often as expected. Direct RMS connections are uncommon, and law enforcement agencies possess valuable information hemmed off in seclusion.

This thesis examines a research-based RMS model and other systems that attempt to solve the data-sharing problem. One case study reveals the costly failure of a records system commissioned by the FBI. A survey and interviews of Texas police agencies reveal gaps in information sharing, including many not furnishing data to exchange networks. Although fusion centers and regional information-sharing systems (RISS) provide valuable intelligence and investigative products, many police agencies do not use these resources.

How can law enforcement improve information sharing? The answer requires agency leaders to become educated on the many resources available and break down bureaucratic or political barriers that prevent the automated sharing of law enforcement RMS data.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACLU	American Civil Liberties Union
API	application programming interface
CAD	computer-aided dispatch
CISC	Colorado Information Sharing Consortium
CLEAR	Citizen and Law Enforcement Analysis and Reporting
CPD	Chicago Police Department
CRIMES	Criminal Research Information Management Evaluation System
DFC	Dallas Fusion Center
DOJ	United States Department of Justice
FBI	Federal Bureau of Investigation
FWINTEX	Ft. Worth Intelligence Exchange
HUMINT	human intelligence
LE	law enforcement
LEEP	Law Enforcement Enterprise Portal
LEITSC	Law Enforcement Information Technology Standards Council
LInX	Law Enforcement Information Network Exchange
NCIC	Nation Crime Information Center
NCIS	Naval Criminal Investigative Service
N-DEx	National Data Exchange
NIEM	National Information Exchange Model
NTFC	North Texas Fusion Center
OIG	United States Department of Justice, Office of the Inspector General
RDW	regional data warehouse
RMS	records management system
RISS	Regional Information Sharing Systems Program
SHSU	Sam Houston State University
TCIC	Texas Crime Information Center
TDEx	Texas Data Exchange
TWC	Texas Workforce Commission
TxDPS	Texas Department of Public Safety

TxFC	Texas Fusion Center (Austin)
TXGANG	Texas Gang Intelligence Index
VCF	FBI’s Virtual Case File

EXECUTIVE SUMMARY

All law enforcement agencies use a records management system (RMS) to organize crime data and criminal case management. Over the last three decades, the technology behind computerized records has significantly advanced, and the capability to share information electronically has seen exponential growth. These innovations have resulted in a market opportunity for dozens of different vendors to create RMS solutions for law enforcement. The variety of RMS choices creates problems and opportunities. The problem is a lack of information sharing because most of these systems are not directly connected to each other. This disconnect means that investigators or analysts in adjacent jurisdictions may not directly see or share crime and offender information without subscribing to additional resources. This lack of sharing hampers law enforcement efforts to build a broader strategy to combat organized criminal or terrorist-related activities.

Law enforcement can improve by examining the possibility that multiple agencies sharing jurisdictional boundaries could also share an RMS. An extension of this theory could be that regions or states adopt a shared RMS so that law enforcement officers are accessing and entering information on the same platform. A shared system means that users across jurisdictional boundaries have a standard operating platform and may be more likely to understand the context and content of data from other jurisdictions.

Absent a shared RMS, other tools such as data exchanges and data warehouses exist in various forms throughout law enforcement. One of the more prominent exchanges is the National Data Exchange (N-DEx), which "provides criminal justice agencies with an online tool for sharing, searching, linking, and analyzing information across jurisdictional boundaries."[1] N-DEx is a useful investigative tool; however, N-DEx depends on agencies to share data from the RMS via an interface. If an agency chooses not to share data, the system loses the value that information could have added. Without proper training, investigators might know about or may not see the value in using N-DEx and other data

[1] "National Data Exchange (N-DEx) System," FBI Criminal Justice Information Services (CJIS), accessed December 5, 2019, https://www.fbi.gov/services/cjis/ndex.

exchanges or data warehouses for research or analysis. These limitations restrict the ability to make consistent investigative connections across jurisdictional boundaries.

There are many different users of law enforcement RMS, including police officers, investigators, administrators, and analysts. External customers such as insurance companies, research universities, and civic organizations also have a stake in the RMS data. RMS contains numerous modules such as computer-aided dispatch, name records, property records, arrest reports, and crime reports, all of which serve essential functions within the organization. RMS serves a critical role in the law enforcement function, both for internal and external stakeholders. Some of the information that can protect our communities and our nation lies with the vast data gathered by local law enforcement agencies.

Law enforcement agencies share and access information in a variety of different ways. The method or platform used is dependent upon the nature and origin of the data. Some of these include NCIC, fusion centers, data exchanges, data warehouses, and private industry data, and the array of choices may be one factor inhibiting the effectiveness of information sharing. Agencies are left to decide what resources they will subscribe to and, significantly, what resources to which they will contribute information. Law enforcement should develop a common strategy to determine how agencies will share information. One alternative could be an extensive, federated records management and sharing system operated by a government agency.

A case study in this research examines the FBI's Virtual Case File (VCF) as a comparative example of a large RMS and how planning errors resulted in substantial financial waste. The harsh lessons learned from the VCF fiasco and the FBI's resultant change of strategy can be a guidepost for other law enforcement agencies in developing large, shared systems. Another case study looks at the Criminal Research Information Management Evaluation System (CRIMES), which Sam Houston State University maintains. CRIMES is an information management platform used by over 50 law

enforcement agencies in Texas.[2] The case study examines the research motives behind the system and the ability for CRIMES to successfully provide an effective and connected RMS for smaller law enforcement agencies.

The author surveyed 125 Texas police departments to examine the state's broader RMS usage and information sharing among municipal police agencies. Only municipal police agencies in Texas were selected so that the research could be confined to organizations with similar functional responsibilities. The survey identified a wide variety of RMS vendors used among these agencies. The data also suggests that many police departments fail to use external resources for investigative or intelligence information. Perhaps the most startling information gained from this survey is that 80 percent of the police departments who responded reported that they did not directly share their RMS information with N-DEx, or other information exchanges.

The author conducted personal interviews with RMS users from police departments to better understand actual and perceived problems with sharing criminal and intelligence information. Some interviews targeted current and recent CRIMES user agencies as part of the case study for that system, which is also only available to Texas law enforcement. CRIMES started as a tool to provide academic researchers in criminal justice direct access to crime data. It has evolved into an information management system that competes directly with the vendors in the private sector. Despite some of the limitations and problems, CRIMES provides a good RMS platform for small and medium-sized agencies that do not have a long list of unique requirements.

Information from the interviews also revealed similar gaps in RMS information sharing as was gleaned from the surveys. CRIMES is currently not sharing information between agencies, although developers are exploring this possibility via a hosted solution.

---

[2] Vincent Webb, *The Criminal Research Information Management Evaluation System (CRIMES): A Comprehensive Records Management System for Smaller Police* (Tempe, AZ: Arizona State University, Center for Violence Prevention and Community Safety, 2017), http://cvpcs.asu.edu/sites/default/files/content/pages/Criminal_Research_Information_Management_Evaluation_System%20.pdf.

Some agencies have discovered other RMS vendors who facilitate sharing across their platforms to include the ability to see data from other agencies using the same vendor.

Records management and information systems are an essential part of the law enforcement organization. Most law enforcement officers agree that sharing this information between agencies is an essential component of information systems.[3] The rapid progression of information technology makes it possible to communicate large amounts of information across the country in seconds. Information storage capabilities continue to grow, as do the opportunities for artificial intelligence to process data in ways only imagined 30 years ago. Why, then, is it so difficult to share this information on a widespread basis across law enforcement organizations in the United States or even with other countries?

This thesis shows that political barriers, lack of governmental regulation, and marketing and training on information sharing resources are challenges to information sharing among law enforcement. Recommendations for improvements include regional agencies combining RMS, governmental sponsorship and funding, raising awareness of information resources, and mandatory participation in data exchanges.

No single solution will fix the lack of information sharing in the homeland security enterprise. Law enforcement agencies collect a great deal of data that holds the potential to improve our country's safety and security. The key is sharing, in particular outwardly. Front line workers need access to the information contained in both neighboring and distant law enforcement information systems to more effectively protect our nation from criminal or terrorist threats.

Whether sharing a multi-agency RMS, participating in data exchanges, or an amalgamation thereof, law enforcement executives must find the right combination of solutions. These solutions should protect the data and the organization's integrity while still providing external agencies the resources needed to connect criminal and intelligence

---

[3] John Hollywood and Zev Winkelman, *Improving Information-Sharing across Law Enforcement: Why Can't We Know?* (Santa Monica, CA: RAND Corporation, 2015), https://www.ncjrs.gov/pdffiles1/nij/grants/249187.pdf.

information. A successful result will be a robust network that puts the United States on the leading edge of law enforcement information sharing.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I wish to express my sincere gratitude to the faculty, staff, and contractors at the Center for Homeland Defense and Security and the Naval Postgraduate School for a truly excellent learning experience. Your thoughtfulness and encouragement, along with your dedication to excellence, truly made this experience life-changing. I appreciate the motivation and guidance on this thesis by Dr. Erik Dahl and Patrick Miller.

Thank you to my colleagues at the Amarillo Police Department for inspiring me to learn and to grow. Your excellence and commitment to your work make my job easy and, most of all, enjoyable. I hope this work adds knowledge and makes improvements to our profession. I appreciate all of my colleagues who took up the slack during my absences.

Thank you to Dr. Larry Hoover and Suman Malempati of Sam Houston State University for their dedication to push the envelope in creating the CRIMES system and their willingness to talk openly to this researcher about the project.

I appreciate all the Texas police chiefs who took the time to respond to my research inquires. I will gladly return the favor.

I also owe a debt of gratitude to Kevin Starbuck, deputy city manager of the City of Amarillo and CHDS Alumni, for recommending me for this program. His foresight and encouragement were essential to my attendance and success.

Thank you to my friends and family who loved and supported me through this journey. I hope to make up some of the missed time with you.

To my loving wife, Heather Renee Birkenfeld, your support has been essential to our success as a family and as professionals over the years. You gave me so much latitude and took great care of me during this project. I am forever grateful, and I love you very much!

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

All law enforcement agencies use a records management system (RMS) to organize crime data and criminal case management. Over the last three decades, the technology behind computerized records has significantly advanced, and the capability to share information electronically has seen exponential growth. These innovations have resulted in a market opportunity for dozens of different vendors to create RMS solutions for law enforcement. The variety of RMS choices creates problems and opportunities. The problem is a lack of information sharing because most of these systems are not directly connected to each other. This disconnect means that investigators in adjacent jurisdictions may not directly see or share crime and offender information without subscribing to additional resources. Similarly, crime analysts are limited by geographical and jurisdictional boundaries in their data-gathering abilities. This lack of sharing hampers law enforcement efforts to build a broader strategy to combat organized criminal or terrorist-related activities.

Investigators and analysts seek alternatives to bridge the information gap. Comprehensive solutions for managing law enforcement data have been in place for decades. The theory of entering and using shared criminal data has roots in the National Crime Information Center (NCIC), governed by the FBI. NCIC connects every subscribing agency to a network of data that can identify wanted or missing persons, stolen cars, or violent offenders, among other things.[1] NCIC is an excellent tool for officers and investigators, but the scope of data is limited. These limitations likely carry over from the legacy system, which relied on old analog technology that could not transmit large volumes of data. With the advent of the internet age, these data restrictions may no longer apply.

The opportunity exists to create better mechanisms and policies for sharing RMS data between law enforcement agencies. A shared RMS could solve many information-sharing problems by consolidating data collection and accessibility into fewer systems. Federated search tools can make the information in one jurisdiction readily available to

[1] "National Crime Information Center (NCIC)," Federal Bureau of Investigation, accessed October 25, 2020, https://www.fbi.gov/services/cjis/ncic.

other users on the same system. One model that tries to solve this problem and create a shared RMS is the Criminal Research Information Management Evaluation System (CRIMES), maintained by Sam Houston State University (SHSU). CRIMES caters to over 50 law enforcement agency subscribers in Texas who use this platform for their RMS.[2] In addition to the core RMS component, CRIMES has a full palette of business modules for law enforcement agencies' various critical functions, including a computer-aided dispatch module, property and evidence management, and data analytics.[3] Although initially a research tool for SHSU, CRIMES developed into a model for a multi-agency solution for organizations that do not desire to procure, build, or maintain an independent RMS. However, CRIMES also faces unique challenges that may hamper its ability to grow beyond small agency use.

Absent a shared RMS, other tools such as data exchanges and data warehouses exist in various forms throughout law enforcement. Some are operated by governmental organizations, while others are private sector enterprises. One of the more prominent exchanges is the National Data Exchange (N-DEx), which "provides criminal justice agencies with an online tool for sharing, searching, linking, and analyzing information across jurisdictional boundaries."[4] N-DEx is a useful investigative tool; however, N-DEx depends on agencies to share data from the RMS via an interface. If an agency chooses not to share data, the system loses the value that information could have added. N-DEx is a separate system from NCIC and a local RMS, and agencies must navigate a degree of bureaucracy to access it. Without proper training, investigators might know about or may not see the value in using N-DEx and other data exchanges or data warehouses for research or analysis. These limitations restrict the ability to make consistent investigative connections across jurisdictional boundaries.

---

[2] "Criminal Research, Information Management and Evaluation System (CRIMES)," Police Research Center, accessed December 8, 2019, http://www.cjcenter.org/prc/crimes/.

[3] Police Research Center.

[4] "National Data Exchange (N-DEx) System," FBI Criminal Justice Information Services (CJIS), accessed December 5, 2019, https://www.fbi.gov/services/cjis/ndex.

Connecting information is vital for investigators in tracking criminals across jurisdictional boundaries. Terrorist activities are challenging to identify without excellent data sharing. Law enforcement can improve by examining the possibility that multiple agencies sharing jurisdictional boundaries could also share an RMS. An extension of this theory could be that regions or states adopt a shared RMS so that law enforcement officers are accessing and entering information on the same platform. A shared system means that users across jurisdictional boundaries have a standard operating platform and may be more likely to understand the context and content of data from other jurisdictions. This thesis explores how agencies share information, policy considerations, and the potential for improvement in the effectiveness and efficiency of using a shared RMS.

A. RESEARCH QUESTION

How can law enforcement agencies directly share information more effectively and efficiently to identify criminal suspects, organized crime, or potential terrorist activities?

B. LITERATURE REVIEW

This thesis focuses on sharing law enforcement records between agencies. Many sources cover ways to share law enforcement records, including data exchanges, fusion centers, and data warehouses. The effectiveness and efficiency of fusion centers have been the topic of many discussions. Other publications provide minimum standards for RMS. This thesis seeks to explore effective models and instances of common-use systems. Multiple law enforcement agencies—specifically, agencies within the same state or those with overlapping jurisdictional boundaries—could use these systems. Information is scarce in this realm, although there are a few alternatives to explore.

1. Linking Law Enforcement Data

A prevailing theme in the literature about law enforcement records is linking together the data from a variety of different systems. The FBI provides information on N-DEx, touting the system's ability to gather information from law enforcement

nationwide and make it available to subscribers.[5] Writers on the N-DEx system boast successes through anecdotal evidence, boldly stating that it "makes the world safer" without providing substantive data to support the claim.[6] Several published articles about the success of N-DEx were written by one of its project managers, Kasey Wertheim.

The Regional Information Sharing Systems Program (RISS) provides another resource for sharing law enforcement records. Information from RISS identifies a network of six centers that serve geographical regions of the United States and some foreign countries.[7] Most literature on RISS support this system as a viable information-sharing resource. Law enforcement agencies are encouraged to join RISS; however, membership is not mandatory, and there are no legislated incentives for participation.

2. Government Standards

Publications from the FBI and the Department of Justice describe common standards for RMS.[8] State agencies also set similar standards to guide law enforcement organizations when making purchases or building RMS.[9] There is no discernable discussion on how the large variety of different RMS contributes to the lack of information

---

[5] Federal Bureau of Investigation.

[6] Kasey E. Wertheim and Kelly Badgett, "The FBI's National Data Exchange (N-DEx)," *FBI Law Enforcement Bulletin*, December 9, 2015, https://leb.fbi.gov/articles/featured-articles/the-fbis-national-data-exchange-n-dex.

[7] "About the RISS Program: A Proven Resource for Law Enforcement," Regional Information Sharing Systems, accessed November 8, 2020, https://www.riss.net/about-us/.

[8] Federal Bureau of Investigation, *Law Enforcement Records Management Systems (RMSs) as They Pertain to FBI Programs and Systems* (Washington, DC: Department of Justice, 2010), https://ucr.fbi.gov/law-enforcement-records-management-system.

[9] California Commission on Peace Officer Standards and Training, *Law Enforcement Records Management Guide*, 5th ed. (Sacramento, CA: California Commission on Peace Officer Standards and Training, 2014), https://post.ca.gov/Portals/0/Publications/Records_Management.pdf?ver=2019-07-12-131135-140.

sharing. Instead, this literature type focuses on meeting records management standards and best practices, including recommending interfaces with legacy systems such as NCIC.[10]

3. Fusion Centers

Literary discussions on fusion centers debate the value, focus, and ethics of fusion center information. A Senate report from 2012 was very critical of fusion centers, identifying problems with spending accountability and questioning the value of the information provided, going so far as to say that fusion centers are "largely ineffective."[11] Civil rights groups such as the ACLU are also critical of the fusion center concept, reporting that the centers collect information on law-abiding citizens and do not make significant contributions in fighting terrorism.[12] There is much discussion about how fusion centers should operate, who the customer is, and whether these centers contribute to the United States' overall security.

On the other side of the fusion center debate are writers who find great value in their existence. Authors with experience in the field view fusion centers as central to the process of information sharing because they gather data from multiple sources and platforms.[13] This supportive viewpoint tends to derive from persons with significant experience in the fusion center realm.

---

[10] Law Enforcement Information Technology Standards Council, *Standard Functional Specifications for Law Enforcement Records Management Systems (RMS)* (Washington, DC: Department of Justice, 2006), https://it.ojp.gov/documents/LEITSC_Law_Enforcement_RMS_Systems.pdf.

[11] Senate Permanent Subcommittee on Investigations, *Federal Support for and Involvement in State and Local Fusion Centers: Majority and Minority Staff Report* (Washington, DC: U.S. Senate Permanent Subcommittee on Investigations, 2012), https://www.hsgac.senate.gov/imo/media/doc/10-3-2012%20PSI%20STAFF%20REPORT%20re%20FUSION%20CENTERS.2.pdf.

[12] Michael German and Jay Stanley, *What's Wrong with Fusion Centers?* (New York: American Civil Liberties Union, 2007), https://www.aclu.org/files/pdfs/privacy/fusioncenter_20071212.pdf.

[13] G. C. Sam McGhee, "The Wicked Problem of Information Sharing in Homeland Security—A Leadership Perspective" (master's thesis, Naval Postgraduate School, 2014), http://hdl.handle.net/10945/42684.

4. Governance Issues

Government-generated literature focuses on creating policies that encourage or require information sharing. Scholars cite a lack of cooperation in this area due to issues over the ownership of data.[14] Smaller agencies may be fearful of the state or federal government having control over their systems. The argument for improving information sharing is valid and is supported in multiple sources. However, there is not a readily discernable discussion of the idea of using a shared RMS. The arguments in this area instead speak to why some different systems cannot share. This information is relevant to the thesis topic because governance issues are likely to be a barrier to using a common RMS in the same way they are currently a barrier to sharing other systems.[15]

5. The Problem

Law enforcement executives agree that developing a comprehensive RMS is a very challenging task and has many solutions. The sharing of law enforcement data is generally recognized as one key to improving homeland security. The federal government has sponsored various solutions to address this, such as RISS, the Law Enforcement Enterprise Portal (LEEP), and N-DEx.[16] However, other writers report that some police data are hemmed off in seclusion due to proprietary vendor RMS.[17] In addition to the CRIMES model in Texas, other researchers have explored the idea of a shared RMS for

---

[14] John Hollywood and Zev Winkelman, *Improving Information-Sharing across Law Enforcement: Why Can't We Know?* (Santa Monica, CA: RAND Corporation, 2015), https://www.ncjrs.gov/pdffiles1/nij/grants/249187.pdf.

[15] Trevor Womack, "Economies of Scale: 9-1-1 Center Consolidation as a Means to Strengthen the Homeland Security Enterprise" (master's thesis, Naval Postgraduate School, 2014), 7, http://hdl.handle.net/10945/41458.

[16] "Law Enforcement Information Sharing," Office of the Director of National Intelligence, accessed June 30, 2020, https://www.dni.gov/index.php/who-we-are/organizations/ise/ise-archive/ise-additional-resources/2142-law-enforcement-information-sharing.

[17] Andrew Dasher and Robert Haynes, "Overcoming Law Enforcement Data Obstacles," *Police Chief Magazine*, September 28, 2016, https://www.policechiefmagazine.org/overcoming-law-enforcement-data-obstacles/.

geographically connected law enforcement agencies.[18] Detailed crime and criminal information are often isolated in otherwise geographically and jurisdictionally affiliated agencies. This siloing is part of the problem of information sharing that this thesis will address.

6. Literature Conclusions

Existing literature reveals both the advantages and the perils of large interconnected data systems. Legacy systems such as NCIC are good examples that show the viability of a sizeable common-user system. CRIMES appears to be a promising study in the area of shared RMS. RMS data is a specific niche of information collected by law enforcement officers. RMS may contain a treasure trove of information that can identify crime trends, information on specific criminals, and connections between specific crimes across artificial boundaries. A shared-use, common operating platform for RMS in law enforcement is one possibility to solve the problem of efficiently connecting information. More research is needed to identify better ways to collect and share RMS data.

C. RESEARCH DESIGN

1. Program Evaluation

One of the research methods for this thesis is program evaluation using the formative method. The subject of the program evaluation is CRIMES RMS. This study identifies the strengths and weaknesses of CRIMES, not just as a software program but as a program of affiliated agencies using the system. The research identifies policies, practices, and functionality that either enables or hinders the end user's ability to collect, share, or access RMS information from other agencies.

2. Case Studies

One case study looks at the FBI's Virtual Case File (VCF) as a comparative example of a large RMS. The VCF study is a review of historical literature on the evolution

[18] Chris Green, "Illinois Law Enforcement Agencies Seek Shared Records Management System," *Government Technology*, March 21, 2017, https://www.govtech.com/public-safety/Illinois-Law-Enforcement-Agencies-Seek-Shared-Records-Management-System.html.

of the system. Another case study examines the strengths of CRIMES and where improvement is needed to successfully achieve the goal of providing a universal platform for RMS and other connected modules. The goal of these case studies is to create some recommendations on the advantages and pitfalls of a multi-agency RMS.

3. Survey

The author sent a survey link to over 642 Texas municipal law enforcement agencies. The survey asked questions to examine the state's broader RMS and information sharing among municipal police agencies.[19] Only municipal police agencies in Texas were selected so that the research could be confined to organizations with similar functional responsibilities. The survey identified the variety of RMS among these agencies and the resources agencies used to contribute to or access outside information.

4. Personal Interviews

The author conducted personal interviews with RMS users to better understand actual and perceived problems with sharing criminal and intelligence information.[20] The interviewees were selected from Texas police agencies who responded to information requests from the author. The research focused on Texas agencies to narrow the scope and compare similarly situated agencies regarding their information requirements. Interviews targeted current and recent CRIMES agencies as part of the case study for that system, which is also only available to Texas law enforcement. The author used the same structured interview with a Utah department due to information gleaned from one Texas agency regarding a shared RMS in the Ogden area. All interview questions were designed to develop information regarding the use, inter-connectivity, and effectiveness of RMS and the agency's use of other information-sharing resources.

---

[19] A determination request was submitted to the Naval Postgraduate School's Institutional Review Board (IRB) on November 25, 2020. The IRB reviewed the request and determined on December 08, 2020, that no further IRB review and approval was required. IRB Determination No. NPS.2021.0029-DD-N

[20] A determination request was submitted to the Naval Postgraduate School's Institutional Review Board (IRB) on July 02, 2020. The IRB reviewed the request and determined on July 10, 2020, that no further IRB review and approval was required. IRB Determination No. NPS.2020.0167-DD-N

D. CHAPTER REVIEW

Chapter II discusses law enforcement RMS users, functions, and challenges. Included is a breakdown of who the users are and the variety of information stored in an RMS. The chapter also explores why RMS is a valuable business enterprise and the challenges law enforcement executives face in procurement.

Chapter III describes the multitude of ways that law enforcement agencies and officers share information. A summary of different systems outlines law enforcement's complicated choices in finding the best system to obtain needed data. These systems are both linked and separated from other systems. The exact overlap is unclear, and the challenges of finding the right combination are abundant.

Chapter IV summarizes a pre and post 9/11 attempt by the FBI to create a nationwide records management system to consolidate sources and connect hundreds of FBI offices. This system came to be known as the Virtual Case File (VCF) and was also famous for abysmally failing as a project. This failure teaches lessons to help organizations build federated records management systems using an intentional and thoughtful planning process and project management methodology.

Chapter V is the methodology and data summary of research on Texas municipal police agencies. The research asks the agencies to identify what RMS they use and what other data sources they access for investigations and intelligence. The research reveals a snapshot of the variety of RMS among these types of agencies. The data also identifies whether agencies share the system with other law enforcement organizations or data exchanges.

Chapter VI describes the CRIMES model managed by SHSU through interviews with members of the user agencies. Similar to but more in-depth than the survey, the agencies describe their use of CRIMES and other information systems. The interviews uncovered information that some of the agencies had recently moved away from CRIMES as their RMS. The interviewed agencies provide an evaluation of the benefits and the shortcomings of CRIMES.

Chapter VII discusses the findings in this research and the implications for leaders of law enforcement agencies. This chapter explores the removal of political barriers, improving governance, and marketing of information-sharing resources. Recommendations for improvements include regional agencies combining RMS, governmental sponsorship and funding, raising awareness of information resources, and mandatory participation in data exchanges. The conclusion is for chief executives to find the right combination of these recommendations to apply to their agency and improve law enforcement information sharing.

II. LAW ENFORCEMENT RECORDS MANAGEMENT SYSTEMS

Like most organizations, law enforcement agencies maintain databases of information on employee personnel records, transaction records, financial records, customer information, and various other data that support the operation, effectiveness, and efficiency of the business. Law enforcement is similar to other industries in need of a functional and user-friendly information system. However, there are unique characteristics and requirements for RMS that create opportunities and challenges. Some of the more common information collected by RMS includes reports of crimes and personal details on both suspected and convicted criminals. RMS also contains reports of suspicious activity that may not be criminal in nature and a personal information database on persons who report activity to law enforcement agencies. RMS usually tracks stolen and recovered property as well as items booked as evidence. A modern and robust RMS is a critical element of an effective law enforcement agency. This chapter will describe RMS users and some of the RMS functions for law enforcement agencies.

A. RMS USERS

Every law enforcement agency at the national, state, and local levels must maintain detailed records as a function of laws and best practices. Although there may still be agencies that use paper and manual record-keeping systems, most law enforcement organizations use electronic systems to store and organize these records. Agencies use RMS for investigative and reporting functions, timekeeping and workload documentation, intelligence information, employee records, property and evidence records, and various other customized sections as needed. The RMS typically has an interface that connects with computer-aided dispatch (CAD) systems. In some cases, RMS may interface with regional, state, or national databases such as the N-DEx.[21]

Every employee in a law enforcement organization is a potential user of the system. Police officers complete crime reports to document incidents from dispatched calls or self-initiated activity. Officers use field contact records to document encounters with persons

[21] Federal Bureau of Investigation, "National Data Exchange (N-DEx) System."

they meet in suspicious circumstances while on patrol. Investigators later read records of field contacts to identify possible suspects from matching crime reports. Investigators also use the RMS to find patterns of criminal activity that match their assigned cases. Investigators update information as they complete casework and add supplemental information to existing crime reports. Officers and investigators alike look at intelligence reports and research criminal history information contained in the RMS. Analysts look at crime trends to provide data for decision-making. Analysts report tactical information to patrol officers or investigators based on the research of specific individuals or locations. Administrative clerks review files for quality control and reporting of agency crime data to state or national entities. Administrators look at jurisdictional crime trends to report to governing bodies and evaluate agency workload and staffing decisions. In short, the RMS may be the essential central operational piece of every law enforcement organization. Accurate data entry and quality control are of particular importance. Data entry standards and training should consider that future RMS consumers will access this information for myriad reasons, including gathering intelligence for analysis or investigation.[22]

People outside of law enforcement agencies also have a stake in the RMS function. Insurance companies obtain copies of police reports to assist in claims investigations. Attorneys seek information from police reports to help their clients through independent investigations. Individuals seek criminal history information for employment background checks or other personal reasons. Journalists or other public interest groups may request publicly available information contained in RMS to further research projects. Governments and non-governmental organizations alike look at crime data to evaluate the safety of communities.

RMS data holds great value for law enforcement agencies and the citizens of the communities they serve. The data's accuracy and accessibility will directly affect the efficiency and effectiveness of a law enforcement agency. This information resource can also influence the safety, quality of life, and the community's economic viability.

---

[22] John Buckley, *Managing Intelligence : A Guide for Law Enforcement Professionals* (Boca Raton, FL: CRC Press, 2017), https://doi.org/10.1201/b15515.

B. RMS FUNCTIONS

The typical RMS will contain information on calls for service, documenting every time a police agency responds to a public request, including date and time. The call for service also contains location and contact information for the caller and the incident, a narrative of details gleaned from the caller, and additional details added by the call-taker, dispatcher, or assigned officer. A core component of RMS is the police reporting and case management system. When an officer completes a call for service, they may be required to prepare a crime report. If there is no crime at the incident, the officer may still complete an information report. Some systems include traffic crash reporting as a separate module. Whatever the report type, a link is established to the call for service so that any subsequent investigation can also access that original call information. The case management module tracks the investigative functions and progress of a criminal investigation. This information might include the investigator's name and assignment and the case status, such as open, pending, cleared, or closed.

Crime or information reports are valuable sources of information. The reports contain names, addresses, phone numbers, vehicle descriptions, and a free form narrative giving details of incidents. The free form narrative may be as important as any other RMS piece because it can contain a limitless description of events that cannot fit neatly into other required fields. The narrative provides human context to the data because it allows the documentation of suspicions or conclusions based on the officer's experience. Undesirably, the narrative can also allow incorrect assumptions or bias to enter the reporting system.

Another RMS function is to keep records on individual persons, including victims, witnesses, property owners, and suspects. This information comes from the crime and information reports completed by officers during calls for service. Self-initiated activities may also generate a report, such as when an officer observes a drunk driver and makes an arrest. Name records are a valuable tool for investigations because of the connections that can be made between persons, locations, and property. Officers often locate fugitives from justice by conducting a comprehensive search of name records and locating known addresses and associates for the wanted person.

The field contact record, also known as a field interview record, is a non-criminal report of contact between an officer and a person who may or may not be the subject of an investigation. An example of a field contact record might occur when an officer encounters a person walking in a business district during the nighttime. Although the officer observed no crime, they document the date, time, the person's identifying information, and a narrative to describe the encounter. Investigators review field contact records to find potential criminal suspects, or in some cases, to provide an alibi.

RMS also contains vehicle records, which can associate persons who are not the vehicle's registered owner with a vehicle at a given date and time. Property records can help identify business owners after hours or the owner of stolen property located during investigations. Evidence records sustain the documented chain of custody and help investigators in tracking characteristics of evidence without physically observing the item.

A robust RMS may contain modules such as traffic warnings and citations, personnel records, civil process records, protective order records, permits or business licenses, internal affairs records, and equipment management. An ideal system will also contain built-in administrative or statistical reports and analytical tools for crime analysis.[23]

The Law Enforcement Information Technology Standards Council (LEITSC) provides detailed specifications for law enforcement RMS to provide a starting point for agencies developing requests for proposals (RFP).[24] LEITSC published *Standard Functional Specifications for Law Enforcement Records Management Systems* to help agencies lower the costs of implementing and maintaining systems and encourage information sharing.[25] The LEITSC recommendations help agencies prepare for the procurement of new or replacement systems. This information likely guides vendors as they research and develop systems to present to the market.

---

[23] Law Enforcement Information Technology Standards Council, *Standard Functional Specifications*.

[24] Law Enforcement Information Technology Standards Council.

[25] Law Enforcement Information Technology Standards Council.

C. BIG BUSINESS FOR RMS VENDORS

Because every law enforcement agency is likely to utilize an RMS, the industry is full of potential vendors. A quick search of the internet reveals dozens of companies that provide RMS for law enforcement. The research found herein reveals many different systems in use in the state of Texas. One can argue that competition is good for the market because it can stimulate innovation and keep prices lower. However, one problem with having so many different choices in the RMS market is creating multitudes of different systems, most of which do not directly share information with each other. Although basic standards are well documented, including the need to share data with other agencies' systems, most companies produce "off-the-shelf" versions that must fit into an existing workflow. Customizations to these systems create added costs to the agency. Other systems may be custom built to fit an agency's wants or needs and the whims of technology influencers who may or may not possess the actual expertise to make informed decisions. Vendors are happy to build and happier to bill, especially with lucrative maintenance agreements that guarantee company revenue for years, regardless of product performance.

D. CHALLENGES FOR AGENCIES

Law enforcement executives such as Chiefs and Sheriffs are frequently the officials who decide on system acquisitions. Often lacking the expertise on how a good RMS should work, these officials are left to conduct their own research or listen to vendor presentations and pick the option that seems most cost-effective while meeting minimum requirements. For complex RMS in larger agencies, it may become necessary to hire a consultant to navigate the entire process from RFP to implementation. The costs add up quickly, and taxpayers are left footing the bill for systems that may duplicate services among agencies in the same jurisdictional boundary. Knowing that these systems may not be able to communicate with each other, on the surface, appears to be wasteful. In some cases, such as the FBI VCF debacle, millions are spent on systems that epically underperform and fail to create a viable information system.[26]

[26] Claudia Irigoyen, "The FBI Virtual Case File System," Centre for Public Impact, June 20, 2017, https://www.centreforpublicimpact.org/case-study/fbi-virtual-case-file-system/.

So what makes it so challenging to create and use a statewide or nationwide RMS for law enforcement? The answer to this piece of the homeland security puzzle is complicated. RMS contains valuable and sensitive information. Much of RMS data is not public information, although state laws vary widely on what is or is not publicly disclosable. A great deal of RMS information is potentially incriminating or embarrassing or could expose a person to identity theft if revealed to nefarious actors. Therefore, the data's privacy and protection must be a paramount consideration from the RFP through end-user access control. This research assumes that database security is of the utmost importance to agencies when considering RMS acquisition and ongoing use. Political, jurisdictional, and ownership questions also create obstacles to integration and sharing data. This thesis sorts through these challenges to develop recommendations for agencies to share information more efficiently, including their RMS.

E. SUMMARY

RMS serves a critical role in the law enforcement function, both for internal and external stakeholders. After the events of September 11, 2001, the intelligence and law enforcement communities were criticized for failing to connect separate pieces of information that could have prevented the terrorist attacks on the United States. Some of the information that can protect our communities and our nation lies with the vast data gathered by local law enforcement agencies. What follows next is an examination of the most common ways that law enforcement RMS is shared and some other methods for data collection.

III. LAW ENFORCEMENT INFORMATION COLLECTION AND SHARING

Law enforcement agencies share and access information in a variety of different ways. The method or platform used is dependent upon the nature and origin of the data. This chapter will outline the most common sharing platforms and some advantages or limitations of each.

A. NATIONAL CRIME INFORMATION CENTER

One of the earliest electronic platforms for sharing law enforcement records was the National Crime Information Center (NCIC). In 1967, the FBI launched NCIC to share information between participating agencies regarding stolen cars and license plates, stolen guns, and wanted persons.[27] NCIC has since grown into a national database housing millions of records and processing as many as 17 million requests for information per day.[28] Nearly every law enforcement agency in the United States uses NCIC.

NCIC follows strict security controls and requires agencies to comply with many rules to maintain access to enter and retrieve information. These rules restrict the type of information that is entered into the system. Generally, this includes persons who have active warrants, stolen vehicles, stolen property serial numbers, missing persons, and persons who present a danger to law enforcement. However, the rules provide a rigorous process for ensuring that data is entered correctly and acted upon quickly to ensure the information system's integrity.

NCIC works very well to share information about wanted or missing persons or stolen vehicles. The narrow focus and strict controls make NCIC a valuable tool for law enforcement across the country. However, these limitations prevent the use of NCIC as a research tool for investigators. For example, a wanted person's record in NCIC does not contain details about the crime; instead, it is merely a verification that a warrant exists. The

[27] Federal Bureau of Investigation, "National Crime Information Center (NCIC)."

[28] Federal Bureau of Investigation.

record focuses on identifying the person, the entering agency, and a related agency case number. The same holds for property and vehicle records. Therefore, NCIC is an excellent platform to locate persons or property nationwide, but not as useful when trying to research crime trends, travel patterns, or operation methods of criminal or terrorist organizations.

Many states have similar and connected systems for locating persons and property. Texas law enforcement uses the Texas Crime Information Center (TCIC). The Texas Department of Public Safety (TxDPS) manages TCIC, which works alongside NCIC and may contain the same records. Law enforcement agencies are more likely to travel within the state to bring people in on misdemeanor crimes, so TCIC includes more misdemeanor warrants than NCIC. The limitations of TCIC are similar to NCIC in that it is a repository for missing or stolen property records and wanted and missing persons. TCIC also contains information on registered sex offenders in the state, alerts on dangerous criminals, and the presence of a protective order.[29]

NCIC, TCIC, and other similar databases are vital tools for law enforcement. They provide easy access to criminal information from anywhere in the country. These databases are accessed millions of times per day by thousands of different agencies. The limited scope of information contained in these records prevents these platforms from being used as research tools. However, they do an excellent job of maintaining an easily verifiable database of information and can serve as a model for a nationwide information-sharing network that could have a broader array of data.

B. FUSION CENTERS

The events of 9/11 revealed that, among other things, federal, state, and local agencies charged with some aspect of keeping our country safe from criminals and terrorists were unable to put together the information needed to stop the attacks that occurred. A new mindset developed that caused the creation of the Department of Homeland Security. This new thinking spurred the development of fusion centers beginning in 2004. The DOJ defines a fusion center as a "collaborative effort of two or

[29] "Texas Crime Information Center (TCIC)," Texas Department of Public Safety, accessed November 8, 2020, https://www.dps.texas.gov/administration/crime_records/pages/tcic.htm.

more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity."[30] Fusion centers seem like an excellent idea to solve the problems of information sharing. Their definition includes criminal activity and terrorist activity, which has appeal at the local and federal level. However, the literature on this topic reveals that the fusion center model also has significant limitations.

Fusion Centers developed across the country in different forms. Initially, there was little guidance to direct the structure of the organizations. This organic development has led to similar problems as before 9/11. Disconnects are inherent in systems developed without consulting other similar systems and with little anticipation of connectivity. As of January 2021, there were 80 fusion centers spread out across the United States and its territories.[31] Several states have more than one center, including Texas, which has eight.

Some sources challenge the effectiveness and efficiency of fusion centers. One researcher identified a lack of a federated search system in at least one-third of fusion centers examined.[32] This essential tool, which allows the user to search across multiple databases using a singular input, seems intuitively necessary for efficiency. In 2012, a Senate investigation into fusion centers issued a highly critical report of centers' design and operations. This report outlined several criticisms and suggestions for improving fusion centers. Among the more harsh criticism was a scathing statement that "[fusion] centers themselves have fallen short of developing the capabilities necessary to meaningfully contribute to the Federal counterterrorism mission."[33] This statement is

---

[30] Global Justice Information Sharing Initiative, United States Department of Justice, *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era* (Washington, DC: U.S. Department of Justice, 2006), https://it.ojp.gov/documents/fusion_center_executive_summary.pdf.

[31] "Fusion Center Locations and Contact Information," Department of Homeland Security, April 1, 2011, https://www.dhs.gov/fusion-center-locations-and-contact-information.

[32] Jody R. Wormet, "Federated Search Tools in Fusion Centers : Bridging Databases in the Information Sharing Environment" (master's thesis, Naval Postgraduate School, 2012), http://hdl.handle.net/10945/17480.

[33] Senate Permanent Subcommittee on Investigations, *Federal Support for and Involvement in State and Local Fusion Centers:*, 83.

disheartening because state and local governments developed fusion centers with this very mission at the forefront of their existence.

The ACLU criticizes fusion centers for lack of a "proper legal framework."[34] While this statement intends to be critical of the lack of oversight in Constitutional regulation, it also speaks to the lack of uniform operation standards. With 80 separate fusion centers working, a lack of standards could be a significant hindrance to information being shared uniformly across these platforms.

The outlook on fusion centers is not all negative. A House committee on homeland security issued a report in 2013 that was more optimistic. The committee found that one of the fusion center network's strengths was a unique expertise and local perspective that each center brings to the process. The report concluded that "The Federal Government and State and local stakeholders must continue to provide the support that fusion centers require to continue to grow and develop, enabling the National Network to reach its full potential as a National asset and homeland security partner."[35]

Fusion centers attempt to bridge the intelligence gaps between federal, state, and local homeland security-focused agencies, including law enforcement. However, it is still unclear if individual law enforcement agencies are knowledgeable enough to adequately utilize fusion center products. Another question is whether or not they are willing and equipped to contribute information. If the answer is no, then it is unlikely that fusion centers can make significant contributions to improving homeland security. Although many individual success stories abound, there is no precise data to show that this model is working as intended.

---

[34] German and Stanley, *What's Wrong with Fusion Centers?*

[35] Michael McCaul and Peter King, *Majority Staff Report on the National Network of Fusion Centers* (Wahington DC: U.S. House of Representatives, 2013), https://www.archives.gov/files/isoo/oversight-groups/sltps-pac/staff-report-on-fusion-networks-2013.pdf.

C. REGIONAL INFORMATION SHARING SYSTEMS (RISS)

The RISS organization consists of six regional centers across the United States that provide many information and resource sharing services. These RISS regions were established between 1973 and 1981.[36] A regional law enforcement policy board manages each center, and Congress funds the overall program.[37] The RISS model differs from fusion centers in that RISS deals primarily with criminal matters such as drug trafficking, organized crime, and gang activity. Fusion centers tend to focus more on connecting federal information to state and local agencies, focusing on terrorism, critical infrastructure, public health, and emergency response.[38]

The RISS web portal contains crime bulletins from regional member agencies and generalized criminal intelligence publications. RISS also contains educational resources, including videos and publications designed to increase law enforcement knowledge about crime trends. RISS also provides information about law enforcement technology and can connect agencies with resources for loaned equipment such as automated license plate readers or investigative tools such as cameras and other surveillance equipment. The RISS web interface is a dashboard that contains links to other investigative resources such as N-DEx, although the user must be a subscriber to those individual resources.

A unique tool of RISS is the Officer Safety Event Deconfliction System, called RISSafe. RISSafe is a tool that law enforcement agencies can use to search for overlapping investigations. Besides avoiding interference in other agencies' investigations, RISSafe can prevent dangerous cross-agency encounters. A key point of deconfliction is that all agencies with overlapping jurisdictional boundaries must participate. Otherwise, the system has considerable gaps in data that could render a single agency's participation useless. Lack of knowledge about and lack of participation in these large information sharing systems is common among law enforcement agencies.

---

[36] Regional Information Sharing Systems, "About the RISS Program."

[37] "Fusion Centers," Department of Homeland Security, July 6, 2009, https://www.dhs.gov/fusion-centers.

[38] Department of Homeland Security.

D. DATA EXCHANGES

A data exchange serves as a repository for criminal information from numerous law enforcement agencies across different jurisdictional boundaries. Agencies can search, link, and share this information from other subscriber agencies. There is no mandate for agencies to participate in such data exchanges. An agency must provide an electronic interface between the agency RMS and the data exchange to share information. This interface creates added cost to the local RMS.

The National Data Exchange (N-DEx) is the national example of this model. N-DEx works with various state agencies to provide information across a wide array of law enforcement organizations. In Texas, for example, the Texas Data Exchange (TDEx) is managed by TxDPS and provides the portal for state agencies to access N-DEx. TDEx vets and controls individual and agency access to the system, which eases the administrative burden on N-DEx. To share data, the agency shoulders the burden of integration costs from their RMS vendor.[39] Depending on the RMS architecture and size, this cost could vary greatly. TDEx and N-DEx expect subscriber agencies to contribute information; however, being a contributor does not appear to be a mandatory usage condition. This expectation is the primary and perhaps the only motivation to incur the associated costs of integration. For smaller and poorly funded agencies, the cost of building the interface could be a barrier to entry.

Many Texas agencies surveyed were familiar with TDEx and N-DEx. AT the time of this writing, TDEx recently changed vendors, which created problems for agencies that use proprietary software for their local RMS. In the best cases, the vendor will work with the new TDEx vendor to ensure the RMS can connect. However, in some cases, the vendor charges a fee to write the appropriate code for the interface without revealing the source code to the TDEx vendor. If the agency cannot absorb the extra expense, their connection

[39] Federal Bureau of Investigation, "National Data Exchange (N-DEx) Data Integration FAQs" (Washington, DC: Federal Bureau of Investigation, November 16, 2016), https://www.fbi.gov/file-repository/ndex_data_integration_faqs.pdf/view.

is lost, and they no longer contribute information. As with RISS, the participation issue becomes a challenge as agencies reject the use of exchanges.

The Naval Criminal Investigative Service (NCIS) maintains the Law Enforcement Information Network Exchange (LInX), representing another information-sharing source. According to LInX, over 2,000 agencies in the United States use this system.[40] LInX maintains a partnership and connectivity with N-DEx and shares some data across the two platforms. Although LInX reports many subscribers and widespread use across the country, few Texas agencies surveyed were using this system.

Data exchanges hold the potential to be valuable tools for law enforcement investigators and analysts, on the condition that agencies who subscribe to access the data also contribute like information. Additionally, agencies in similar geographic areas or who share jurisdictional boundaries should coordinate as to which system(s) they will use for information sharing. If these mutual agreements and consistency in contributing information are lacking, data exchanges leave large gaps in their networks and less effective for those who choose to use them.

E. DATA WAREHOUSES

A different model for information sharing is called a data warehouse. Data warehouses gather large amounts of historical data stored for research and analysis. The ideal warehouse model is the democratization of data that allows many users to investigate the information within without a choke point that limits otherwise authorized availability. Data warehouses are particularly useful for the analysis of large amounts of data. They are also used to access individual records.

The Colorado Information Sharing Consortium (CISC) is one such model. CISC serves nearly eighty law enforcement agencies who contribute and access data from the system.[41] LexisNexis Risk Solutions, a company that provides various data and analytics

---

40 "LINx/D-Dex," Naval Criminal Investigative Service, accessed January 10, 2021, https://www.ncis.navy.mil/Mission/Partnership-Initiatives/LInX-D-Dex/.

41 "Member Agencies," Colorado Information Sharing Consortium, accessed December 13, 2020, https://cisc.colorado.gov/member-agencies.

solutions worldwide, hosts the Regional Data Warehouse (RDW) for CISC. LexisNexis performs the foundational data integration into the RDW for subscriber agencies and serves as the gatekeeper via an application programming interface (API). The API allows users to analyze the data, and an additional application is available for deeper analytic capabilities.

Members of the CISC also have access to enhanced investigative tools, including a team of analysts. CISC also provides a portal to N-Dex and LInX. The CISC provides subscriber agencies with an in-depth resource of information to help criminal investigators and crime analysts. In case of RMS change or failure, the CISC can restore a contributing agencies' data, which reduces risk to the individual organization.[42]

As early as 2002, the Chicago Police Department (CPD) began work on a data warehouse that allows access to agencies from around the state and surrounding areas. The Citizen and Law Enforcement Analysis and Reporting (CLEAR) project give agencies throughout Illinois access to an RDW maintained by the CPD. After a pilot program was successful, the CPD embarked on a vigorous campaign to allow CLEAR access to any other area law enforcement agency at no cost.[43] CPD also provided train-the-trainer sessions for the adopting agencies. This robust marketing combined with the zero cost for using the system made joining CLEAR an easy option for law enforcement agencies, and nearly four hundred agencies use CLEAR.[44]

The City of Chicago also provides a data portal that includes a section for public safety information. This portal extracts CLEAR data to give the public free access to datasets such as all crimes reported, crime maps, and even police station locations.[45]

---

[42] David M. Shipley, CISC/LInX RM Executive Director, provided the author with information on CISC.

[43] Wesley Skogan and Susan Hartnett, "The Diffusion of Information Technology in Policing," *Police Practice & Research* 6, no. 5 (December 2005): 401–17, https://doi.org/10.1080/15614260500432949.

[44] "Citizen and Law Enforcement Analysis and Reporting (CLEAR)," Government Innovators Network, accessed December 13, 2020, https://www.innovations.harvard.edu/citizen-and-law-enforcement-analysis-and-reporting-clear.

[45] See "Chicago Data Portal," Chicago Data Portal, accessed February 25, 2021, https://data.cityofchicago.org/browse?category=Public%20Safety..

CLEAR represents an excellent example of public engagement and transparency in data collection and dissemination and provides law enforcement officers a tool to research crimes and criminals who jump jurisdictional boundaries of a heavily populated metropolitan area.

F. SAME RMS VENDOR

Although Texas municipal police agencies were the primary research area for this thesis, the author also spoke to the Ogden Police Department in Utah.[46] Ogden police use the same RMS vendor as 13 other police agencies in the same geographical area. The department reported that officers could view, but not make changes to, RMS data from these neighboring agencies. This data includes such information as crime reports, arrest reports, name records, and vehicle records. The department considers the ability to share information with other agencies a benefit because many of the criminals they deal with in Ogden cross into other nearby jurisdictions.

There are likely other examples of agencies collaborating on information sharing by using the same vendor. CRIMES was another potential example of this type of partnership. However, as will be discussed in Chapter VI, the ability to share information on the CRIMES RMS platform was not available to agencies at the time of this research. Nonetheless, this model holds promise for agencies with the foresight to work together before making an RMS acquisition.

G. PRIVATE DATA RESOURCES

Several companies engage in the collection and dissemination of data as a for-profit enterprise. Transunion offers a product called TLOxp for law enforcement use. TLOxp provides subscribers with an extensive resource of data on people, businesses, and assets and claims to have data on over 95% of the United States population.[47] This data includes phone numbers, addresses, driver's license information, social security numbers, and

---

[46] Chief of Police Eric Young, of the Ogden, Utah Police Department, provided information on the RMS used by multiple agencies in the Ogden geographical area.

[47] "Law Enforcement," TransUnion, accessed January 14, 2021, https://www.tlo.com/law-enforcement.

employment information. TLOxp also provides historical information to include previous addresses, old phone numbers, vehicle ownership history, and prior familial relationships. Agencies pay a subscriber fee based on the amount of information accessed per month. The majority of law enforcement agencies surveyed for this thesis were familiar with and used TLOxp for investigative research.

There are several other investigative databases on the market. LexisNexis Risk Solutions provides a product called Accurint for Law Enforcement. Accurin is similar in many ways to TLOxp. Thompson Reuters has another similar database called CLEAR. The Thompson Reuters database product should not be confused with CLEAR, which is a facial recognition and secure identification platform. Thompson Reuters CLEAR is also different than the previously described data warehouse in use by the Chicago police. TLOxp, Accurint, and Thompson Reuters CLEAR all provide similar services, but each has its pros, cons, and pricing schema.

Many investigative solutions from non-governmental entities exist, and each can offer an alternative to traditional government-operated information networks. However, many companies rise and fall with good or bad leadership or with rapid technology changes that render once innovative solutions quickly irrelevant. The private market for data can be perplexing when seeking solutions to help with investigations or gathering intelligence. Law enforcement leaders should seek solutions based on an analysis of investigative and intelligence needs rather than making purchasing decisions based on vendor recommendations. It may also be prudent for agencies to avoid long-term contracts and frequently re-evaluate information services' usefulness. Adequately vetted and sourced, privately owned data sources are valuable tools for law enforcement investigation and intelligence.

H. PERSON-TO-PERSON CONTACT

Law enforcement should not overlook the value of keeping personal contact with human sources in other agencies. Person-to-person contact, also known as human intelligence or HUMINT, is one of the oldest intelligence methods and maintains relevancy even with modern computing proliferation. In this research, several organizations reported that investigators often call neighboring agencies to inquire about specific criminals or

criminal activity. One study found patterns in the way investigators contacted other agencies for information, including geographic proximity and similar size.[48] The geographic relevancy of HUMINT seems intuitive since crime trends often follow regional patterns, irrespective of jurisdictional boundaries. If investigators tend to contact peers in regionally located agencies, it also seems logical to conclude that these agencies should share electronic records. By sharing records, the agencies can take advantage of computing technology to analyze large area crime trends and identify individuals or groups responsible for organized criminal or terrorist activity. However, in addition to the automated sharing of electronic records, personal contact between agencies should be encouraged. A good conversation can give more context to the situation and build trust and rapport between agencies.

I. SUMMARY

Information is gathered and shared by law enforcement agencies in various ways, both locally and on a national scale. The array of choices may be one factor inhibiting the effectiveness of information sharing. Agencies are left to decide what resources they will subscribe to and, significantly, what resources to which they will contribute information. Law enforcement should develop a common strategy to determine how agencies will share information. One alternative could be an extensive, federated records management and sharing system operated by a government agency. The next section will examine one such case; how an ambitious attempt to consolidate nationwide systems turned into an embarrassing and expensive debacle.

48 Aki Roberts and John M. Roberts, Jr., "The Structure of Informal Communication Between Police Agencies," *Policing: An International Journal of Police Strategies & Management* 30, no. 1 (2007): 93–107, https://doi.org/10.1108/13639510710725640.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CASE STUDY: THE FBI VIRTUAL CASE FILE

Managing and sharing law enforcement records within a single interconnected system seems like an idea that could solve the problem of sharing data on a national scale. However, it is an idea with a troubled history. It is crucial to examine the lessons of successes and failures in technology aspirations and upgrades for law enforcement to form better recommendations for the future. Scholars of information technology management have studied and analyzed one such project, known as the FBI's Virtual Case File (VCF), and later, the Sentinel program. The VCF project started as an ambitious and laudable attempt to update an antiquated and disconnected system that hampered one of the nation's largest law enforcement agencies' efficiency and effectiveness. It ended as a generally recognized failure and a monumental waste of taxpayer money. Sentinel repeated some of the missteps made during the VCF project but was eventually righted through innovative project development and management. Both systems provide valuable lessons for the creation of extensive records management and sharing systems.

A. TRILOGY

Well before the events of 9/11/2001, the FBI began working on upgrading its technology systems. The overarching project, which came to be known as Trilogy, consisted of three major components. The first was a massive upgrade of outdated hardware, including the desktop computers and servers used by field agents.[49] The second piece was creating a web-based system that would allow for widespread sharing of information among agents. The third piece of Trilogy was to create a case information management system that could be used by agents spread out all across the United States. This system was the VCF, which was arguably one of the most valuable pieces of the upgrade.

Before the Trilogy project proposal, FBI agents worked on outdated pieces of equipment. They relied on paper files for many transactions due in part to an arcane

[49] Irigoyen, "The FBI Virtual Case File System."

electronic filing system and a general organizational resistance and distrust of existing electronic systems.[50] Agents manually scanned papers into electronic systems but also kept paper backups. By the late 1990s it was evident that the Bureau required a new organizational system to improve efficiency. This forward-thinking vision meant new computers, new infrastructure, and a new records management system that agents could trust to be reliable and that could connect the information contained in 56 separate field offices and nearly 400 resident agencies across the country.

In 2000, Congress approved $379.8 million for a proposal to span three years, a project that would become known as Trilogy.[51] The project required two contractors because it was considered too large a project for one contractor to complete. Field offices received new desktop machines and servers as the hardware and software technology upgrades were completed; however, it took until April of 2004 to complete the infrastructure portions of the project.[52] The FBI enhanced the communications infrastructure and installed secure and robust communication transportation networks. The last Trilogy piece, which was supposed to have been concurrently developed and implemented, was a records, evidence, and case management system.

B. VIRTUAL CASE FILE

Before conceptualizing the Trilogy project, the FBI used a program called Automated Case Support. As a part of the Trilogy enhancements, the FBI envisioned a system that would combine the functions of managing the various pieces of information required to be kept during a case investigation. One part of the system is records management, which is the fundamental recording and storing of an investigation's detailed documentation. Evidence management is another part of the file and includes the documentation of the collection and storage of case-related evidence. A third critical piece

---

[50] Harry Goldstein, "Who Killed the Virtual Case File? [Case Management Software]," *IEEE Spectrum* 42, no. 9 (September 2005): 24–35, https://doi.org/10.1109/MSPEC.2005.1502526.

[51] U.S. Department of Justice, Office of the Inspector General, *The Federal Bureau of Investigation's Management of the Trilogy Information Technology Modernization Project*, Audit Report No. 05–07 (Washington, DC: U.S. Department of Justice, 2005), https://oig.justice.gov/reports/FBI/a0507/intro.htm.

[52] U.S. Department of Justice, Office of the Inspector General.

is case management, which is the organization of case files for prosecutorial presentation, the records of assignments for accountability, and the tracking of the investigation's disposition.

VCF was the solution to take care of all of the functions for investigation and hold the information in an environment that could be shared across all agency offices. In other words, an agent working in one part of the country could conceivably access records of an investigation that was occurring in an entirely different office hundreds of miles away. This type of system was precisely the type of information sharing that did not exist at the FBI at that time but was sorely needed. While this concept may seem simple in modern times, in 2000, the internet was not nearly as robust, and secure technologies were much less sophisticated. The VCF was a bold project, poised to create a nationwide network of information sharing for the FBI in a manner unlike anything seen before.

C. PROBLEMS

Unfortunately, the FBI appears to have inadequately organized the planning of the VCF portion of the project. The concept of agile development may have been a foreign term to those within the FBI tasked with driving the system's development. For example, in 2003, there were over 400 change requests after the code was 25 percent completed, leading to tensions between the developer and the FBI.[53] Another major factor was the events of 9/11, which happened as the Trilogy project was just getting started. 9/11 highlighted the problems with the lack of information sharing within the FBI and spurred the agency to fast track Trilogy's implementation and the development of the VCF. Congress approved additional spending to speed up the development, but the contracts failed to specify product acceptance criteria.[54] In other words, the FBI did not and perhaps could not define what exactly they expected from VCF and when it would expect the finished product.

---

[53] Jack T. Marchewka, "The FBI Virtual Case File: A Case Study," *Communications of the IIMA* 10, no. 2 (2010): 6.

[54] Goldstein, "Who Killed the Virtual Case File?," 29.

The Office of the Inspector General (OIG) issued a report in 2005 that outlined problems with the Trilogy development.[55] One was the lack of an enterprise architecture plan to describe how the technology helps the organization accomplish its goals. The FBI lacked a detailed plan to define the requirements from the beginning of the project through completion.[56] This disorganization created a series of new problems as definitions changed and conflicted with the previously completed work. The problem of the numerous change requests exacerbated the evolving design requirements. Project management was also an issue, as several changes in managers occurred during the VCF development. In 2002 alone, there were four different information technology managers at the FBI.[57] This lack of leadership continuity within the core segment of the organization responsible for managing VCF compounded many problems in developing a useful product. The OIG found other issues, including unrealistic schedules for the required tasks and a lack of acceptable project integration practices.[58]

The various problems outlined by the OIG combined to add both cost and delays to the project. Although the infrastructure enhancements eventually came to fruition, the VCF development was never fully completed. The core piece of technology meant to solve the legacy issues within the FBI records system failed to meet even minimum expectations and was eventually abandoned in 2005. The project's estimated sunk cost was $105 million, mostly in VCF code that was unusable.[59]

D. THE SENTINEL SOLUTION

Although the VCF project died, the need for a case management solution still existed. The FBI almost immediately regrouped and set out with a similar mission to

---

[55] U.S. Department of Justice, Office of the Inspector General, *The Federal Bureau of Investigation's Management*.

[56] Goldstein, 33.

[57] Goldstein, 30.

[58] U.S. Department of Justice, Office of the Inspector General, *The Federal Bureau of Investigation's Management*.

[59] Goldstein, 25.

develop a singular system to manage cases and share information across all FBI offices. The new plan, called Sentinel, was bold and expensive, with an estimated cost of $425 million over four implementation phases, each lasting 12–16 months.[60] Sentinel got off to a good start in 2006, and the contractor completed phase one on time. Unfortunately, this project started to bog down in phase two, and then FBI Director Robert Mueller requested the OIG to audit the process and the contractors. The OIG expressed "serious concerns about the progress of the FBI's Sentinel Project."[61] The FBI took delivery of several Sentinel segments by phase three, but it was evident that the software was not working as intended.

In December 2008, Mueller brought in Chad Fulgham from the private sector to serve as the chief information officer, taking advantage of his corporate world experience. Fulgham eventually released the original contractor and brought the project back in-house to manage. Fulgham adopted an agile development strategy and completed Sentinel within the allotted budget.[62] Although agents reported some problems after implementation, a 2014 audit report concluded that most Sentinel users had a positive experience and the software was adequately performing the required functions.[63]

E. LESSONS

The harsh lessons learned from the VCF fiasco and the FBI's resultant change of strategy can be a guidepost for other law enforcement agencies in developing large, shared systems. From the beginning, there must be a commitment from leadership to embrace an agile development process and to define the essential elements that the agency's RMS must contain for a minimally viable product. In other words, start with a common-sense

---

[60] U.S. Department of Justice, Office of the Inspector General, *Status of the Federal Bureau of Investigation's Implementation of the Sentinel Project*, Report 10–22 (Washington, DC: U.S. Department of Justice, 2010), 1, https://oig.justice.gov/reports/FBI/a1022.pdf.

[61] U.S. Department of Justice, Office of the Inspector General, 6.

[62] John Foley, "FBI's Sentinel Project: 5 Lessons Learned," InformationWeek, August 2, 2012, https://www.informationweek.com/applications/fbis-sentinel-project-5-lessons-learned/d/d-id/1105637?

[63] U.S. Department of Justice, Office of the Inspector General, *Audit of the Status of the Federal Bureau of Investigation's Sentinel Program*, Audit Report 14–31 (Washington, DC: U.S. Department of Justice, 2014), 23, https://oig.justice.gov/reports/2014/a1431.pdf.

approach to acquiring a system that will function with the agency mission in mind rather than trying to define abstract functions for end-users. Leadership should be asking questions such as, “What problem do we need to solve, and can we do it with technology?”

A simple example of this scenario is figuring out a way to track an individual’s criminal activities across several state lines. If a truck driver is suspected of kidnapping in Oklahoma City, how can that information be available to an investigator looking for a missing person in Albuquerque? The problem presented here is how to develop a lead when the suspect is highly mobile. The solution is to ensure that two separated agencies can see the same information and detect similarities using a system that automatically flags the possible connections.

The development of Sentinel created the solution that the FBI was seeking for records management and data sharing across a wide geographical area. However, it was a very costly system and took over six years to develop into a useable product. Sentinel solved a problem for one law enforcement agency but did not address information sharing across multiple agencies. The Sentinel solution’s complexity creates valuable knowledge for other organizations that desire to create similar extensive information management and sharing networks.

The looming question here is whether a large shared RMS system is practical for nationwide use by state and local officers, given the complexity of law enforcement duties in the thousands of different agencies across the United States. Who would run such a system, and what laws would govern it? With current information systems, the possibilities are widely varied and inconsistent. Planners must consider the numerous vendors, data exchanges, and data warehouses that factor into any new project. Differing political jurisdictions are likely to have unique records management requirements, and varying state laws could interfere with interstate sharing. Privacy laws could hamper federal agencies from sharing information with state and local police departments. Lessons learned from the VCF debacle and the Sentinel project point towards the exploration of alternative solutions.

Municipal police organizations comprise the largest number of independent law enforcement organizations in the country. These organizations work under differing state and local laws but have a significant degree of similar duties. This research will look

primarily at Texas agencies to reduce the variance in laws between states and identify criminal and intelligence system sharing and alternatives. The next chapter examines Texas police departments' information systems and how those systems and agencies communicate with each other.

THIS PAGE INTENTIONALLY LEFT BLANK

V. RESEARCH METHODOLOGY-SURVEY

This research was designed to find better ways that law enforcement can share information. It is essential to get an expansive view of what is already happening in this realm in order to find out where to improve. Texas has over 1900 different law enforcement agencies, with over 700 of those being municipal police agencies.[64] Law enforcement organizations include the state police, county sheriff's offices, constable's offices, municipal police departments, and dozens of other miscellaneous agencies that perform essential law enforcement functions. Texas has one of the largest varieties of law enforcement agencies, and each type has both unique and overlapping jurisdiction and functions with other agencies. To narrow the scope of this research, the focus of interviews and surveys were municipal police agencies in Texas. This study looks at municipal police departments to better understand how organizations with similar functions interact and what tools they use to gather intelligence or investigate crimes.

A. SURVEY RESULTS

The survey portion of this research was designed to find answers to reveal the variety of different RMS, the frequency of automated information sharing, and other data sources for investigation or intelligence. If the agency responded that they used CRIMES as their RMS, the survey revealed a second section. The second set of questions elicited additional information on CRIMES from agencies not part of the separate interview research. Police agencies that participated in the CRIMES personal interviews did not receive the survey solicitation to prevent duplication of responses. The survey request went to 642 municipal police agencies in Texas via email. There were 125 completed surveys returned. The survey responses were analyzed collectively and individually to look for patterns of information sharing or the lack thereof. The end of the survey allowed the participant to provide contact information for follow-up interviews. The follow-up

64 Brian A. Reaves, *Census of State and Local Law Enforcement Agencies, 2008*, NCJ 233982 (Washington, DC: Bureau of Justice Statistics, 2011), 15–16, https://www.bjs.gov/content/pub/pdf/csllea08.pdf.

interviews attended to the same questions as the survey while seeking clarification of the responses and expanding the answers.

1. Agency Size

The first question asked the respondent to categorize the agency's size by the number of sworn law enforcement officers. The categories were under 50, 51–100, 101–250, 251–500, and over 500. This design categorized the agency size from small to mid-sized to large. Over 73% of the responding agencies had less than 50 officers. Only one responding agency had more than 500 officers (see Table 1). There were no discernable patterns from the survey revealing whether the organization's size was a factor in that agencies' participation in a shared RMS. The same was true as to the likelihood of the organizational use of other data and investigative resources.

Table 1. Number of sworn officers

Less than 50	93	74.4%
51-100	15	12.0%
101-250	15	12.0%
251-500	1	0.8%
More than 500	1	0.8%

2. RMS Vendor

The second question asked, "What vendor does your agency use for its records management system (RMS)?" The results revealed that the 125 agencies were using 21 different RMS. Nine of the vendors appeared only once, while the other vendors appeared two or more times in the answers, as demonstrated in Figure 1.

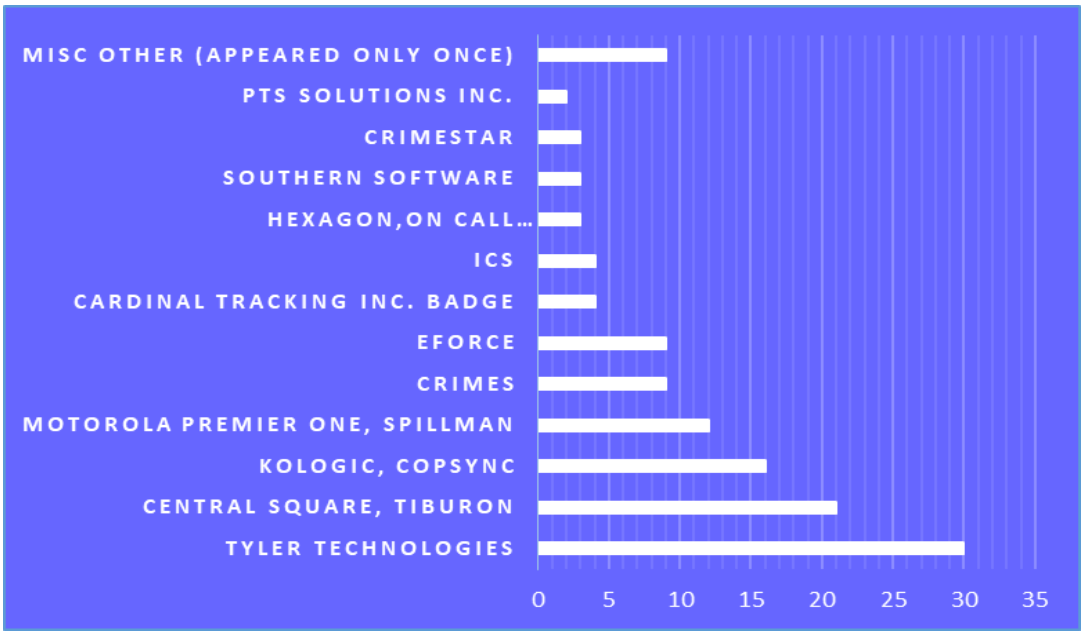

Figure 1. Number of agencies per vendor

3. Sharing RMS

The third question in the survey asked, “Does your agency share the RMS platform with another agency or agencies?” This question was designed to find out how many agencies are sharing their core RMS with another agency. The responses included the possibility that the agency shared RMS with more than one other agency. Table 2 shows the number and the corresponding percentage of agencies in each category.

Table 2. Sharing RMS

No, we are the only agency connected to this RMS.	78	62.4%
Yes, we share RMS with another law enforcement agency.	17	13.6%
Yes, we share the RMS with multiple law enforcement agencies.	30	24.0%

Analysis of these responses did not reveal any discernable connection between the organization's number of officers and the agency's likelihood to share RMS with another agency. It is possible that analysis could reveal connections between agency size and the likelihood of sharing RMS services with one or more agencies given a more extensive data set. Overall, 62% of agencies surveyed did not share their RMS with other agencies.

4. Other Sources of Information

Question number four asked, "Besides local RMS and NCIC, what other crime information databases does your agency use to conduct investigations or gain intelligence information?" This question reveals the number of agencies using other resources outside of their RMS and the types of resources most often used. One of the answer options allowed for an open-ended response to reveal potentially unknown sources of information. Some data resources were mentioned by only one agency and were not included in the summary shown in Figure 2.

The survey found that 60% of the agencies surveyed used some type of fusion center product, while 48% used N-DEx as a source of information. Less than 17% of the agencies used RISS to share or collect information for investigations or intelligence. This number is deficient considering the widespread reach of RISS, which includes the entire state of Texas. Other resources reported to be used by more than one Texas agency included TLOxp, Accurint, and Thompson Reuters CLEAR. LeadsOnline appeared in slightly more than 5% of the responses. LeadsOnline is a resource that tracks property through pawnshop records. Pawnshop employees enter the data of pawned goods, usually to comply with local or state laws that require these types of businesses to keep detailed records of transactions.

Law enforcement agencies can subscribe to LeadsOnline, which allows the agency to search the records and identify potentially stolen items.

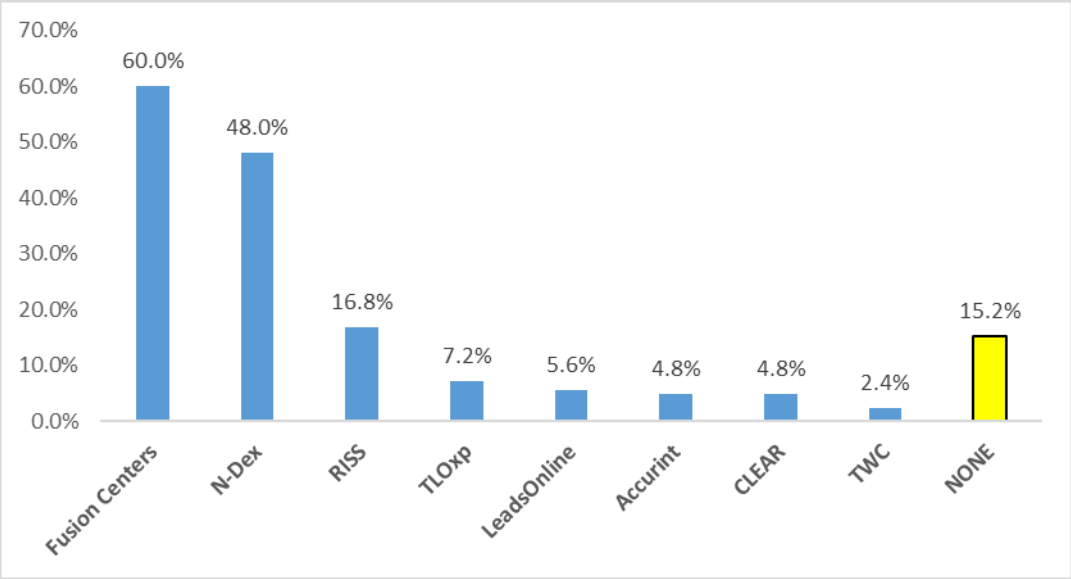

Figure 2. Agencies using other information resources

Three municipal police agencies identified the Texas Workforce Commission (TWC) as a source for information. TWC keeps unemployment insurance records that can help identify the location of suspected criminals or fugitives from justice. In some cases, TWC records can also assist in investigating fraud cases by identifying employment periods for persons who otherwise claim to be injured or unemployed.

Four of the agencies who used Kologik as their RMS also listed COPsync as an external resource for information. Kologik is the parent company of COPsync. Although COPsync officially refers to the mobile software platform by the same name, Kologik produces the RMS. The COPsync name was used interchangeably with Kologik RMS in the survey responses. Follow-up interviews revealed that because agencies on the Kologik/COPsync RMS system can see data from other Kologik/COPsync agencies, this was considered a valuable resource for investigative and intelligence information. However, the data was not included in this question analysis group because Kologik/COPsync is an RMS and not an external information source.

5. Direct Sharing Connections to RMS

Question number five solicits information on whether agencies have direct connections to share information by asking, "Does your agency directly share or provide data (such as through an interface or API) to another database such as RISS or NDE-x?" A "yes" answer left an open-ended response for the agency to report the system's name with which they were sharing information. Over 80% of the responding agencies reported they were not sharing information in this manner. The remaining responses included sharing with N-DEx, RISS, LInX, or miscellaneous other sources (see Figure 3).

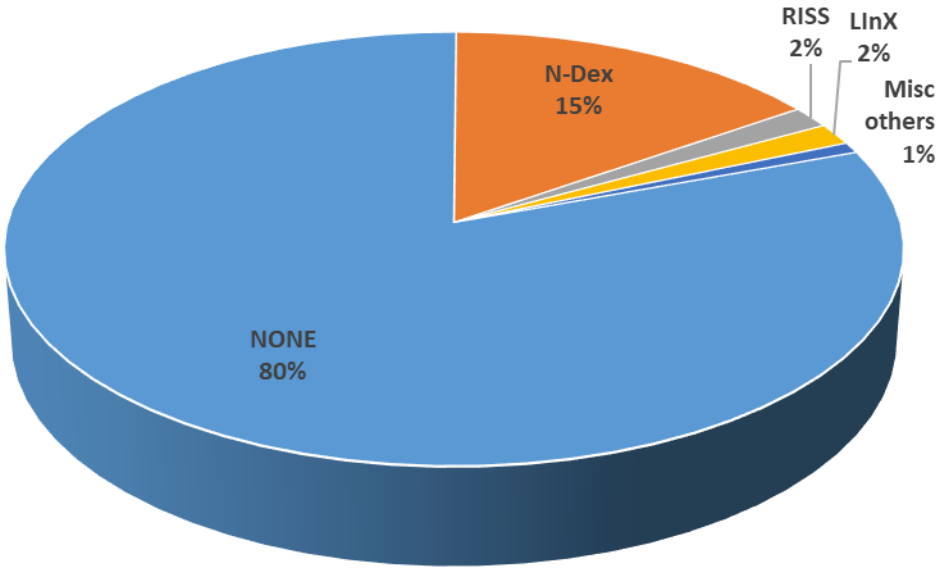

Figure 3. Agencies who share to other databases

It is apparent from this survey that the vast majority of Texas police agencies are not directly sharing data with a known information-sharing system. Additionally, out of the 60 agencies who report using N-DEx to gather information, only 19 provide information back to N-DEx through a direct connection. The implication here is that Texas agencies are far less willing or able to provide information to N-DEx than they are to access N-DEx for gathering information.

The remaining survey questions were viewable only to agencies who selected CRIMES as their RMS. An analysis of these additional survey questions is combined with the personal interview analysis and the CRIMES case study in the next chapter.

B. SURVEY ANALYSIS

This research reveals some interesting data about information sharing at Texas municipal police agencies. In this study, 125 agencies used 21 different RMS vendors. 7% of the agencies used systems that were not reported by any other agency. If 7% of all Texas police agencies have a unique individual system, there could be as many as 50 different RMS vendors used by municipal police in Texas. This diversity of systems highlights the problem of systems not connecting to each other due to an array of disconnected and sometimes proprietary systems.

Nearly 38% of the agencies reported sharing their RMS with other police organizations. A closer analysis identified that some RMS vendors provide a sharing mechanism as an inherent part of their product. However, the agencies varied in their response to whether or not they were using or were aware of that RMS vendor's sharing capability.

Right at 60% of responding agencies reported that they utilize fusion center services for additional criminal or intelligence information. The frequency of each organization's fusion center utilization was not measured in this survey and could be a future study topic. Less than half of the agencies used N-DEx as a resource. This issue was explored through personal interviews with some of the responding agencies. The primary reason for not using N-DEx was a lack of knowledge on what N-DEx can provide to investigators or analysts. Another reason for the lack of usage was the complexity of accessing the system. In Texas, the TDEx portal allows access to N-DEx. However, at the time of this study, TDEx was changing the vendor that hosts the TDEx service. Another way to access N-DEx is through the LEEP portal; however, several agencies were unfamiliar with the credentialing process to access the connection via LEEP.

A smaller number of agencies reported using RISS. Follow-up interviews revealed that some agencies simply did not see RISS as a useful solution for their everyday

investigative needs. The few police departments who do use RISS found it valuable for getting criminal information related to gangs. Others found RISS (RISSafe) very helpful as a tool for deconfliction.[65]

The Texas Workforce Commission (TWC) provides a wide variety of services to employers and employees in Texas, including training and placement services and the administration of unemployment benefits.[66] In the process of conducting business, this agency collects a great deal of data about where people are working or if they are unemployed, along with their contact information. This survey identified that TWC information contained in unemployment insurance records is subject to disclosure to police departments. TWC makes agreements with law enforcement agencies to access the data for a fee based on the number of persons who will access the data.[67]

Non-governmental agencies collect vast amounts of information and provide products used for investigative or intelligence information. These products appear to have evolved from credit reporting organizations and other companies that specialize in large volumes of personal data collection. Although this extensive data collection has been around for decades, the use of these products by law enforcement is not as prolific as expected. While some agencies were not aware of such products, others cited the cost of subscriptions as being a barrier to obtaining the service. Agencies who do not have the excess capacity in their budget are likely to view these resources as a luxury they cannot afford. The most common use for these commercial databases was locating suspects and fugitives from justice.

Perhaps the most startling information gained from this survey is that 80% of the police departments who responded reported that they did not directly share their RMS

---

[65] De-confliction describes the process by which agencies check with other agencies to see if they are investigating the same individual or group. Investigators are encouraged to run de-confliction checks before serving arrest or search warrants to reduce the chances of encountering another agency during the process, or otherwise interfering a co-occurring investigation.

[66] "About Texas Workforce," Texas Workforce Commission, August 16, 2018, https://www.twc.texas.gov/about-texas-workforce.

[67] One such agreement between the Williamson County Constable Precinct 1 and TWC can be found at https://agenda.wilco.org/docs/2017/COM/20170523_1316/17367_TWC%20Contract%20renewal.pdf

information with N-DEx, RISS, or other information exchanges. The lack of data being pushed out is an inherently obvious problem with the overall information-sharing landscape. Suppose this data holds true for other types of law enforcement in the state and other law enforcement agencies in the rest of the country. In that case, there is a large piece of missing information in the law enforcement and homeland security enterprise.

C. LIMITATIONS OF THE SURVEY

One of the primary limitations of this survey is the relatively small sample size. Given that only 19.5% of police departments responded to the survey request, there is likely information missing from this analysis. It is possible that agencies who see information sharing as an issue were more or less likely to respond to the survey, or that agencies who lack information sharing capabilities were more or less likely to report this issue.

This survey does not explore the individual customizations that vendors might apply at agencies that allow information linking between other agencies who use that same RMS. The answers reveal that this is occurring, but it is also apparent that not all agencies have the same capabilities, even when using the same software vendor. There may also be a lack of full understanding of the full RMS potential at the responding agency. For example, some agencies that reported using Kologik/COPsync responded that they could share information with every other agency that also used Kologik/COPsync. However, other agencies with the same RMS reported that they did not share RMS information. There is some discrepancy in organizational knowledge. A more in-depth study is needed to determine if each agency has a customized version of the RMS or if the users simply do not understand how to maximize the record-sharing potential.

Another limitation in this study is the type of agencies that were the subject of inquiry. The numerous Texas agencies have different law enforcement duties, but many of these functions overlap with municipal police agencies' responsibilities. The RMS and other information-sharing requirements would likely be similar in these types of agencies. However, some significant differences are bound to appear, for example, in organizations that are responsible for operating a jail. Those agencies would likely look for RMS or software systems that have a robust jail management module. The similarities in the type

of work and essential job functions of municipal police agencies reduced the need to adjust for these differing RMS and information sharing priorities.

The issue of information management is very complex, and it is possible that some respondents failed to understand the context of the questions. For example, question number four asks, “Besides local RMS and NCIC, what other crime information databases does your agency use to conduct investigations or gain intelligence information?” Some respondents included NCIC in their open-ended responses to this question. Others included Kologik/COPsync, which is very much a local RMS, albeit Kologik/COPsync connects information with other COPsync agencies.

The survey limitations do not invalidate the learned assumptions about how law enforcement records are shared. From this survey, it is clear that comprehensive information sharing between Texas municipal police agencies is not happening. The next chapter will look at the CRIMES RMS and how user agencies describe the benefits and challenges of a system used by over 50 law enforcement agencies in Texas.

VI. THE CRIMES MODEL IN TEXAS

One model to solve the problem of information sharing between law enforcement agencies is to have agencies share their core records management systems. Sharing RMS between agencies sounds simple at first glance. With the advent of cloud-based solutions and remotely hosted storage options, sharing RMS is a theoretical possibility at every law enforcement level. Unfortunately, as observed in the FBI case study from Chapter IV, each added network node multiplies the system's complexities, as does each user request for jurisdictional or situation-specific capabilities.

Some law enforcement organizations share the same RMS among multiple agencies, and one such system exists in Texas. Sam Houston State University (SHSU) operates an information system for law enforcement organizations called Criminal Research Information Management Evaluation System (CRIMES), which has over 50 subscriber agencies. CRIMES includes CAD, RMS, and several other standard record-keeping modules used by law enforcement agencies. CRIMES is unique in that a university operates and maintains the system as a non-profit project that supports law enforcement research and operations.[68] This chapter will look at information systems as described by CRIMES users. The evaluation of CRIMES includes agency perspectives on the benefits and the problems they have encountered.

A. HOW CRIMES STARTED

SHSU has historically been a research institution for law enforcement scholars. CRIMES began as a project designed by SHSU to speed up and make more straightforward access to raw crime data from Texas agencies.[69] SHSU collaborated with several law enforcement organizations in Texas to mine crime data for scholarly research in criminal

---

[68] Vincent Webb, *The Criminal Research Information Management Evaluation System (CRIMES): A Comprehensive Records Management System for Smaller Police* (Tempe, AZ: Arizona State University, Center for Violence Prevention and Community Safety, 2017), http://cvpcs.asu.edu/sites/default/files/content/pages/Criminal_Research_Information_Management_Evaluation_System%20.pdf, 3.

[69] Suman Malempati is the project manager for CRIMES, and provided the historical context of the SHSU CRIMES project and subsequent system iterations.

justice and eventually built an automated repository for RMS data to use for the research. They agreed to return datasets to departments when requested. Eventually, some of the police chiefs asked the university if it would be possible for SHSU to host the data and allow the police agency to log back in to do criminal investigation research. SHSU built the system as requested. This hosted solution soon evolved into the CRIMES model as SHSU built an RMS and a CAD software solution.

As the project grew and evolved, the university saw the need to expand research and created new CRIMES components. The expansions eventually added mobile components, incident (case) management, booking and jail management, traffic citations, traffic crash reporting, and property room management to the core modules.[70] The CRIMES project was provided as a subscription service to offset the growing cost of setting up and maintaining the system. Subscriber agencies had to provide the necessary local hardware, but initially, CRIMES maintained a hosted software platform at the university. The subscription price is based on the number of officers at the agency.

When TDEx arrived on the scene as a data exchange in Texas, SHSU eventually abandoned the hosted solution and moved the software out to the agencies. The CRIMES managers understood the value of TDEx's information-sharing capabilities, and CRIMES was configured to connect to TDEx easily. Since changes began occurring at TDEx, some agencies have requested that CRIMES revert to a hosted solution so they can again have access to records from other departments. SHSU is currently exploring this option, and several of the agencies interviewed for this research were anxiously hoping for this change.

B. METHODOLOGY OF THE INTERVIEWS

Dr. Larry Hoover from SHSU was a longtime administrator over the CRIMES project and provided a list of 53 subscriber agencies that the author used to develop a list of potential interview subjects.[71] The agency list included sheriff's offices, university

[70] Police Research Center, "Criminal Research, Information Management and Evaluation System (CRIMES)."

[71] Dr. Larry Hoover, Director of the SHSU Police Research Center, provided the user agency list and some additional background information on the development of CRIMES.

police departments, and community supervision and corrections departments. The author chose municipal police agencies for the interview requests to keep the research scope in line with the survey model. The author sent requests to 36 municipal police departments, and 13 of them agreed to the interviews. In some cases, the agency chief was the interviewee, while in others, a records manager or other resident RMS expert provided the information. Four of the participating agencies had recently moved away from CRIMES to another RMS vendor but agreed to talk about their experience with CRIMES. The author sent interviewees an advance list of the interview questions.

The interview questions revealed how the agency uses CRIMES and how they connect to other investigative or intelligence information sources. The interview also produced a qualitative evaluation of CRIMES as an information management system. The interviews showed that none of the CRIMES users were sharing their RMS with another agency. This lack of sharing is a result of the changes that CRIMES made after the proliferation of TDEx. Some of the agencies had heard that CRIMES was considering a hosted, centralized solution. Every respondent agreed that a hosted solution that could share information among the other CRIMES agencies would significantly improve the system's value.

C. INTERVIEW AND SURVEY RESULTS

The municipal police departments that use CRIMES are mostly smaller to medium-sized agencies. The mean number of police officers in the responding agencies was 60, while the median was 65. The largest responding agency had 120 officers, and the smallest had 14. The agencies served an average population size of 26,585 persons. The author looked at the number of police officers for all 53 agencies listed as current or recent CRIMES subscribers. The largest agency on the list had 297 officers.

The interview questions followed similar lines as the survey, and one question asked what other databases the agency was using to conduct investigations or gather intelligence outside the RMS. These organizations reported using several of the sources identified by respondents in the Chapter 5 surveys. Additionally, two agencies used the Texas Gang Intelligence Index (TXGANG) as an intelligence resource. TXGANG is "a database index of persons associated with street gangs as reported by criminal justice

agencies within Texas."[72] One department reported using LiNX for investigations. All of the agencies reported using at least one external resource. Figure 4 shows the number of interviewed agencies using an identified investigative resource.

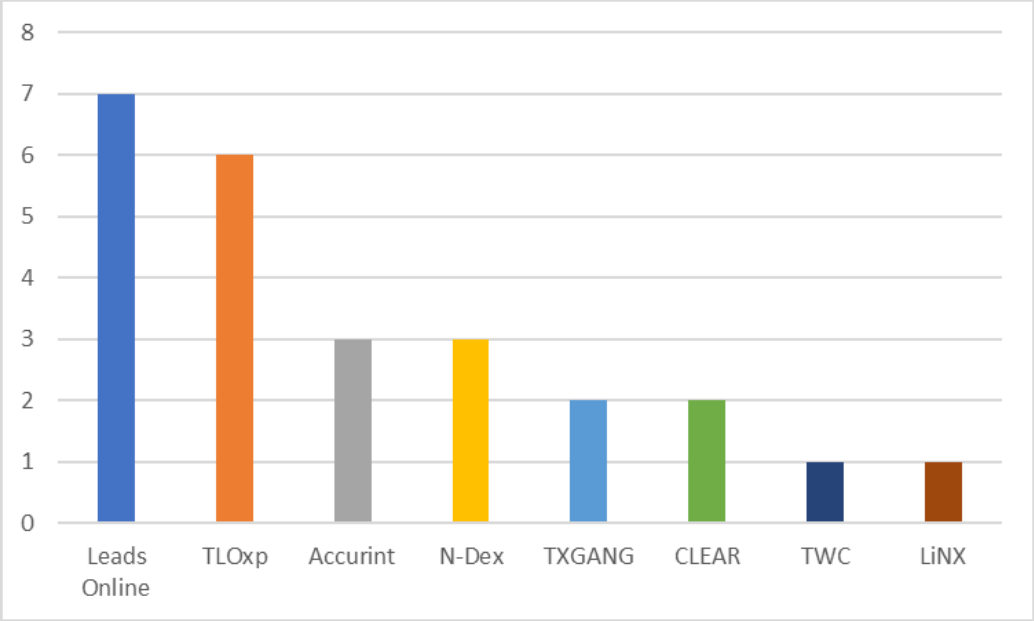

Figure 4. Interviewed agencies using other data sources

The next two questions discussed what fusion center the department accessed and what information users gained from fusion centers. Two of the agencies reported not using fusion center products. The others used one of four centers: Texas Fusion Center (TxFC), Ft. Worth Intelligence Exchange (FWINTEX), The North Texas Fusion Center (NTFC), or the Dallas Fusion Center (DFC). Figure 5 shows the number of interviewed agencies using each fusion center.

[72] "Texas Gang Intelligence Index," Texas Department of Public Safety, accessed February 25, 2021, https://www.dps.texas.gov/section/criminal-investigations/texas-gang-intelligence-index.

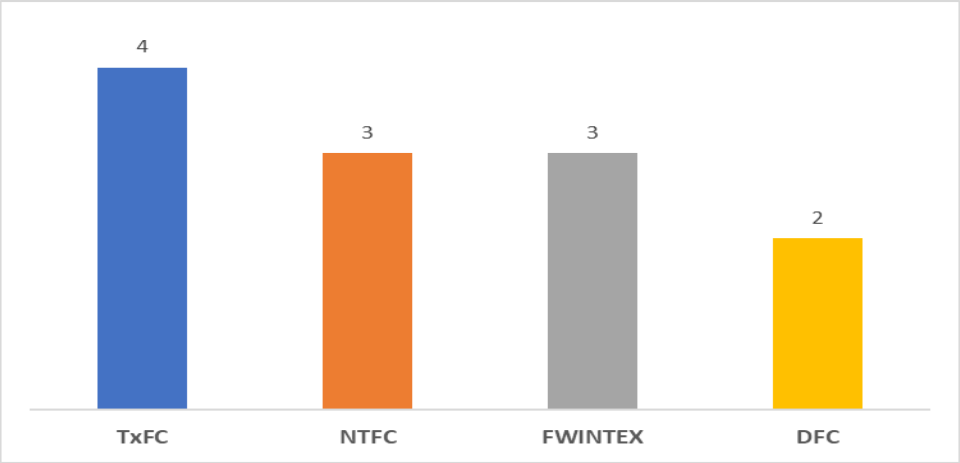

Figure 5. Fusion centers used by interviewed agencies

The answers varied as to what products or information agencies obtained from fusion centers. Two respondents stated they were unsure what information they routinely received from fusion centers. The other agencies reported that fusion centers provide useful information and intelligence to law enforcement. Those agencies reported receiving products and information such as:

- Deconfliction
- Wanted person and stolen property bulletins
- Intelligence on anticipated protests
- Narcotics trafficking
- Gang intelligence
- Help in the identification of suspected criminals
- Police reports from other agencies
- Facial recognition
- Crime trends in specific geographic areas
- Training bulletins

The next topic for the interview identified whether the agency was accessing N-DEx for information. Seven of the police agencies used N-DEx for criminal investigations, and six did not. Some agencies reported using N-DEx to access police reports from other agencies while investigating criminal cases. Others used historical address, phone, and vehicle information for tracking fugitives. Six of the agencies reported accessing N-DEx through the TDEx portal, and one used the LInX portal. Five of the agencies regularly accessed RISS for criminal or intelligence information.

The last part of the interview covered questions specific to the CRIMES RMS. These questions evaluated CRIMES using qualitative responses. These were the same questions asked in the survey responses for agencies that reported using CRIMES. There were nine agencies in the survey using CRIMES and nine in the interviews. The interviews provided more in-depth responses, as encouraged by the author. However, this analysis combines responses from both the survey and the interviews.

The first question in this section asked, "What functions does your agency believe CRIMES performs best?" The responses to this question were open-ended, but several similarities stood out. The first is that seven different agencies included the CAD and mobile software in this category. Some agencies described it as "very easy to use" and "simple." The overall simplicity of CRIMES functionality both in CAD and RMS was a common theme in the interviews. However, some respondents viewed simplicity as a negative trait because of the lack of in-depth analytic capabilities.

Another common theme was the ease of customization, and six agencies listed this as one of the positive traits of CRIMES. Five agencies reported excellent customer service as a performance measure. Interviews revealed that the CRIMES staff was very responsive to requests for custom reports or features. In contrast, one agency that had recently moved away from CRIMES reported poor customer service as one factor that caused them to consider a different RMS. Another noted minor syntax errors in the user interface that detracted from the professionalism of the product. Overall, the police departments considered customization and customer service to be beneficial to their organizations.

The next question asked whether the agency considered CRIMES an effective RMS platform and asked for an explanation of the response. The positive responses centered on

the simplicity and cost of the system. Seven different agencies reported the low cost as a being factor in the overall effectiveness of CRIMES. Most agreed that the lower cost than commercial software products was a good value, even when considering the reduced functionality of CRIMES vs. commercial products. The effectiveness was consistently tied to the ease of use and simplicity of the system.

Not everyone considered CRIMES to be effective. Five agencies described problems with getting consistent results when retrieving information in the form of statistical reports. Specifically, they reported not getting the same results when running the same report at different times. One agency subscriber identified the lack of detailed statistical reporting as a performance measure that reduces the effectiveness of CRIMES. Another agency indicated that CRIMES is unable to create relationships between people, cars, and addresses. This feature is essential for investigators when trying to connect criminal incidents with suspects or when searching for fugitives. Creating relationships to master name records is one of the standard functional specifications outlined by LEITSC.[73]

Four of the police departments had recently moved away from CRIMES as their RMS. Two of them were using Central Square two were using Spillman Flex. The primary reason for moving away from CRIMES was the lack of robust analytics and some concerns about the statistical inconsistency. One of these departments identified concerns that CRIMES was slow in responding to the federal mandate switch to the National Incident-Based Reporting System. The same department was also interested in sharing and seeing data from other agencies, which CRIMES was unable to do at the time. Another agency reported that the mobile component was too slow, and the police officers were frustrated with the system. The simplicity and minimalism that attracts some agencies to CRIMES also appear to be factored in some agencies' departure.

D. ANALYSIS

CRIMES started as a tool to provide academic researchers in criminal justice direct access to crime data. It has evolved into an information management system that competes

[73] Law Enforcement Information Technology Standards Council, *Standard Functional Specifications.*

directly with the vendors in the private sector. This model seems to work well for agencies on a constrained budget or agencies that cannot develop and maintain an elaborate RMS proposal. One agency noted the low cost of entry because there is no software start-up or installation costs. Instead, the agency provides the specified hardware, and SHSU provides the installation as part of the subscription cost. This low entry barrier model appeals to smaller-agency executives who must acquire and sustain one of the essential technology pieces of every law enforcement organization.

Unfortunately, the CRIMES model may not be well suited for use by large agencies. Project manager Suman Malempati identified two challenges for growing the system to meet the demands of larger police organizations. One challenge is the fact that the university facilitates the system as a non-profit research venture. Building and maintaining RMS for law enforcement is not a core responsibility of the university. Although the project serves a valuable research purpose, it is unlikely to see significant financial investment from the university for future research and development. This constraint keeps the system operating at a nominal level with unlikely hope of dramatic technological advancement. Another challenge is that some agencies require or request additional features that CRIMES cannot provide due to the research and development capacity limitations. Larger agencies tend to have more complex and demanding needs, reducing the likelihood that CRIMES will be seen as a viable RMS solution.

The conversion of CRIMES to a hosted solution will improve the system, provided that a federated search capability allows agencies to search across jurisdictional boundaries. Unfortunately, the limited number of agencies that use CRIMES will hamper the effectiveness of a federated search. A connection to TDEx and N-DEx will be a desirable feature to increase information sharing that CRIMES can provide. Agency executives expect an RMS to provide consistent statistical analysis, so any discrepancies in this area will need to be addressed.

Despite some of the limitations and problems, CRIMES provides a good RMS platform for small and medium-sized agencies that do not have a long list of unique requirements. Although future growth may be limited, departments should consider that

the cost of CRIMES will likely have to increase to support a sustainable future. In the meantime, CRIMES users can expect a simple, straightforward RMS solution.

E. LIMITATIONS

One significant limitation of this case study is the small number of agencies that participated in the interviews. The addition of CRIMES agencies from the survey doubled the number of respondents on this topic. Although the survey questions on CRIMES were the same as the interview questions, the agency interviews significantly increased the depth of information gleaned about the system.

Another limitation to the study may be the persons who were interviewed. The author contacted the police chief of each organization to request access to the agency personnel who were most knowledgeable about their RMS. In some cases, the chief completed the interview, but the chief assigned another department employee in other cases. It is possible that the person being interviewed was not the RMS expert or had a bias for or against CRIMES. Additionally, other persons in the agency may have voiced different views about CRIMES and the other information sources used by that agency. Several interviewees reported that they had checked with other people in their agency to answer some of the questions.

There are many vendors for RMS and likely many possible solutions to improving information sharing among law enforcement agencies. The CRIMES model is one option for Texas agencies, although such a system's continued development will need significant financial backing. The efficiency and effectiveness of crime control and terrorism prevention depend upon reliable and robust networks of information that multiple agencies can share, up to and including the federal government. The next chapter will combine the conclusions from this research to develop recommendations for law enforcement organizations to improve their ability to share criminal and intelligence information.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. DISCUSSION AND RECOMMENDATIONS

Records management and information systems are an essential part of the law enforcement organization. Most law enforcement officers agree that sharing this information between agencies is an essential component of information systems. The rapid progression of information technology makes it possible to communicate large amounts of information across the country in seconds. Information storage capabilities continue to grow, as do the opportunities for artificial intelligence to process data in ways only imagined 30 years ago. Why, then, is it so difficult to share this information on a widespread basis across law enforcement organizations in the United States or even with other countries?

A. BARRIERS TO SHARING

In a world where search engines and algorithms dominate most aspects of learning and entertainment, it seems logical that law enforcement would have easy solutions available to access vast amounts of criminal and intelligence information. Unfortunately, as this thesis reveals, what exists is not nearly as robust as what is actually possible. Many police agencies continue to be silos of information, segregated from sharing information with bordering jurisdictions. These organizations remain stagnated in bureaucratic policies or under-budgeted technologies that inhibit investigators and analysts from gathering information from what should be reasonably simple searches of singular or connected systems.

The potential problems of politics are one barrier to the implementation of shared systems. Even though many agency executives are appointed and somewhat insulated from political influences, city councils and county commissions approve law enforcement agencies' funding. Funding priorities for adjoining agencies may not line up during the same budget cycles. Furthermore, these governing bodies often turn over after two or four years, leading to priorities changes. Implementing an RMS acquisition or change may require several years from concept to completion and is likely to span more than one iteration of an elected government. Albeit an extreme example, as discussed in Chapter IV, the FBI took more than a decade to create a viable RMS solution.

Another problem examined in this thesis is the issue of data ownership. Two of the agency respondents in the research interviews reported that agency ownership issues prevented them from consolidating RMS with a neighboring agency. RMS users in both agencies saw the value of accessing information directly from the other. Unfortunately, the organizational leadership was unable to work through and find a solution. Historically, law enforcement agencies have struggled with sharing information between agencies out of fear of losing control of data or not knowing what will happen to their data.[74] This problem can be exacerbated by political foes or agency executives who don't get along. What is required is an educated understanding of the value of sharing and consolidating resources. Much like the standardization of radio communications systems, political leaders and law enforcement executives must learn to see interoperability of information systems as mutually beneficial.

B. GOVERNANCE

There is a lack of governmental regulation that mandates guidelines for building single or multi-agency information systems that can easily share information. Such policies exist in other homeland security realms, such as standard emergency 911 call specifications outlined by the FCC for decades, which are the same for all phone carriers.[75] Despite standard specifications for RMS and guidelines for information exchange standards, no regulation seems to be in place to require vendors or law enforcement agencies to share information. The National Information Exchange Model (NIEM) provides useful guidance to help agencies share essential information in emergencies and daily operations.[76] Making these standards mandatory among law enforcement RMS in the United States would be a step toward better sharing information.

---

[74] Hollywood and Winkelman, *Improving Information-Sharing Across Law Enforcement*.

[75] "911 and E911 Services," Federal Communications Commission, January 29, 2021, https://www.fcc.gov/general/9-1-1-and-e9-1-1-services.

[76] "National Information Exchange Model (NIEM)," Justice Information Sharing, accessed February 13, 2021, https://it.ojp.gov/initiatives/niem.

Related to standardization is the problem of vendors who create proprietary databases and algorithms that limiting the agency's ability to share data without the additional expense of a custom-built interface.[77] Although some agencies can afford this expense, many cannot, and thus the propriety of an RMS becomes a barrier to sharing information. The vendor's propriety level should be a significant consideration for agency executives in the procurement process of upgrading or replacing an information system.

C. MARKETING AND TRAINING

Although the sample of agencies in this thesis is small, it is clear that police organizations would benefit from more information or training on information access. One area is fusion centers. Fusion centers provide a significant amount of support and helpful products to aid law enforcement. However, one must know what questions to ask and be aware of the existence of these resources. Of the police departments surveyed for this thesis, 40 percent did not list fusion centers as a resource for information or intelligence. For this reason, it is reasonable to conclude that it would be beneficial for fusion centers to consider how they are (or are not) marketing their presence and capabilities.

The same could be said for improving the visibility of RISS and N-Dex, as both of these systems provide valuable data and resources. RISS provides gang intelligence, deconfliction services, investigation support, and equipment loans in certain circumstances; however, less than 20 percent of the respondents seemed to understand RISS or how to access it. N-DEx gives agencies a way to connect with each other, even while using different RMS platforms. The information on N-DEx seems to be more widespread, and NDE-x has the endorsement of the International Association of Chiefs of Police along with many other large law enforcement organizations.[78] These endorsements likely increase the visibility of N-DEx, but additional marketing would help more agencies understand the potential benefits to membership.

---

[77] Dasher and Haynes, "Overcoming Law Enforcement Data Obstacles."

[78] Federal Bureau of Investigation, "National Data Exchange (N-DEx) System."

One crucial aspect of improving the presence of any of these sharing tools is training. Agency administrators should educate themselves on what tools are available to improve information sharing. Likewise, they are responsible for training their staff on the importance of good research, the availability of these tools, and how to access them. The agency head may also need to provide proper credentialing for the agency and the employee to access one or more systems. Additionally, the agency must commit one or more employees to maintain the credentialing process. During this research, one agency interviewed revealed that the process for maintaining credentials with N-DEx was too complicated, and the agency lost interest in keeping that connection. A commitment to training and allocating personnel to maintain linkage to N-DEx, RISS, and fusion centers is essential to improving information sharing.

Administrators must also consider budget requests to provide the ability to share information mutually and be prepared to explain to political bodies why this funding is necessary. This funding may include payment to vendors to build interfaces to overcome proprietary issues and purchase equipment or software to connect to other systems. The chief executive must educate the political jurisdiction on the benefits and the risks of contributing information to the greater homeland security enterprise, both locally and nationally.

D. PROMISING MODELS

Although Texas agencies were the primary research area for this thesis, the author also spoke with the Ogden Police Department in Utah, as discussed in Chapter III. The Ogden Police Department provided valuable insight on the advantage of collaboration with nearby agencies. The department considers the ability to directly share information with these agencies a tangible benefit because many of the criminals they deal with in Ogden easily cross into other nearby jurisdictions. This example provides evidence that the concept of connected information systems is valuable to law enforcement officers in bordering geographic areas. Additional research is needed to determine if there is a measurable result in metrics such as crime clearance rates in areas that collaborate on the same RMS.

Another promising sharing model is the data warehouse examples in Colorado. The Colorado Information Sharing Consortium (CISC) serves nearly 80 law enforcement agencies contributing and retrieving data from the warehouse.[79] The CISC model combines the elements of information sharing with access to an analyst team. With portals to N-DEx and LInX, the CISC provides subscriber agencies a valuable information resource, not unlike a fusion center. State governments or regional collaborations of government agencies should consider the feasibility of sponsoring such a model. Regional consortiums could work in conjunction with fusion centers to provide vast arrays of collaborative networks.

N-DEx provides a data exchange model that is robust enough to support a nationwide network. Next to fusion centers, N-DEx was the most widely recognized resource for data in this study. N-DEx provides immediate access to a wide variety of records, including incident reports, probation and parole reports, booking reports, traffic citations, mug shots, and even images of arrestees' scars, marks, or tattoos.[80] It is hard to understate the value of such a vast resource of potential information. One key to improving N-DEx is for agencies to understand the value of contributing their data and not just being passive subscribers.

E. ANSWERING THE QUESTION

This thesis asked the question: How can law enforcement agencies directly share information more effectively and efficiently to identify criminal suspects, organized crime, or potential terrorist activities? The answer has several possible solutions and could depend on agency size, location, and mission. Law enforcement agencies in the United States tasked with providing general protective and investigative services to a defined geographic jurisdiction can use these recommendations as a starting point for improvement.

---

[79] Colorado Information Sharing Consortium, "Member Agencies."

[80] Wertheim and Badgett, "The FBI's National Data Exchange (N-DEx)."

1. Regional Agency Combined RMS

Although using a singular RMS solution requires considerable political cooperation and agency coordination, a combined system can reduce wasted duplication of resources in bordering or overlapping jurisdiction areas. A multi-agency CAD and RMS is a viable option, especially when agencies plan well in advance and agree in writing to issues of ownership, cost bearing, and maintenance. Smaller agencies may find more significant benefit in signing on as subscribers to a larger agency's system. The complexities and risks of procurement can be delegated to the host agency, while the smaller agency benefits from a robust product and information access to the other organization's data.

An alternative to a single combined RMS is for agencies near each other to consider using the same RMS vendor. Some vendors provide information sharing between different agencies using their product, as seen in the Ogden example. If agencies are wary of not retaining ownership of the RMS, the alternative of using the same vendor as their nearby partners can provide an agency-specific solution that still allows investigators to research relevant data in their region quickly.

2. Governmental Sponsorship and Funding

Both the Chicago and Colorado models provide excellent examples of data warehouses that connect dozens of law enforcement organizations. Regional councils of government or state-level law enforcement organizations are excellent candidates to sponsor information-sharing initiatives. Participation may require agencies to contribute funds as a subscriber. Alternatively, governmental bodies could allocate funding to support data warehouse initiatives.

CRIMES is a useful model as a research-based, government-subsidized system. The operation cost is lower per agency, and the research benefits are helpful to the overall criminal justice system. A system like this deserves better funding, specifically if it provides a valuable resource for smaller agencies, as CRIMES seems to do. If the university-funded model is not ideal, then local or state governments should consider sponsorships.

Funding is a critical component of improvement in information sharing. Smaller agencies may need help with funding the appropriate hardware or software additions needed to share data with exchanges directly. Some agencies may need help in paying for a proper, basic RMS. Grant opportunities should exist to spur innovation of information sharing between law enforcement, especially at the regional or state level.

3. Raising Awareness of Information Resources

This research supports improvements in the marketing and training on the value of fusion centers, RISS, and N-DEX. There are also tools on the open market that law enforcement agencies should use to improve their investigative capabilities, although there is a cost involved for these products. The responsibility for training lies primarily with law enforcement leaders. Agency executives should purposefully research the full breadth of information gathering tools, then educate their staff on the options. Leaders must also educate their constituents and their politicians, working to garner support for information resources that will make the community safer.

Government-sponsored resources should ensure that all potential users and their agencies are shown their products' value. The mere existence and passive subscribership of these tools are not good enough. Instead, the taxpayer funds dedicated to supporting programs like RISS or fusion centers demand widespread and consistent usage by small and large organizations. Fusion centers provide valuable products, and increasing the marketing of these products is likely to increase their usage and, in turn, their effectiveness.

4. Mandatory Participation in Data Exchanges

Data exchanges such as LInX or N-DEx can connect agencies nationwide; however, they are only as useful as the information they receive. Participation in contributing information to data exchanges should be encouraged, incentivized, or even mandated. Best practices or accreditation programs should require it. The federal or state government could have a role in this by allocating funding to help agencies purchase the needed technology to contribute data. The requirement to participate in data exchanges could later be tied to eligibility for other funding types, for example, grant funding for law enforcement terrorism prevention activities.

Full participation in a data exchange may be one of the best solutions to the information-sharing problem. This option allows agencies to retain ownership of their data while still contributing critical information to the greater homeland security enterprise. In turn, investigators and analysts can access a vast resource of information across municipal and state boundaries. The data exchange model reduces many of the political and technical barriers to sharing RMS. Implementing this solution is not without cost and will require a great deal of marketing, education, and motivation to be fully effective.

F. THE RIGHT COMBINATION

No single solution will fix the lack of information sharing in the homeland security enterprise. Law enforcement agencies collect a great deal of data that holds the potential to improve our country's safety and security. The key is sharing, in particular outwardly. Although local law enforcement in the United States is traditionally and sometimes stubbornly independent, agencies cannot remain silos of information. Instead, those in the profession must come to understand the value of a controlled yet robust sharing program. Front line workers need access to the information contained in both neighboring and distant law enforcement information systems to more effectively protect our nation from criminal or terrorist threats.

Whether sharing a multi-agency RMS, participating in data exchanges, or an amalgamation thereof, law enforcement executives must find the right combination of solutions. These solutions should protect the data and the organization's integrity while still providing external agencies the resources needed to connect criminal and intelligence information. A successful result will be a robust network that puts the United States on the leading edge of law enforcement information sharing.

LIST OF REFERENCES

Buckley, John. *Managing Intelligence : A Guide for Law Enforcement Professionals*. Boca Raton, FL: CRC Press, 2017. https://doi.org/10.1201/b15515.

California Commission on Peace Officer Standards and Training. *Law Enforcement Records Management Guide*. 5th ed. Sacramento, CA: California Commission on Peace Officer Standards and Training, 2014. https://post.ca.gov/Portals/0/Publications/Records_Management.pdf?ver=2019-07-12-131135-140.

City of Chicago. "Chicago Data Portal." Chicago Data Portal. Accessed February 25, 2021. https://data.cityofchicago.org/browse?category=Public%20Safety.

Colorado Information Sharing Consortium. "Member Agencies" . Accessed December 13, 2020. https://cisc.colorado.gov/member-agencies.

Dasher, Andrew, and Robert Haynes. "Overcoming Law Enforcement Data Obstacles." *Police Chief Magazine*, September 28, 2016. https://www.policechiefmagazine.org/overcoming-law-enforcement-data-obstacles/.

Department of Homeland Security. "Fusion Center Locations and Contact Information." April 1, 2011. https://www.dhs.gov/fusion-center-locations-and-contact-information.

———. "Fusion Centers." Department of Homeland Security, July 6, 2009. https://www.dhs.gov/fusion-centers.

Federal Bureau of Investigation. *Law Enforcement Records Management Systems (RMSs) as They Pertain to FBI Programs and Systems*. Washington, DC: Department of Justice, 2010. https://ucr.fbi.gov/law-enforcement-records-management-system.

———. "National Crime Information Center (NCIC)." Accessed October 25, 2020. https://www.fbi.gov/services/cjis/ncic.

———. "National Data Exchange (N-DEx) Data Integration FAQs." November 16, 2016. https://www.fbi.gov/file-repository/ndex_data_integration_faqs.pdf/view.

———. "National Data Exchange (N-DEx) System." Accessed December 5, 2019. https://www.fbi.gov/services/cjis/ndex.

Federal Communications Commission. "911 and E911 Services." January 29, 2021. https://www.fcc.gov/general/9-1-1-and-e9-1-1-services.

Foley, John. “FBI’s Sentinel Project: 5 Lessons Learned.” *InformationWeek*, August 2, 2012. https://www.informationweek.com/applications/fbis-sentinel-project-5-lessons-learned/d/d-id/1105637?

German, Michael, and Jay Stanley. *What’s Wrong with Fusion Centers?* New York: American Civil Liberties Union, 2007. https://www.aclu.org/files/pdfs/privacy/fusioncenter_20071212.pdf.

Global Justice Information Sharing Initiative, United States Department of Justice. *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*. Washington, DC: U.S. Department of Justice, 2006. https://it.ojp.gov/documents/fusion_center_executive_summary.pdf.

Goldstein, Harry. “Who Killed the Virtual Case File? [Case Management Software].” *IEEE Spectrum* 42, no. 9 (September 2005): 24–35. https://doi.org/10.1109/MSPEC.2005.1502526.

Green, Chris. “Illinois Law Enforcement Agencies Seek Shared Records Management System.” *Government Technology*, March 21, 2017. https://www.govtech.com/public-safety/Illinois-Law-Enforcement-Agencies-Seek-Shared-Records-Management-System.html.

Harvard Kennedy School. “Citizen and Law Enforcement Analysis and Reporting (CLEAR).” Government Innovators Network. Accessed December 13, 2020. https://www.innovations.harvard.edu/citizen-and-law-enforcement-analysis-and-reporting-clear.

Hollywood, John, and Zev Winkelman. *Improving Information-Sharing across Law Enforcement: Why Can’t We Know?* Santa Monica, CA: RAND Corporation, 2015. https://www.ncjrs.gov/pdffiles1/nij/grants/249187.pdf.

Irigoyen, Claudia. “The FBI Virtual Case File System.” Centre for Public Impact, June 20, 2017. https://www.centreforpublicimpact.org/case-study/fbi-virtual-case-file-system/.

Law Enforcement Information Technology Standards Council. *Standard Functional Specifications for Law Enforcement Records Management Systems (RMS).* Washington, DC: Department of Justice, 2006. https://it.ojp.gov/documents/LEITSC_Law_Enforcement_RMS_Systems.pdf.

Marchewka, Jack T. “The FBI Virtual Case File: A Case Study.” *Communications of the IIMA* 10, no. 2 (2010): 1–14.

McCaul, Michael, and Peter King. *Majority Staff Report on the National Network of Fusion Centers.* Washington, DC: U.S. House of Representatives, 2013. https://www.archives.gov/files/isoo/oversight-groups/sltps-pac/staff-report-on-fusion-networks-2013.pdf.

McGhee, G. C. Sam. "The Wicked Problem of Information Sharing in Homeland Security—A Leadership Perspective." Master's thesis, Naval Postgraduate School, 2014. http://hdl.handle.net/10945/42684.

Naval Criminal Investigative Service. "LINx/D-Dex." Accessed January 10, 2021. https://www.ncis.navy.mil/Mission/Partnership-Initiatives/LInX-D-Dex/.

Office of the Director of National Intelligence. "Law Enforcement Information Sharing." Accessed June 30, 2020. https://www.dni.gov/index.php/who-we-are/organizations/ise/ise-archive/ise-additional-resources/2142-law-enforcement-information-sharing.

Police Research Center. "Criminal Research, Information Management and Evaluation System (CRIMES)." Accessed December 8, 2019. http://www.cjcenter.org/prc/crimes/.

Reaves, Brian A. *Census of State and Local Law Enforcement Agencies, 2008*. NCJ 233982. Washington, DC: Bureau of Justice Statistics, 2011. https://www.bjs.gov/content/pub/pdf/csllea08.pdf.

Regional Information Sharing Systems. "About the RISS Program: A Proven Resource for Law Enforcement." . Accessed November 8, 2020. https://www.riss.net/about-us/.

Roberts, Aki, and John M. Roberts, Jr. "The Structure of Informal Communication Between Police Agencies." *Policing: An International Journal of Police Strategies & Management* 30, no. 1 (2007): 93–107. https://doi.org/10.1108/13639510710725640.

Senate Permanent Subcommittee on Investigations. *Federal Support for and Involvement in State and Local Fusion Centers: Majority and Minority Staff Report*. Washington, DC: U.S. Senate Permanent Subcommittee on Investigations, 2012. https://www.hsgac.senate.gov/imo/media/doc/10-3-2012%20PSI%20STAFF%20REPORT%20re%20FUSION%20CENTERS.2.pdf.

Skogan, Wesley, and Susan Hartnett. "The Diffusion of Information Technology in Policing." *Police Practice & Research* 6, no. 5 (December 2005): 401–17. https://doi.org/10.1080/15614260500432949.

Texas Department of Public Safety. "Texas Crime Information Center (TCIC)." Accessed November 8, 2020. https://www.dps.texas.gov/administration/crime_records/pages/tcic.htm.

———. "Texas Gang Intelligence Index." . Accessed February 25, 2021. https://www.dps.texas.gov/section/criminal-investigations/texas-gang-intelligence-index.

Texas Workforce Commission. “About Texas Workforce.” August 16, 2018. https://www.twc.texas.gov/about-texas-workforce.

TransUnion Risk and Alternative Data Solutions. “Law Enforcement.” Accessed January 14, 2021. https://www.tlo.com/law-enforcement.

U.S. Department of Justice. “National Information Exchange Model (NIEM).” Justice Information Sharing. Accessed February 13, 2021. https://it.ojp.gov/initiatives/niem.

U.S. Department of Justice, Office of the Inspector General. *Audit of the Status of the Federal Bureau of Investigation’s Sentinel Program*. Audit Report 14–31. Washington, DC: U.S. Department of Justice, 2014. https://oig.justice.gov/reports/2014/a1431.pdf.

———. *Status of the Federal Bureau of Investigation’s Implementation of the Sentinel Project*. Report 10–22. Washington, DC: U.S. Department of Justice, 2010. https://oig.justice.gov/reports/FBI/a1022.pdf.

———. *The Federal Bureau of Investigation’s Management of the Trilogy Information Technology Modernization Project*. Audit Report No. 05–07. Washington, DC: U.S. Department of Justice, 2005. https://oig.justice.gov/reports/FBI/a0507/intro.htm.

Webb, Vincent. *The Criminal Research Information Management Evaluation System (CRIMES): A Comprehensive Records Management System for Smaller Police*. Tempe, AZ: Arizona State University, Center for Violence Prevention and Community Safety, 2017. http://cvpcs.asu.edu/sites/default/files/content/pages/Criminal_Research_Information_Management_Evaluation_System%20.pdf.

Wertheim, Kasey E., and Kelly Badgett. “The FBI’s National Data Exchange (N-DEx).” *FBI Law Enforcement Bulletin*, December 9, 2015. https://leb.fbi.gov/articles/featured-articles/the-fbis-national-data-exchange-n-dex.

Womack, Trevor. “Economies of Scale: 9-1-1 Center Consolidation as a Means to Strengthen the Homeland Security Enterprise.” Master’s thesis, Naval Postgraduate School, 2014. http://hdl.handle.net/10945/41458.

Wormet, Jody R. “Federated Search Tools in Fusion Centers : Bridging Databases in the Information Sharing Environment.” Master’s thesis, Naval Postgraduate School, 2012. http://hdl.handle.net/10945/17480.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California