2014-09

Information sharing from 9-1-1 centers

Simpson, Carl P.

Monterey, California: Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

INFORMATION SHARING FROM 9-1-1 CENTERS

by

Carl P. Simpson

September 2014

Thesis Advisor: Kathleen Kiernan
Second Reader: John Rollins

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2014	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE
INFORMATION SHARING FROM 9-1-1 CENTERS

5. FUNDING NUMBERS

6. AUTHOR(S) Carl P. Simpson

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. IRB Protocol number ____N/A____.

12a. DISTRIBUTION/ AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

Public safety first responders deal with life and death emergencies, natural disasters, school shootings, trauma created by lone shooters and major events, yet have not enabled members from the private sector, business owners, school administrators, and other public safety stakeholders to participate fully in the mitigation or prevention of these events. At no time in this nation's history is the public more attuned to the potential threats in the homeland, and simultaneously, willing, wanting, and able to be part of the solution.

This thesis outlines proactive case studies that demonstrate the ability to share public-safety sensitive and law enforcement information in a safe, secure, and timely method with those who can help first responders make a difference and keep this country's communities safer.

14. SUBJECT TERMS
homeland security, information sharing, public safety answering points, PSAP, technology, fusion center, suspicious activity report, suspicious activity reporting, first responders, 9-1-1, 911, emergency

15. NUMBER OF PAGES
73

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

INFORMATION SHARING FROM 9-1-1 CENTERS

Carl P. Simpson
Executive Director, Denver 9-1-1, Denver, Colorado
B.A., Regis University, Denver, Colorado, 1992

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
September 2014

Author: Carl P. Simpson

Approved by: Kathleen Kiernan, Ph.D.
Thesis Advisor

John Rollins, Ph.D.
Second Reader

Mohammed M. Hafez, Ph.D.
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Public safety first responders deal with life and death emergencies, natural disasters, school shootings, trauma created by lone shooters and major events, yet have not enabled members from the private sector, business owners, school administrators, and other public safety stakeholders to participate fully in the mitigation or prevention of these events. At no time in this nation's history is the public more attuned to the potential threats in the homeland, and simultaneously, willing, wanting, and able to be part of the solution.

This thesis outlines proactive case studies that demonstrate the ability to share public-safety sensitive and law enforcement information in a safe, secure, and timely method with those who can help first responders make a difference and keep this country's communities safer.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ALI	automatic location identification
ANSI	American National Standards Institute
APCO	Association of Public Safety Communications Officers
API	application programming interface
C2C	CAD to CAD
CAD	computer aided dispatch
CAP	Common Alerting Protocol
CIAC	Colorado Information Analysis Center
CISO	chief information sharing officer
CISPA	Cyber Intelligence Sharing and Protection Act
COTS	commercial-off–the-shelf
CSP	Colorado State Patrol
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DOJ	Department of Justice
DPD	Denver Police Department
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
GAO	Government Accountability Office
GIS	geographical information systems
GPS	global positioning system
HDSSC	Homeland Defense and Security Standardization Collaboration
IC	intelligence community
ISE	Information Sharing Executive
IT	information technology
JMS	jail management system
JTTF	Joint Terrorism Task Force
LOA	letter of agreement
MDC	mobile data computers
MOU	memorandum of understanding

NENA	National Emergency Number Association
NG	Next Generation
NIS	National Intelligence Strategy
NSIS	National Strategy for Information Sharing
NIST	National Institute of Standards and Technology
NPS	Naval Postgraduate School
NRF	National Response Framework
PCLOB	Privacy and Civil Liberties Oversight Board
PDF	portable document format
PSAP	public safety answering point
PSKN	public sector knowledge network
RMS	records management system
SAR	suspicious activity report
SECURE IT	Strengthening and Enhancing Cyber-security by Using Research Education
TCP/IP	Transmission Control Protocol/Internet Protocol
TIES	Trusted Information Exchange Services®
U.S.	United States

DEFINITION OF TERMS

Public Safety Answering Points

Public safety answering points (PSAPs), Communication Centers, or emergency dispatch centers, are configured in a wide variety of sizes and capabilities, dependent primarily on the sizes of the jurisdictions and communities in which they serve. Some communication centers are standalone PSAPs and one of the better-known examples of a standalone center is the Los Angeles Police Department dispatch center. Call-takers field law enforcement requests for service and send the information electronically to the dispatchers working across the center. The City of Phoenix has a well-regarded fire dispatch center; these configurations serve those communities and executive officers of those agencies best.

Smaller centers may not have the call volume that the previous two urban call centers handle but the employees work as hard, answering telephone calls for service while simultaneously entering information into the dispatching system, dispatching first responders via radio, and managing the customer walk-up counter at the police department.

Computer Aided Dispatching Systems

"Law enforcement agencies use computer aided dispatch systems (CAD) to facilitate incident response and communication in the field. CAD systems, in many cases, are the first point of entry for information coming into the law enforcement system. Typical CAD system functions include resource management, call taking, location verification, dispatching, unit status management, and call disposition.

"Additionally, mapping functionality, interface with mobile data computers (MDC), and interfaces with other external local, state, and federal information systems

may be included. Call-takers, dispatchers, and their supervisors are primary users of CAD."[1]

9-1-1 Telephone Systems

"The establishment of a single, three-digit telephone number for citizens who require immediate police assistance, emergency medical aid or fire suppression. With the advent of the E-911 telephone system that automatically routing the caller to the closest PSAP. The telephone system interfaces with CAD to make the determination as to which police, fire or EMS agency is closest to the emergency."[2]

[1] "Law Enforcement Information Technology Standards Council (LEITSC)," *The Police Chief*, 2014, http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=1199&issue_id=62007.

[2] "9-1-1 History," Louisiana National Emergency Number Association, accessed July 10, 2014, http://www.louisianananena.org/911history.asp.

EXECUTIVE SUMMARY

Call centers, also known as Public Safety Answering Points (PSAPs), are the public's first point of contact with public safety authorities during emergencies.[1] To the layman, the nation's 9-1-1 system is a single network that connects communities across the country. This concept is perpetuated by television crime dramas whose writers unintentionally provide misinformation to eager and captivated audiences on a daily basis.

In reality, 9-1-1 systems are stove-piped networks that serve specific regions, communities, and jurisdictions; no nationwide system exists. Counties or metropolitan areas with large communities may have several PSAPs whose employees work for a variety of municipal and county organizations. Fortunately, and in spite of the fragmented system, emergency telephone services are available to 98% of the American population[2] and the centers are connected to one another via an aging telephone network of central offices, copper wire, and analog switching stations.

Most PSAPs also serve as emergency dispatch centers, and America's dispatchers are often referred to as the lifeline between emergency responders and the public[3] for it is the call-takers and dispatchers who coordinate the emergency caller with the first responders who will ultimately assist the public. PSAP employees are the first of the first responders. This nation's PSAPs are rich with information collected from citizens requesting emergency assistance, processed by call-takers, summarized, prioritized, and utilized to dispatch first responders to emergency and non-emergency situations. The primary mission of PSAP employees is to help people on what they may perceive to be their worst day. In the author's opinion, gained from more than 20 years of personal

---

[1] "9-1-1 Call Centers/PSAPs," Federal Communication Commission, Public Safety and Homeland Security Bureau, accessed May 14 2014, http://transition.fcc.gov/pshs/psaps.html.

[2] "Homepage," National Emergency Number Association, 2014, http://www.nena.org/?.

[3] Michelel McConnaha, "Week Recognizes Hard Work of County's 911 Dispatchers," *Ravalili Republic*, April 15, 2014, http://ravallirepublic.com/news/local/article_1e3cab92-c508-11e3-b7d1-001a4bcf887a.html.

experience, PSAP employees do amazing work in less than ideal circumstances, which is often difficult, stressful and challenging, and invisible to the public.

Once events are mitigated and first responders have left the scene to return to headquarters to file their reports, all the updated information is archived in databases and is rarely reviewed again. The data, in aggregate, could be exploited to identify patterns, trends, and clusters of incidents, which could be leveraged to identify among other key issues, public safety and or traffic hazards, patterns of illegal use of narcotics, trends in firearm related violence, and patterns of fraudulent insurance claims. Each of these issues has collateral impacts on a community, the public, and those first responders who serve them.

These same bits of information, breadcrumbs that succinctly and chronologically describe events happening in and around United States (U.S.) communities, can be leveraged to improve the situational awareness of the community public safety stakeholders, including business owners and school administrators. The United States has more than 9,600 PSAPs[4]; each operates unique equipment and utilizes non-standardized policies and procedures. Police chiefs, fire chiefs, and sheriffs who control and manage dispatching operations manage them differently. The one operational issue consistent from one PSAP to another is that chiefs and sheriffs prefer not to share information with other agencies.[5]

This research explored several case studies that have improved public safety by sharing information with public safety stakeholders, school administrators, and business owners. As described in this thesis, some projects were more effective and cost effective than others; however, they share the common goal to share PSAP-based information. This thesis determined that through sharing information with trusted public safety stakeholders and networks, communities could collaborate more effectively with law enforcement agencies to reduce crime, and at the same time, improve working relationships.

---

[4] "Homepage."

[5] Darrell O'Donnell, "Enabling Information Sharing," Slideshare, 2013, http://www.slideshare.net/ForgeRock/how-do-get-police-fire-paramedics-and-others-to-share-information-built-trust-into-the-system.

ACKNOWLEDGMENTS

Few endeavors undertaken as leaders, spouses, and parents simply cannot be accomplished to their fullest without the help of the special people in our lives—this research and the Naval Postgraduate School coursework being two of them. I could not have successfully accomplished either without the unconditional support and encouragement from my beautiful wife, Jonye. She sacrificed her weekends, holidays, and vacations to ensure that I had the time and freedom to study and research, and was a constant source of encouragement.

Special thanks to my parents who were consistently interested in the progress of my studies and provided encouragement at every step along the way. They instilled a strong work ethic in me that helped me press through the competing challenges for my time and energy.

My team at Denver 911 picked up the slack for me on more than one occasion while I was away; they ensured the mission to help people on their worst day was fulfilled each and every day. Thank you Laura Wachter, Kim Carroll, Donna Trujillo, Shelly Lesnansky, Brian Blick, Ernie Franssen, David Garcia, and Garry Hinderliter for helping my seemingly impossible tasks possible.

Thanks to my cohort, whose battle cry was "cooperate to graduate!" Many times someone picked me up by the scruff of the neck and literally carried me across the finish line. I hope that in some small way I was able to pay that gift forward.

My instructors made the difference in my education; each of them gave me special attention, recognized when I did not understand and reached out to me, either electronically or by telephone, and provided encouragement.

With everyone standing at my 6, I never felt alone; I never experienced the desire to give up or surrender; the prospect of not finishing was never considered.

Studying at the Naval Postgraduate School was a privilege and a gift that I commit to my cohorts, instructors, administrators, family, and the public that I will not squander.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

Many after-action assessments of critical events and emergencies have concluded that communication breakdowns lead to significant performance failures, unnecessary loss of life, and loss of property. After action reports of the Columbine High School shooting,[1] Hurricane Katrina,[2] 9/11,[3] and Super Storm Sandy[4] are examples of such reports highly critical of inter-agency and inter-department communications, and each document offers recommendations for improvement, largely around communication breakdowns. The common theme in the after action reports is that responses to emergency situations have historically not been effective due to the lack of effective coordination and communication between agencies and departments. Problems include lack of interoperability due to radio devices, inconsistent radio protocols, incongruent policy, and a clear chain of command.[5]

In spite of government reports recommending agencies share information more effectively, over the past two decades, these functional communication and information sharing gaps have shown no measurable improvement. Such crises do not improve with the passing of time; therefore, critical emergency communications must be immediate, crisp, timely, and accurate.

Federal, state, and local information sharing and intelligence development remains mission focused for the home agency, not the overall mission. The 9/11

---

[1] Kieran Nicholson, "Columbine: Training Before Massacre 'Flawed,'" *Denver Post*, September 23, 2000, http://extras.denverpost.com/news/col0923.htm.

[2] Robert Miller, Ph.D., "Hurricane Katrina: Communications & Infrastructure Impacts," in the 2006 Conference *Threats at Our Threshold* (Washington, DC: National Defense University, 2006), 192.

[3] Andrea Stone and John Rudolf, "9/11 Commission Recommendations on First Responder Network, Civil Liberties Unmet 10 Years after Attacks," *Huffington Post*, September 9, 2011, http://www.huffingtonpost.com/2011/09/09/911-commission-recommendations-unmade_n_950896.html.

[4] Gary Nelson, "Hurricane Sandy Causes "Failure to Communicate," *CBS Miami*, October 30, 2013, http://miami.cbslocal.com/2012/10/30/hurricane-sandy-causes-failure-to-communicate/.

[5] Ibid.

Commission directive stating, "…the importance of an integrated, all inclusive effort to 'connect the dots' is a national objective" remains an admirable goal for more than ten years following the 9/11 attacks.[6]

Few would object that communications and collaboration between agencies and public safety stakeholders must improve and that the public and private sectors are key partners to keeping this nation secure. Thus, what prevents public safety officials from sharing information with other first responders and non-traditional public safety stakeholders?

Excellent examples of information sharing systems are available that function optimally with adequate security measures by credentialing and trusting authorized users without risking the safety of first responders, victims of emergencies, and simultaneously, maintaining the integrity of criminal investigations.

The Federal Bureau of Investigations (FBI) participated in several information-sharing initiatives in 2011. It continues to promote appropriate sharing and collaboration with the goal of protecting the United States and defeat national security threats while preserving the privacy and civil liberties of U.S. citizens. A report presented by the FBI chief information sharing officer (CISO) summarizes and characterizes the many information-sharing activities currently engaged in by the FBI.[7]

> The year 2012 was marked by significant change within the FBI regarding information sharing and safeguarding. In response to numerous challenges and potential threats, the FBI took steps to more effectively and efficiently share vast amounts of information with Law Enforcement and Intelligence Community partners, as well as to better protect sensitive information to preserve the integrity of operations while ensuring the privacy and civil liberties of U.S. persons.[8]

---

[6] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report* (New York: W.W. Norton & Co., 2004), 208.

[7] "Information Sharing and Safeguarding Report 2012," Federal Bureau of Investigation (FBI), 2012, http://www.fbi.gov/stats-services/publications/national-information-sharing-strategy-1/fbi-information-sharing-and-safeguarding-report-2012-2.

[8] Ibid.

B. RESEARCH QUESTIONS

This research is linked to the author's work as the director of a large urban public safety answering point (PSAP) interested in improving the information exchange between centers, federal, state, and local law enforcement agencies, state fusion centers, business owners, and school principals.

Can information sharing between PSAPs, and federal, state, local, and fusion centers improve? Should a conceptual framework be adopted and operated under that addresses policy, trust, social, technology, and funding barriers? Can information flow upward from the municipal level to the state and federal levels?

Information collection in the American PSAPs consists of more than merely information gathering about public safety events, such as burglaries, structure fires, and medical emergencies. Buried in the hundreds of hundreds of thousands of telephone calls received in PSAPs are potential indicators of significant criminal and potential terrorist events. Should this information be culled and analyzed if the collection and sharing of information across the spectrum of law enforcement, public safety agencies, public safety stakeholders, business owners, and school administrators could improve national security, create a safer community and improve the safety of the American people?

Senate and House legislation similarly create mechanisms for oversight of information-sharing procedures to protect privacy and civil liberties and place limitations on the use of the cyber threat information shared with the government. For example, the Cyber Intelligence Sharing and Protection Act (CISPA) requires annual reports from the intelligence community inspector general. The Lieberman-Collins Cybersecurity Act requires an evaluation by the Privacy and Civil Liberties Oversight Board (PCLOB), and annual reports from chief privacy and civil liberties officers and relevant agency inspectors general.[9]

[9] "Cyber Security Task Force: Public-Private Information Sharing," Bipartisan Policy Center, Homeland Security Project, National Security Program, 2012, http://bipartisanpolicy.org/sites/default/files/Public-Private%20Information%20Sharing.pdf.

Although the Strengthening and Enhancing Cyber-security by Using Research Education[10] (SECURE IT) Act did not pass, it proposed biennial evaluation from the PCLOB, the agency or department heads overseeing cyber security centers,[11] and annual reports from agency inspectors general.[12] Admittedly, it is an ambitious objective. Known barriers prevent information sharing between federal, state, and local law enforcement agencies and PSAPs. Fiscal, policy, control, trust, risk, governance, and technical issues need to be assessed and mitigated. Perhaps the biggest barrier is the cultural barrier that many agencies experience, "have never done it that way."

Is it possible that other state and federal projects can be leveraged or modeled to create an information-sharing environment? The creation of the Joint Terrorism Task Force (JTTF) to break down information-sharing roadblocks that can exist between state and federal law enforcement agencies has been considered a step in the right direction. The JTTF reviews active cases being handled by local and state agencies.

A measure of success is to comply with the recommendations from the Intelligence Reform and Terrorism Prevention Act of 2004, The National Strategy for Information Sharing (NSIS), "As the terrorist attacks on transportation infrastructure in London and Madrid demonstrate, critical infrastructure can be a prime target for the transnational terrorist enemy we face today. The private sector owns and operates an estimated 85% of infrastructure and resources that are critical to our Nation's physical and economic security. It is, therefore, vital to ensure we develop effective and efficient information sharing partnerships with private sector entities."[13] It is time to include the fusion centers and the private sector to the table; by using data from PSAPs, it is possible to improve the amount of information sharing from the local level.

---

[10] "Strengthening and Enhancing Cyber-security by Using Research, Education, Information, and Technology Act of 2012," American Public Power Association, accessed September 8, 2014, www.publicpower.org/files.

[11] Bipartisan Policy Center, Homeland Security Project, National Security Program, *Cyber Security Task Force: Public-Private Information Sharing*.

[12] Ibid.

[13] "Sharing Information with the Private Sector," The National Security Council, accessed August 25, 2014, http://georgewbush-whitehouse.archives.gov/nsc/infosharing/sectionV.html.

C. RESEARCH METHODOLOGY

Research for this thesis follows three approaches: a literature review to summarize federal guidelines for information sharing initially developed immediately following 9/11, and subsequent documents describing best practices and interpretations of information sharing from public and private sectors. The second is a review of best practices, risks, and the cost benefits to be considered when implementing an information-sharing model. The third presents four separate case studies that have demonstrated a variety of success, wide range of costs, types of technology implemented, and sustainability issues.

A review of return on investment is included in the assessment. As with most projects, an unending supply of resources and funding is most invaluable. This study considers the cost of implementation and the on-going maintenance costs. The level of effort to implement is also a critical decision-making factor for most agencies, as many PSAPs do not have dedicated staff members who can create, install, monitor, troubleshoot, and enhance products designed to receive data and forward it to other systems for further dissemination.

D. BIAS SENSITIVITY

In psychology, heuristics are simple, efficient rules that people often use to form judgments and make decisions. They are mental shortcuts that usually involve focusing on one aspect of complex problems while ignoring other aspects. These rules work well under most circumstances, but they can lead to systematic deviations from logic, probability, or rational choice theory.[14]

"Rational choice theory is the view that people behave as they do because they believe that performing their chosen actions have more benefits than costs. That is, people make rational choices based on their goals, and those choices govern their

[14] *Wikipedia*, s.v. "Heuristics in Judgment and Decision-Making," accessed July 16, 2014, http://en.wikipedia.org/w/index.php?title=Heuristics_in_judgment_and_decision-making&oldid=622513820.

behavior."[15] Data sets, presented in clear and understandable manner, should be developed that demonstrate the desired outcome can be achieved by using simple information strategies and credentialing trusted and secure networks. Trust does not come easy but this nation must be willing to create an environment that helps law enforcement understand the objective, how it benefits the agency and the community, and most importantly, that law enforcement has a say in how the process is affected.

The resulting errors are called cognitive biases. Many different types have been documented that have been shown to affect people's choices in situations, such as valuing a house or deciding the outcome of a legal case. These choices are not necessarily based on fact but often based on prior experience or comfort levels with the current decision-making methods and the pre-desired outcome. Another way to describe it is, *if it is not broken, don't fix it*.

> In the early 1970s, psychologists Amos Tversky and Daniel Kahneman demonstrated three heuristics that underlie a wide range of intuitive judgments. These findings set in motion the Heuristics and Biases research program, which studies how people make real-world judgments and the conditions under which those judgments are unreliable. This research challenged the idea that human beings are rational actors, but provided a theory of information processing to explain how people make estimates or choices. This research has guided almost all current theories of decision-making.[16]

Although a significant amount of research has focused on how heuristics lead to errors, they can be seen as rational in an underlying sense. According to this perspective, heuristics are good enough for most purposes without being too demanding on the brain's resources. Another theoretical perspective sees heuristics as fully rational in that they are rapid, can be made without full information, and can be as accurate as more complicated procedures. By understanding the role of heuristics in human psychology, marketers and

---

[15] "Rational Choice," Chegg.com, 2014, http://www.chegg.com/homework-help/definitions/rational-choice-49.

[16] *Wikipedia*, s.v. "Heuristics in Judgment and Decision-Making."

other persuaders can influence decisions, such as the prices people pay for goods, or the quantity they purchase.[17]

As a manager of several PSAPs during the past 12 years and having worked in this industry for more than half of his life, the author considers himself to have a strong understanding of the technological requirements and the operational considerations of operating a contemporary PSAP. The author recognizes that he may have some inherent cognitive and rational choice biases based on professional experience, training, and education. Having spent time in the private sector delivering 911 services and data in real time, the author has observed that these types of technical projects, when funded properly with employees who possess the required competencies, can be delivered quickly and effectively in the public sector. The author is aware of his biases and has worked diligently to recognize when these biases present themselves during the research.

[17] Ibid.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

This literature review identifies information resources relevant to the assessment of the nation's PSAP ability to gather potentially important public safety-related information from millions of callers, and automatically forward the information and data to state fusion centers, public stakeholders, school administrators, business owners, and other state and federal agencies for analysis. Various publications and project documentation describe the tactics, strategies, and best practices in the area of public safety information sharing including academic research conducted on the topic of information sharing between PSAPs and other public safety stakeholders. For these projects to be successful, business rules for information sharing must be established and agreed upon by all participants. This literature review identifies three types of information and research resources regarding the sharing of information between federal, state, municipal, and media entities.

A. STUDIES AND REPORTS BY THE UNITED STATES GOVERNMENT

A significant amount of literature exists about information sharing between the federal government and municipal entities, which clearly demonstrates that the body of knowledge supports a top down methodology of information sharing. In other words, much of the literature discusses in detail how intelligence flows from the federal level to the state and down to the municipal level. This is not to say that the problem of information sharing has been resolved, for it has not. What is missing is research and discussion of bottom up and peer-to-peer information sharing.

America faces a dynamic and constantly changing national security environment in which nation states, talented non-state actors, domestic lone wolves, and transnational entities continue to use technology and information to create opportunities to exploit the national security networks. The National Intelligence Strategy (NIS) describes a new paradigm in the war on terror.

"Rapid technological change and dissemination of information continue to alter social, economic, and political forces, providing new means for our adversaries and

competitors to challenge us."[18] The public sector must be engaged in any rapid change of direction affected by the government or a requirement for information.

Residents call 911 when they are injured, observe crimes, fires, and witness critical events. The Aurora Cinema[19] attack in Aurora, Colorado, on July 20, 2012, and the Boston Marathon Bombings[20] in Boston, Massachusetts, on April 15, 2013 are recent examples of the types of critical events in which PSAPs were the initial point of contact and crucial in the emergency and multi-agency tactical response. Had the incident commander been notified immediately of these incidents, it is possible that the intelligence gathering could have begun at earlier phases of these events.

Consider the recent shootings at the Washington Navy Yard in the District of Columbia, even as the suspect was being identified, Americans heard "No piece of information is too small," from Valerie Parlave, deputy assistant director in charge of the Washington, DC FBI office."[21] Parlave demonstrates the importance of information irrespective of its apparent insignificant. PSAPs have mountains of categorized data that can literally become a forensics expert's goldmine.

Improved bottom up information sharing warrants further research, as demonstrated by Parlave's call from the community to be on alert and seeking the assailant, "Communication breakdowns between military, federal and local law enforcement complicated the search for the gunman during Washington Navy Yard,"[22] according to a District police report stating police officers were unable to access live video of the shooter as they stormed into harm's way. "…the U.S. Navy failed to tell

---

[18] "The National Intelligence Strategy," Office of the Director of National Intelligence, 2009, http://fas.org/irp/offdocs/nis2009.pdf.

[19] Tom Foreman, "A Timeline of the Colorado Theater Shooting," *CNN.com*, July 20, 2012, http://www.cnn.com/interactive/2012/07/us/aurora.shooting/index.html.

[20] "Updates on Boston Marathon Bombing," Federal Bureau of Investigation (FBI), August 2013, http://www.fbi.gov/news/updates-on-investigation-into-multiple-explosions-in-boston.

[21] Barbara Starr, Catherine E. Shoichet, and Pamela Brown, "12 Victims Slain in Navy Yard Shooting Rampage; Dead Suspect ID'd," *CNN.com*, September 16, 2013, http://www.cnn.com/2013/09/16/us/dc-navy-yard-gunshots/index.html.

[22] Peter Herman and Clarence Williams, "Confusion Marred Police Response to Navy Yard Shooting," *The Washington Post*, July 11, 2014.

local police commanders that a video feed from 160 cameras in the corridors where Aaron Alexis, 34, opened fire could be accessed from a room just inside the building."[23]

During the response after action, it was learned that too many officers were self-deployed to the scene in an effort to help. For all their good intentions, their presence overcrowded the scene, which made it difficult to maintain chain-of-command, and officers were unable to command the field force effectively. Commanders were communicating on a variety of radio channels. When they were on the same radio channel, they talked over one another. Command vehicles blocked tactical pathways for officers, and according to a report issued by the Navy, "there was confusion among some responders—and even top officials—about who was in charge."[24] This confusion could have been avoided with a communications tool directing officers where and when to respond. The incident commander did not have the ability to manage the incident effectively.

The self-deployment issue continues to plaque law enforcement and other first responder communities, and complicates all aspects of the response, including the fundamentals of incident command. Self-deploying officers without direction from the incident command could be resources that might be needed in another aspect of the event, and by reporting to the active scene could actually compromise responder safety when appearing in tactical zones at which they are not expected.[25]

The same problem occurred in Boston during the public safety response to the Boston Marathon bombings. During the post-incident assessment, the question of self-deployed officers was raised, as it related to the shooting of the campus police officer maintaining a perimeter in Cambridge. Investigators were unable to determine whether the officer was killed by friendly fire.

---

[23] Herman and Williams, "Confusion Marred Police Response to Navy Yard Shooting."

[24] Ibid.

[25] "National Incident Management System. Resource Management and Complex Incidents," Federal Emergency Management Agency (FEMA), 2010, http://training.fema.gov/EMIWeb/IS/IS703A/06_IS703_SM_Aug2010.pdf.

> We had so many self-deployed officers, we don't know where the bullets from all of those guns came from," the source said. "In such a confused set of circumstances, with so many local, state and federal police folks there, there was very little coordination, and each of those agencies has a different set of policies and different set of training, so altogether it's amazing no innocent person was killed.[26]

Relevant and contemporary literature begins with an overview of a Department of Homeland Security program titled, *If You See Something, Say Something*™. This public awareness campaign is intended to "raise public awareness of indicators of terrorism and terrorism-related crime and to emphasize the importance of reporting suspicious activities to the proper authorities, by calling 911."[27] Since PSAPs are the de facto points-of-contact for the communities that adopt the *If You See Something, Say Something* program, PSAP employees must be prepared to meet the expectations of the community, customers, and program administrators.[28]

The 9/11 Commission Report framed the failures that led to 9/11. It identified a key structural failure of the intelligence community, both before and after 9/11, as the organization of national intelligence around the intelligence "collection disciplines of home agencies," which makes it impossible to connect the dots due to a lack of integrated information.[29] A review of a public safety information-sharing project in New York State focused on information sharing and endorsed the citywide network that connected law enforcement agencies with federal agencies. Public safety leaders created the "public sector knowledge networks" (PSKNs) that worked to "treat information and knowledge

---

[26] Phillip Martin, "'Self-Deployment' May Have Caused Confusion during Boston Marathon Bombing Manhunt," WGBH Online, October 16, 2014, http://wgbhnews.org/post/self-deployment-may-have-caused-confusion-during-boston-marathon-bombing-manhunt.

[27] "If You See Something, Say Something™," Department of Homeland Security, August 20, 2013, http://www.dhs.gov/if-you-see-something-say-something%E2%84%A2-campaign.

[28] Ibid.

[29] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report*, 408.

sharing across traditional organizational boundaries as a primary purpose as they try to address public needs that no single organization or jurisdiction can handle alone."[30]

The NSIS[31] states, "information sharing should be the rule, not the exception," and that the information-sharing environment will not be constructed overnight, but will *evolve* over time. The NSIS was created with the understanding that homeland security information, terrorism information, and law enforcement information related to terrorism, can come from multiple sources, all levels of government, as well as from the private sector. The directive makes it clear that information should flow "top down" but also "peer-to-peer and bottom up."

The 108th Congress enacted the Intelligence Reform and Terrorism Prevention Act[32] of 2004, which was legislation to reform the intelligence community and the intelligence-related activities of the U.S. government. Fostering information sharing is a core Department of Homeland Security (DHS) mission. Specific relevance of the PSAP roles is found in the Intelligence Reform and Terrorism Prevention Act in Subtitle C– National Preparedness,[33] which outlines the public safety role in national preparedness, interoperability (section 7303), critical infrastructure (section 7306), and readiness assessments (section 7306).[34] The question at this point is whether the nation's PSAPs are capable of connecting to the *secure* information-sharing networks.

---

[30] Sharon S. Dawes, Anthony M. Cresswell, and Theresa A. Pardo. "From "Need to Know" to "Need to Share": Tangled Problems, Information Boundaries, and the Building of Public Sector Knowledge Networks," *Public Administration Review* 69, no. 3 (May/June 2009): 39–402, http://onlinelibrary.wiley.com/doi/10.1111/j.1540-6210.2009.01987_2.x/full.

[31] Department of Homeland Security, "National Strategy for Information Sharing, Successes and Challenges in Improving Terrorism-Related Information Sharing," Information Sharing Environment, October 2007, http://www.ise.gov/sites/default/files/nsis_book.pdf.

[32] "National Strategy for Information Sharing and Safeguarding," The White House, December 2012, http://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy_1.pdf.

[33] *Intelligence Reform and Terrorism Protection Act of 2004 (IRTPA)*, Pub. L. No. 108–458, 118 Stat. 3638 (December 17, 2004), codified at 42 U.S.C. §2000ee, 50 U.S.C. §403-1 et seq., §403-3 et seq., §404o et. seq, accessed August 24, 2013, http://www.gpo.gov/fdsys/pkg/PLAW-108publ458/pdf/PLAW-108publ458.pdf.

[34] Ibid.

Congress and President Obama have made it clear that one of DHS's core missions is to create the technological and organizational infrastructure necessary to promote the sharing of information regarding terrorism, homeland security, law enforcement, weapons of mass destruction, and incidents of all types within the DHS realm, across the federal government, and with state, local, tribal, territorial, private sector, and international partners.[35] Many of the capabilities exist but the mindset of public safety leaders, for the most part, has yet to change.

The 9/11 Commission Report[36] made numerous recommendations to improve information sharing, and in 2011, the DHS published a report on the status of implementing the recommendations from the 9/11 Commission Report. The follow-up report provides a glowing review of work completed to improve information sharing, but makes no reference of bottom up information sharing despite recognizing that security begins with hometown security: "Over the past several years, DHS has strengthened and evolved our homeland security enterprise to better mitigate and defend against dynamic threats. This approach is based on the simple premise that homeland security begins with hometown security."[37] Examples of information gathering from the local level are scarce. "Simply put, DHS is focused on assembling information and sharing it across the country in a way best designed to protect the homeland."[38]

The National Response Framework (NRF)[39] describes the delivery of "coordinated, prompt, reliable, and actionable information to the whole community through the use of clear, consistent, accessible, and culturally and linguistically appropriate methods to effectively relay information regarding any threat or hazard."

---

[35] "Information Sharing Strategy," Department of Homeland Security, 2008, http://www.dhs.gov/xlibrary/assets/dhs_information_sharing_strategy.pdf.

[36] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report*.

[37] "9/11 Commission Recommendations, Progress Report," Department of Homeland Security, 2011, http://www.dhs.gov/xlibrary/assets/implementing-9-11-commission-report-progress-2011.pdf.

[38] Ibid.

[39] "The National Framework for Strategic Communications," The White House, 2009, http://www.fas.org/man/eprint/pubdip.pdf.

Missing is a strategy or recommendation to move information and data from front-line information gatherers upward to federal, state information analysts, or peer-to-peer.[40]

The NIS[41] August 2012 warns that state, non-state actors will have an increasing impact on this nation's national security. Many of these actors have attempted to deploy, or have deployed, strategies that have direct impacts on the commerce and well-being of the residents of U.S. communities, such as the release of pandemics, improvised explosive devices, school shootings, or wild land fires.[42] PSAP employees are the first of the first responders and have the responsibility to not only gather information quickly, and dispatch first responders, but also to share critical information promptly with state fusion centers and state and federal partners.

The Patriot Act[43] directs the sharing of information inter-agency cooperation among government agencies. The Patriot Act removes the legal barriers that prevented the intelligence community (IC), law enforcement entities, and military stakeholders from collaborating when working to ensure the safety of the American people. A spokesperson from the Department of Justice (DOJ) stated, "now police officers, FBI agents, federal prosecutors and intelligence officials can protect our communities."[44] Yet, no structured mechanism is in place for sharing information *from* the front lines or *with* the front lines.

B. ACADEMIC LITERATURE

In the book, *Megacommunities*, the authors present a compelling argument for federal, state, and local entities to collaborate with private sector and municipal entities to identify and resolve increasingly complex security issues. The concept is based on the studies in the fields of group dynamics, network theory, behavior, and in the service of the goal of sustained solutions to problems, "that no single organization or methodology

---

40 "National Response Framework," Federal Emergency Management Agency (FEMA), 2013, http://www.fema.gov/core-capabilities#IntelandInfo.

41 "The National Intelligence Strategy."

42 Ibid.

43 "What is the Patriot Act?" Department of Justice, 2002, http://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf.

44 Ibid.

can solve alone."[45] The argument is sound as no silver bullet exists to fix the information-sharing conundrum for all communities, but it should serve as a model to encourage communities and law enforcement to begin to build a patchwork of information-sharing networks, and create proofs of concept models that other communities can adopt.

Mark Lowenthal's work explains in great detail how information should be gathered to contribute to the intelligence gathering process.

- "Requirements
- Collection
- Processing and exploitation
- Analysis and production
- Dissemination
- Consumption
- Feedback"[46]

Lowenthal states that information is not intelligence; rather *gathering* is a critical aspect of the intelligence cycle that must be completed so that information can be sent to IC for analysis. Increased amounts of information increase the level of effort of finding truly important intelligence.[47] Information and data come from a variety of sources and each need to be given credence, and not summarily dismissed based on the source. "Given the nature of the intelligence cycle and the segmented organizational structure used to perform it, knowledge sharing among agencies is necessary to produce good intelligence."[48] Information from PSAPs can be sent to fusion center analysts who can

---

[45] Mark Gerencser, Reginald Van Lee, Fernando Napolitano, and Christopher Kelly, *Megacommunities: How Leaders of Government, Business and Non-profits Can Tackle Today's Global Challenges Together* (New York: Palgrave Macmillan, 2008), 18.

[46] Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 5th ed. (Los Angeles: SAGE/CQ Press, 2012), 57.

[47] Lowenthal, *Intelligence: From Secrets to Policy*, 62.

[48] William J. Lahneman, *Keeping U.S. Intelligence Effective, The Need for a Revolution In Intelligence Affairs* (Maryland: Scarecrow Press, 2011), 187.

then develop reports and publish the reports not only to the PSAP providing the data but those agencies within the same proximity of the events; those most likely to be impacted by the findings of the fusion center.

Jennifer Simms states in *Transforming U.S. Intelligence*, "the heart of intelligence, then, is not in the plumbing for getting raw data from the collector to the appropriate user. It is rather the *enabling* of appropriate action over time."[49] The objective is to move information into the pipeline for further analysis. Those agencies that provide information or raw data to the fusion centers are the exception. Fusion center employees may have one or two sources at each agency on whom they can depend but the information flow is inconsistent and limited.

James J. Wirtz, Dean at the Naval Postgraduate School (NPS), School of International Graduate Studies, states that globalization and the information revolution will make collaboration between agencies easier; it will also make the challenges of keeping up with the flow of information more difficult. "The barriers are breaking down between intelligence practitioners and scholars."[50] Wirtz reiterates that information does not flow easily across the bureaucratic boundaries, even against well-understood threats, and good intentions of sharing information. Information should be disseminated to a state fusion center or a similar entity at which it can be evaluated and determined whether it represents actionable information that can result in a product or a tip. This dissemination is not happening across the county.

C. STUDIES BY THE MASS MEDIA

"Information Sharing in the Era of Social Media," an article published in *Homeland Security Magazine*,[51] discusses the pros and cons of using social media to

---

[49] Jennifer E. Sims, *Transforming U.S. Intelligence* (Washington, DC: Georgetown University Press, 2005), 27.

[50] James J. Wirtz, "The Sources and Methods of Intelligence Studies," Naval Postgraduate School, Center for Homeland Defense and Security, 2012, https://www.chds.us/coursefiles/NS4156/lectures/intel_sources_methods/player.html.

[51] Chris Russo, "Information Sharing in the Era of Social Media," 9-1-1 Magazine.com, July 2011, http://www.9-1-1magazine.com/ELERTS-Russo-Information-Sharing.

notify shopping centers, large commercial facilities, schools, and universities of nearby emergencies. The concept can be difficult for PSAP managers and first responders to embrace, as the methodology steps outside the routine processing of calls for service, but PSAP employees must be able to publish information that will reach the most people as quickly as possible. "As emergency managers, PSAP employees have the opportunity to make dramatic changes in the way we do business."[52]

D. SUMMARY OF LITERATURE REVIEW

Adequate literature is available to conduct meaningful research on the information-sharing capabilities, policies, and practices of the nation's PSAPs. A variety of technologies is available; some proprietary and some open source that could enable the information sharing in the bottom up methodology described earlier. It is time for the American PSAPs to step into the 21st century and leverage relationships and existing technologies to help keep America safe by being part of the information continuum.

What is surprising is the relatively small number of programs utilizing simple programs to share information. When agencies do share information, it generally goes right back up the stovepipe as opposed to peer-to-peer or to public safety stakeholders, such as schools, businesses, and corporate partners.

[52] Russo, "Information Sharing in the Era of Social Media."

III. INFORMATION SHARING FROM THE PSAP

A. BENEFITS OF INFORMATION SHARING

Information and knowledge are vastly different; information is the basis for knowledge, yet knowledge is required to interpret and understand information.[53] Information sharing must go beyond the simple exchange of data. The Information Sharing Executive (ISE) was established in the Office of the Director of National Intelligence (DNI) to establish and affect information sharing protocols; however, the mindset of local law enforcement is slowly changing from the collective mindset is "need to know" to "need to share."

Admittedly, the primary duties of the nation's PSAPs are to gather information from callers, summarize the information into concise and crisp details, and dispatch the closest and most appropriate first responders as promptly as possible. The question then becomes is it feasible to expand the responsibilities and duties of PSAP employees not only to receive information and dispatch emergency responders, but to also become active participants in the intelligence cycle by forwarding potentially actionable data breadcrumbs to fusion centers and other state and federal partners?

Many computer aided dispatching systems (CAD) have the capability to forward information automatically to other systems, which in turn, can, automatically develop reports and forward information to records management systems (RMS), jail management systems (JMW) or other entities. PSAP employees do not have the responsibility to analyze the data, nor do they have the time to do so.

Creating and maintaining an information-sharing environment has many benefits. It provides access to neighborhood resources and current program information, such as information about public safety threats. Environmental and societal issues, and

[53] Thomas Davenport, David DeLong, and Michael Beers, "Successful Knowledge Management Projects," *Sloan Management Review* (Winter 1998): 43–57, https://www.ischool.utexas.edu/~i385q/readings/Davenport_DeLong-1998-Successful.pdf.

information-sharing networks create an environment for developing trust.[54] Yet, despite the generic police practice of instructing people to call 911 when they need help, by law enforcement is hesitant to involve the community in fighting crime or sharing information related to crime. In short, the local law enforcement entities need to *lean* into preventing, observing, and reporting crime, as opposed to responding to the scene after it has occurred.

B. PROBLEMS WITH INFORMATION SHARING

Publishing and sharing information can be problematic; law enforcement agencies may be leery of sharing information that might compromise the integrity of an investigation or crime scene. Law enforcement officers need to protect active crime investigations to preserve the integrity of evidence collection and the evidentiary chain of custody for subsequent prosecutorial action.

Sharp lines of authority are drawn between the government branches, including federal, state, and local agencies, and those boundaries are pervasive, embedded, and are in fact, the way business is conducted in most law enforcement environments. The process appears flawed and chaotic to those standing on the periphery, although to those who operate daily in this paradigm, the system works well, as long as the user requires information only from the home agency. Information is used to barter position and power, and sharing information is considered bad form in some entities.[55]

Another problem with information sharing is that stakeholders may not share a common understanding of business practices, jargon, nomenclature, or may not have a clear understanding or meaning of the data. While the required action to take may be clear to one agency, the messages may not exist in the lexicon of other agencies.

---

[54] Matthew S. Kraatz, "Interorganizational Networks and Adaption to Environmental Changes," *Academy of Management Journal* 41, no. 6 (1998): 621–43; Walter W. Powell, "Hybrid Organizational Arrangements: New Form or Transitional Development?" *California Management Review* 30, no. 1 (1998): 67–87; Lynne G. Zucker et al., "Collaboration Structure and Information Dilemmas in Biotechnology: Organizational Boundaries As Trust Production, NBER WorkingPaper No. 5199, *National Bureau of Economic Research*, July 1995.

[55] Dawes, Cresswell, and Pardo, "From "Need to Know" to "Need to Share": Tangled Problems, Information Boundaries, and the Building of Public Sector Knowledge Networks."

Data can be interpreted differently through inexperience, or unfamiliarity with the manner in which it is collected, stored, and distributed. The transference of data and information must be done consistently and congruently with end user education and instruction in the use of the data.

A complete and common understanding of the information can only come after an exchange of theory, practice, policy, terminology, analysis, and presentation. William Bratton was instrumental in the development of a now widely used police agency accountability tool developed by the New York City Police Department, known as Comp Stat crime reviews. Crimes were tracked by precinct, and commanders were summoned to headquarters to explain the changes, or lack of changes, in crime patterns. What was initially viewed as a bureaucratic annoyance translated into improved information for the officer on the beat, improved performance, and ultimately, a reduction in crimes. The image of New York City improved to become one of the safest large cities in the world because the police department developed a common language, common metrics, and held officers accountable.

Bratton framed his argument well, "Your vision needs to be broad enough to appeal to a variety of people and organizations. You can't be all things to all people. But you need to be something to enough people to come together and make their aspirations a reality."[56]

C. CONTEMPORARY BARRIERS TO INFORMATION SHARING

Barriers to information sharing occur in a variety of combinations: Governance, policy, and legal issues prevent the ability for agencies to collaborate and permit the free flow of information from public safety agencies to public safety stakeholders.[57]

---

56 William J. Bratton and Zachary Tumin. *Collaborate or Perish!: Reaching across Boundaries in a Networked World*. (New York: Crown Business, 2012).

57 Todd R. La Porte and Daniel S. Metlay, "Hazards and Institutional Trustworthiness: Facing a Deficit of Trust," *Public Administration Review* 56, no. 4 (1996): 341–47.

Cost factors also create barriers to information sharing across jurisdictional boundaries, as agencies do not want to incur costs for a partering entity, especially those that may have competing agendas and missions.

Sharing information can lead to the perceived loss of control, breaches of confidentiality, and a lack of inclusion in decision making. Trust, or the lack of trust, is another inhibitor to information sharing. Work cultures, values, and relationships often define the outcomes of information sharing. When trust is low or non-existent, the flow of information is hindered, and efforts are increased to prevent any exploitation of shared information, which is the opposite of collaboration.[58]

Risk is inevitable and inherent in knowledge and information sharing, which impedes the free flow of information. Privacy, security, storage, authority, the release or the potential for the release of information, and confidentiality breaches, create a potential for risk. The definition of risk may vary between entities. This difference also adds to the disagreement of risk and decreases the trust in the relationship.

Arguably, the most difficult aspect of establishing information-sharing networks or systems is the development of governance and policy between agencies. It is fair to say that the higher the number of participating agencies contributing information to the knowledge base or system, the higher the complexity of the project doctrine. Certainly, some legal framework for sharing information is prudent and networks that have well defined expectations seem to operate more effectively and for longer durations. Roles and responsibility, fiscal responsibilities, resource allocation, and administrative tasks should be clearly defined in the project governance, memorandums of understanding (MOU) or letters of agreement (LOA).

D. PRIVACY ISSUES

Since 9/11, the FBI has transitioned from crime-fighting to an intelligence-led, threat-driven organization that is guided by clear operational strategies. "The FBI works

[58] Anthony M. Cresswell, G. Brian Burke, and Theresa A. Pardo, "Advancing Return on Investment Analysis for Government IT: A Public Value Framework," *Center for Technology in Government*, 2006, http://www.ctg.albany.edu/projects/proi.

to predict and prevent the threats we face while at the same time engaging with the communities we serve. This shift has led to a greater reliance on technology, collaboration, and information sharing."[59]

> Effective information exchange is a requisite for the success of the unique FBI national security and law enforcement missions. Dynamic operations, a shifting policy environment, and improvements in technological capabilities characterized the FBI in 2011, reinforcing continued need for broad, agile, but secure information exchange. The FBI is committed to sharing timely, relevant, and actionable intelligence with the widest appropriate audience while protecting the privacy and civil liberties of the American people. It is also committed to making the best possible use of information these partners share with the FBI. The FBI continually promotes an information-sharing culture, deploys new technologies, and refines its policies and procedures in support of its commitment.[60]

E. THE CHALLENGES OF DEVELOPING AN EFFECTIVE INFORMATION SHARING MODEL

Therefore, these questions remain, what barriers exist that prevent first responders from adopting the mindset of "need to share?" What is the currency they need to buy into the system? How do public safety stakeholders, school administrators, and business owners build trust with the local and state law enforcement agencies? Will this public sharing actually help to keep this nation's schools and malls safer?

The difficulty of information sharing is rooted in the long-standing history of traditions, the need to control, leadership ego, hubris, and outmoded business rules. The idea of sharing information with non-traditional business partners is completely contrary to the manner in which public safety has done business for decades. The concept challenges current command and control systems, the values and the missions of public safety leadership teams that have been founded in military models, and paramilitary leadership models.

---

[59] "Information Sharing and Safeguarding Report 2012."

[60] Ibid.

Trust, risk, cost, liability, breaches of confidentiality, and the fear of change can all be components of the hesitation. Other reasons for this hesitation deserve to be illuminated and discussed in an academic setting. Are the challenges too great?

F. ESTABLISHING A NEW PARADIGM

Today's leaders must innovate and utilize existing technology to help improve the safety and security of the homeland. First responders may use social media or similar technologies to inform schools and neighborhoods of recurring problems, or at the minimum, repurpose existing technologies so that the learning curve is reasonably rapid. In so doing, various elements can be actively engaged and have a participatory role in their own safety as well.

> Federal agencies increasingly use recently developed Internet technologies that allow individuals or groups to create, organize, comment on, and share online content. The use of these social media services, including popular Web sites like Facebook, Twitter, and YouTube and provides opportunities for agencies to more readily share information with and solicit feedback from the public. However, these services may also pose risks to the adequate protection of both personal and government information.[61]

The General Accountability Office (GAO) has outlined rules and regulations for the government to follow and the risks that come with utilizing social media.

G. CURRENT STATUS OF PSAP INFORMATION SHARING

Residents have expectations that they will receive prompt service from first responders. Yet, law enforcement agencies are hesitant to share public safety information with public safety stakeholders, and allege that doing so could compromise public safety, jeopardize crime scenes, or impact investigations. The truth is that sharing information facilitates improve information collection and speed of response,[62] and integrated

---

61 Government Accountability Office. *SOCIAL MEDIA: Federal Agencies Need Policies and Procedures for Managing and Protecting Information* (GAO-11-605) (Washington, DC: GPO, 2011), http://www.gao.gov/products/GAO-11-605.

62 David Landsbergen Jr. and George Wolken Jr., "Realizing the Promise: Government Information Systems and the Fourth Generation of Information Technology," *Public Administration Review* 61, no. 2 (2001): 206–220.

information-sharing systems provide citizens with access to information and services. Landsbergen says "positive information sharing experiences can help government professionals build and reinforce professional networks and communities of practice." Communities of practice are people who share concerns and learn how to do it better as they interact regularly.[63]

Law enforcement agencies will demand that information-sharing systems must be managed with high degrees of security and credentialing. This thesis also supports the availability of technologies to extend information to non-traditional public safety stakeholders, including school administrators and business owners without risking first-responder safety. Deploying these technologies can enhance school safety, alert mall security personnel to nearby emergencies in an effort to keep the public safe, while still meeting the security requirements required by state and local law enforcement communities. For example, the vetting of public safety stakeholders by law enforcement personnel can assure that adequate credentialing, training, testing, and auditing is conducted on a routine basis, while at the same time, public safety stakeholders can become law enforcement force multipliers by enhancing situation awareness for trusted partners.

The question then is it feasible to expand the responsibilities and duties of the PSAP employees not only to receive information and dispatch emergency responders but also to become active participants in the intelligence cycle by forwarding potentially actionable data breadcrumbs to fusion centers and other state and federal partners? If these duties cannot completed by an already busy PSAP employee, can information sharing be conducted in a timely manner?

Organizations large enough to own and operate contemporary 911 CAD systems have access to emergency information via an application programming interface (API). An API, defined by *PC Magazine*, is an interface that when implemented, provides linkage to a required computer function to be executed. "…an API implies that a driver or program module is available in CAD to perform a system operation that be linked into an

[63] Etienne Wenger-Trayner, "Communities of Practice: A Brief Introduction," Wenger-Trayner, accessed November 14, 2013, http://wenger-trayner.com/theory.

existing program to perform computer tasks."[64] In layman's terms, an API is a spigot that can connect CAD systems to other systems to share information. To leverage the API, organizations need access to a CAD system administrator and a resource that can parse the desired data and process it by another program, such as a neighborhood notification system, Excel, or Crystal Reports.

The decision not to share is a conscious decision public safety leaders make, based often on prior experience, skills, heirloom knowledge, information gaps, legacy policy issues, risk, and the difficulty of operating in the new paradigm of sharing information with people who are not police officers. The shift requires law enforcement officers to recognize that community stakeholders, school officials, and business owners are indeed as equally, or more, vested in the safety and security of the community. However, information-sharing programs do involve cost.

64 "Definition of API," *PC Magazine, Encyclopedia*, accessed August 15, 2014, http://www.pcmag.com/encyclopedia/term/37856/api.

IV. COST OF COLLABORATION

Costs are most certainly associated with collaboration, as potential partners come together with established expectations, real or imagined, and the hope to create a situation better than the status quo. Give and take occurs in the negotiations, the operation and the maintenance of the public safety dispatching systems, and information collection system maintained by public safety and private sector entities. "Every collaboration has its own currency. It might be money, job advancement or prestige; it might be the deep satisfaction of a mission accomplished, a job well done, a world made better."[65] The currency of PSAP information sharing is the delivery of situational awareness, and for some of the public safety stakeholders, the collaboration impacts the safety of families and the security of this nation's communities.

Lastly, emergency notifications broadcasts cannot be left to public safety personnel. Any event that would require a notification broadcast is also an event that will very likely keep the team members occupied managing the tactics of the operation and working to keep first responders and citizens safe. A personal observation is that these types of notifications were made late, after the fact, or not at all. As Pete O'Dell says in his book, *Silver Bullets*, "humans are the weak link in information sharing."[66] The latency of information sharing from PSAPs is often the human element.

Agencies considering migrating to or adopting an information-sharing platform must consider the intended use of for sharing the information. If the need to share is immediate, then the better solution is to develop an automated platform. If the information is less urgent, then an ad hoc reporting/information-sharing platform may be the best solution.

---

[65] Bratton and Tumin, *Collaborate or Perish!: Reaching across Boundaries in a Networked World*.

[66] Pete Odell, *Silver Bullets: How Silver Bullets: How Interoperable Data Will Revolutionize Information Sharing and Transparency* (Bloomington, IN: AuthorHouse, 2010), 13.

THIS PAGE INTENTIONALLY LEFT BLANK

V. INFORMATION SHARING STANDARDS

> Sharing data can change the world. The web, at its root, is simply a standard protocol for data and virtually the whole network as we use it today from a similar source. Successful data standards come to be taken for *granted*, but building them takes work, foresight, and both technical and political leadership.
>
> —Gary Wolf, Contributing Writer *Wired Magazine*

For the purpose of this thesis, information-sharing standards are defined as documents that describe technical specifications and criteria used as "guidelines, rules and characteristics, definitions to work toward consistency and predictability in the use of data."[67]

A. STATE OF MINNESOTA, METRO GIS POLICY BOARD

The State of Minnesota, Metro Geographical Information Systems (GIS) Policy Board, is one of the earliest standards-setting organization for information sharing. It established a set of guidelines and standards for those entities working with addresses,

> because many datasets are geographically referenced by an address. Defining and using a standard address format will increase the ease with which these datasets can be incorporated into the GIS for mapping and analysis. In addition, because addresses are so often used as a means of communication between and within organizations, standardizing addresses will increase an organizations ability to share these datasets with other organizations. Standard addresses can also increase the efficiency of automated applications. For example, standards may make locating addresses on an E-911 system more efficient and accurate or usable over a wider area covering several communities.[68]

B. NATIONAL EMERGENCY NUMBER ASSOCIATION

The National Emergency Number Association (NENA) is an organization that works to standardize the management, police, and operational procedures of PSAPs and

---

[67] "ISO 9001 Quality Management System: Business and Quality Management," International Organization for Standards, 2011, http://www.standards.org/standards/listing/iso_9001.

[68] "Addressing Workgroup," State of Minnesota, Metro GIS Policy Board, accessed July 16, 2014, http://metrogis.org/teams-governance/addressing-work-group.aspx.

offers dozens of standards; however, the following standards are the most relevant with regard to this thesis.

Standard Number	Document Name	Committee	Approved Date
	Data Structures & Management Documents		
02-010	Standard Legacy Data Formats For Data Exchange GIS Mapping	Core Services	3/28/2011
02-014	GIS Data Collection and Maintenance Standards	Core Services	6/17/2007
71-001	NG Additional Data Standard	Core Services	9/17/2009
71-501	Synchronizing Geographic Information System Databases with MSAG & ALI Information Document	Core Services	9/8/2009
71-502	An Overview of Policy Rules for Call Routing and Handling in NG Information Document	Core Services	8/24/2010

Table 1. All NENA Standards

- 02-101—This standard recommends the use transmission control protocol/Internet protocol (TCP/IP) in the exchange of data
- 20-014—GIS Data collection provides a standard for archiving data and maintaining the databases in which the data will reside
- 71-001—This standard recommends that agencies size the databases to include additional information for later use, such as GPS data from patrol cars, address routing instructions, and additional premise information
- 71-502—This document describes an overview of how policy is defined, and the ways that they may be used. Policy rules influence the delivery of calls to a PSAP and how these calls are handled based on call-taker skill sets and other criteria. The governing authority defines and implements policy and rules.

C. ASSOCIATION OF PUBLIC-SAFETY COMMUNICATION PROFESSIONALS

The Association of Public Safety Communications Officers (APCO) has far fewer published standards than NENA, but one in particular stands out as relative to information sharing, as it standardizes the naming conventions of the types of emergencies. The standard known as *Public Safety Communications Common Incident Types for Data Exchange* "focuses on providing a standardized list of Common Incident Type Codes to facilitate effective incident exchange between Next-Generation (NG) PSAPs and other authorized agencies, which is a critical component of public safety interoperability."[69]

If an agency is receiving incident information, a basic level of incident classification is required to assure the agency personnel understand the nature of the situation. The creation of this standardized incident type code list does not mean that the agency is required to change the codes it uses internally. The intent is to have each agency map its internal codes to the standardized list."[70]

D. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Founded in 1901, the National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve this nation's quality of life.[71] The most relevant NIST standard related to information sharing can be found in the *Guidance to Promote Security Planning, and Secure System Operations and Administration.* It is important, as it is the first standard in the review that mentions access for the private sector.

---

69 "Standards to Download," The Association of Public-Safety Communications Officials (APCO), 2014, https://www.apcointl.org/standards/apco-standards-for-download.html.

70 Ibid.

71 "NIST General Information," National Institutes of Standards and Technology, updated April 2013, http://www.nist.gov/public_affairs/general_information.cfm.

> …there is a need for timely, relevant, and easily accessible information to raise awareness about the risks, vulnerabilities and requirements for protection of information systems. This is particularly true for new and rapidly emerging technologies, which are being delivered with such alacrity by our industry.[72]

E. AMERICAN NATIONAL STANDARDS INSTITUTE

The American National Standards Institute (ANSI) Homeland Defense and Security Standardization Collaborative (HDSSC) has released a roundtable report examining pressing standardization needs associated with the work of emergency preparedness and response practitioners, including public safety agencies, fire departments and law enforcement entities. The most relative standard from the ANSI is *IEC 15415 Automatic Identification and Data Capture Techniques Package* that defines an international format for data exchange. While not a required American standard, it would be prudent for agencies developing products to adhere to these standards in the event the agency integrates a foreign system in the public safety network.

[72] Karen H. Brown, Deputy Director, "National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce before the Committee on Government Reform, Subcommittee on Government Management, Information, and Technology," National Institute of Standards and Technology, March 9, 2000, http://www.nist.gov/director/ocla/testimony/brown-030900.cfm.

VI. CASE STUDIES

A. REVERSE 911

Systems generically known as Reverse 911 are excellent tools for notifying communities of threats that have lead time, such as a tornados and flooding. These events are sometimes predictable, as forecasters can observe these events developing, which gives PSAP employees time to prepare and launch notifications for looming events.

These systems generally do not require much effort to install and maintain, as they are hosted systems and the hardware and software maintenance costs are part of the contracted services. The PSAP manager has some control over the on-going costs by updating the telephone number database on a less frequent basis; the risk is operating the system with less accurate data. The problem with utilizing less accurate data is that residents or businesses that may have moved into any of the potential zones are omitted from the notifications. The more frequently the telephone database is updated, the more accurate are the telephone numbers in the potential notification zones; however, a higher maintenance cost does occur due to the level of effort to update the database. Most PSAPs have access to reverse notification systems and communities have come to expect these services from their municipal governments.

This thesis argues that reverse notification systems are not the ideal solutions for quick public safety tactical event notifications primarily due to the requirement of human intervention. Tactical neighborhood notifications are generally conducted after incidents have been reported to 911, responders have been dispatched, tactical radio channels have been established, and all the first responders have arrived on the scene, ready to take action. Launching neighborhood notifications are generally an afterthought once a first responder or incident commander realizes that the neighborhood, a nearby school, or businesses must be made aware of the incident.

The actual time required to set up a neighborhood notification includes the transfer of messaging from the incident commander, the PSAP employees' time for inputting the message into the system, developing the target neighborhood boundaries,

testing the message for accuracy, and then actually launching the message. Based on the size of the message, and the number of households that must be contacted, the actual launch can last from five minutes to more, and at times, more than 45 minutes. The author, speaking from personal experience, has observed notification processes that take as long as 60 minutes to complete.

Reverse 911 processing time should be measured from the onset of the emergency. Other factors that impact the delivery of the message to all residents in the targeted area include the duration of the message, the geographic size of the event, and the capacity of the telephone company infrastructure. Telephone company switching centers or central offices can be choke points for telephone messaging. These neighborhood notification systems work well when the PSAP employees have time to develop a crisp and concise message and time for it to be delivered prior to the emergency.

B. AUTOMATED CAD SUSPICIOUS ACTIVITY REPORTS

1. Colorado Information Analysis Center (CIAC)

The Colorado Information Analysis Center (CIAC) is a multi-jurisdictional fusion center staffed by local, state, and federal agencies managed by the Colorado State Patrol (CSP). The CIAC was established in response to the attacks on September 11 with the goal to "prevent, protect against, respond to, recover from and prosecute acts of terrorism."[73] The CIAC is the single point of data collection, analysis, and distribution of terrorism-related information in the form of a daily, or more frequent when necessary, updates, bulletins, and reports to public safety agencies across the state of Colorado.[74]

The main objectives of the CIAC are to provide tactical, strategic collection, analysis, and dissemination of information to local, state, and federal public safety agencies; maintain a terrorism warning communication system; document and disseminate an on-going threat analysis for the state; create and publish intelligence

[73] "Colorado Information Analysis Center," State of Colorado, Official State Web Portal, accessed July 13, 2014, http://www.colorado.gov/cs/Satellite/StatePatrol-Main/CBON/1251594440125.

[74] Ibid.

products for local public safety stakeholders; liaison with the FBI JTTF, and the U.S. Attorney's Office of Anti-Terrorism Task Force; provide training to intelligence consumers, including police officers, firefighters and other first responders; and communicate information sharing initiatives, progress, and successes to stakeholders in order to foster collaboration. This last objective is the basis of this case study.

The vast majority of actionable information sent to the CIAC is from detectives and investigators from law enforcement entities law enforcement agencies across the state. The FBI sends information to the CIAC, as does the U.S. Attorney Office and other fusion centers across the country; what is missing is local information from first responders working the streets.

In 2011, the leaders of the CIAC approached a statewide body of PSAP managers and implored them to send information categorized as suspicious activity report (SAR) to the CIAC as the events were occurring. The proposal was that if a particular event were happening in one jurisdiction, the CIAC's leadership team was certain that the same type or similar criminal activities could be occurring in neighboring jurisdictions sometimes literally across the street. The CIAC would then facilitate the communication to the other jurisdictions in an effort to expedite communication, foster collaboration, and reduce crime. In true government fashion, a form was presented to submit information.

The reception from the PSAP managers was lukewarm and it was apparent that the CIAC's request was going to be largely ignored not because it was a bad idea; the level of effort was outside the scope the PSAP manager's jobs and it was just one more thing that already busy dispatchers would be asked to do. It was not a reasonable request. Within a week of the PSAP manager's meeting, the CIAC leadership team met with the Denver PSAP managers, and in the 10 minutes of the meeting, the CIAC leaders were asking the management of Denver 911 to supply SAR incident information in real time. The request was that once a suspicious event had occurred, a PSAP employee would complete a form and fax it to the CIAC; again, another unreasonable expectation for an already busy communication center.

The Denver PSAP manages more than one million calls per year with a staff of less than 150 employees. Therefore, the likelihood of Denver reporting significant events to the CIAC was highly unlikely. The management team could agree to make those calls, but doing so would create an unfulfilled expectation, and ultimately, damage the working relationship. The simplest solution to providing CAD to the CIAC was to place a CAD terminal in the CIAC, but once the call volume was assessed, it was determined Denver would be delivering haystacks to the CIAC when the CIAC needed needles. This solution was neither feasible nor acceptable; again, due to the call volume handled by the Denver PSAP. Watching the volume of CAD data in an attempt to pick out the salient events would be a full-time job for a CIAC analyst.

Rather than denying the sharing of real time information the Denver team asked the CAD information technology (IT) support team to join the meeting to determine whether or not data could be sent *automatically* to the CIAC in real time, and following a series of meetings, the CIAC and Denver teams were able to automate notifications to the CIAC. The second proposal was more acceptable to the CIAC team, although it represented some effort by the Denver IT team. Information from each 911-telephone call received is entered into CAD by 911 call-takers and then assigned a "nature code," i.e., an in-progress burglary is assigned the nature code "Burg." The teams developed business rules that would be used to create a report, specifically about suspicious activity. The CAD IT team would utilize the CAD API to export data and create a report in Excel, convert it to a portable document format (PDF), and then email the resulting report to the CIAC automatically.

Phase One of the project was simple; the information from any CAD incident that was nature coded as "suspicious occurrence" would be automatically sent to the CIAC analysts.The information would include the fundamentals of information that call-takers were already trained to obtain, including the location of the incident, the caller's name, a call back telephone number, and any of the narrative entered into the CAD incident by the call-taker. Entering this required no additional effort by the call-taker or the dispatcher, and no one had to remember to send the information to the CIAC.

In addition, the CIAC would receive the names of the officers dispatched to the event and the outcome of the police officer's investigation. The Denver management team agreed to send the information to the CIAC with the stipulation that the CIAC analysts would not call the employees at Denver 911 to obtain additional information that may or may not be in the CAD incident. The CIAC analysts would follow-up with the police officers or the victims of the crimes, if appropriate. This project rolled out without any problems, and to the knowledge of any of the participants, absolutely no law enforcement information leaks occurred.

The CIAC team was able to handle the amount of information being forwarded from the Denver 911 CAD system and was ready to enhance the business rules to meet the needs of the CIAC. The teams met again to review the progress and the CIAC team's satisfaction with the CAD SARs report. The level of effort involved with the development of automating the SAR report was 23 hours of IT technician time, estimated at $23.73 per hour for a total of $545.79. Emailing the report to the Denver Police Department (DPD) officers working in the intelligence division so that they can immediately follow up with the officer who handled the incident is an unexpected outcome of using the CAD SAR report.

In the past seven months, the CIAC analysts have been able to attribute numerous successes to the automatic CAD SAR report, including the development of 27 officer safety intelligence briefs disseminated to eight neighboring jurisdictions, the arrests of seven individuals with felony warrants, the recovery of six stolen handguns, and the recovery of stolen equipment issued to police officers, including uniforms, badges, a Tazer, and a long gun. These results were due to sending the CIAC breadcrumbs and the CIAC analysts working with a variety of police agencies in the Denver metropolitan area.

2. Connect and Protect®

The main responsibilities of 911 employees, police officers, paramedics, and fire personnel are to mitigate emergencies. While neighborhood notifications are critical, they are an afterthought. Due to the nature of the event being handled, public safety personnel are already busy stabilizing the event, and notifications become a second thought. It is not

that the public safety practitioners take the task of notifications lightly; they are just extremely busy. One of the best ways to handle emergency notifications with an acceptable level of consistency is for them to be done automatically, essentially taking the human intervention out of the equation.

Portland 911 (Oregon) collaborated with several private technology companies led by Swan Island Networks in association with Redlands, Calif.-based ESRI, FORTiX, and TripWire. The application known as Connect and Protect® automatically pulled information from the Portland 911 CAD system and sent in-progress emergency information over an encrypted Internet connection to credentialed subscribers based on the proximity of the school or business location to the emergency. Not all users received all the information. Only those subscribers in close proximity to the emergency received the information.

The BETA version of Connect and Protect® was intended to notify school administrators and business owners located near emergencies with a goal of providing real-time information to help principals and safety managers make better decisions to maintain the safety of the buildings' occupants. In the first six months of operation, Portland 911 and Connect and Protect® sent 60,000 automatic alerts.

The system was well received by the Portland school district and several of the local businesses and Connect and Protect® was credited for notifying the Lloyd Street Shopping Mall security team for locking gunmen out of the mall following a burglary allegedly committed by them at a nearby bank. The program was recognized by the Kennedy School of Government at Harvard for innovation and received an award in the category of improving homeland security. Swan Island Networks and Portland 911 went their separate ways at the beginning of the recession; Portland 911 stopped working with Swan Island, and Connect and Protect ®was developed into a more advanced product.

Seven years after Connect and Protect®, the application developed by Swan Island Networks was considerably improved. The company has expanded its customer base, entered into commercial partnerships, including with Microsoft, and launched a new product in 2010.

3. Trusted Information Exchange Services®

Swan Island launched a new software called Trusted Information Exchange Services® (TIES) that was developed for organizations using Microsoft CityNext. In February, CityNext, an initiative Microsoft started last July to create smart cities worldwide, partnered with Swan Island to help departments within city governments to communicate better with one another.

The product creates a real-time dashboard that allows municipal leaders to see an overview of city metrics, which provides situational awareness and the advantage of situational awareness. Denver is a pilot site for the improved Connect and Protect application. TIES® has monitored Denver CAD and issued alerts during past three years, and for the past 12 months, Denver 911 has used TIES to distribute its data to trusted partners including the CIAC, which in turn, verifies the data and then distributes critical information and products to law enforcement in neighboring communities. Denver PSAP employees monitor TIES® maps providing real-time situational awareness of the city. The system permits them also to share that data with other agencies in real time.

At the center of TIES is the Common Operating Picture, which shows real-time data from a variety of sources fused in various maps on dashboards. It can display the latest information about severe weather, road closures, health scares, electricity outages, fire conflagrations, and cyber attacks, for instance. TIES works in two phases. First, it gathers data from hundreds of sources, such as social media, local 911 centers, NWS bulletins, intelligence analysis, and even the locations of school buses, using global positioning system (GPS) tracking. Second, it filters the information based on individual preferences and delivers updates on dashboards, as an email, text, or phone call alerts.

It also uses the Common Alerting Protocol (CAP), "a digital format for exchanging emergency alerts that allows a consistent alert message to be disseminated simultaneously over many different communications systems," according to the Federal Emergency Management Agency (FEMA).

For example, a school administrator might desire access to information about pedophiles living nearby, breaking crime news, and gang activity. However, many

schools lack the security resources to address all these threats, so they rely on a close relationship with local police departments.

Similarly, principals can monitor the location and type of emergency calls to determine whether the nearby incidents could affect the school. Implementing TIES requires access to a secure connection and must be vetted by law enforcement personnel.

4. CAD-to-CAD Interfaces

Improving situational awareness is a common objective for many PSAP managers and sharing CAD information with adjacent PSAPs is one way to do it. Some PSAPs are literally located across the street from a neighboring jurisdiction PSAP, and surprisingly, due to the silo business model, those communication centers often have no idea of what emergencies are being handled by the neighboring PSAPs. Sheriff Deputies actually respond through municipal areas, drive using emergency lights and sirens, and pass idle city police cars. The agency may be sending its closest responder, but the closest resource from an adjacent jurisdiction is not being dispatched due to the silo mentality. This situation is not a new dilemma.

A recent trend is to connect CAD systems to create a common operation platform so that one PSAP can interface seamlessly with the neighboring jurisdiction with the objective of sharing information in an effort to identify the closest first responder visually. No doubt exists that having the capability to move information between disparate CAD systems can save precious time, and in the dispatch business, saving time means saving lives.

Another objective of a CAD-to-CAD (C2C) system interface is to connect PSAPs to expedite the dispatch of emergency calls for service by avoiding transferring the telephone caller, a time intensive task that generally confuses the caller. The call-taker who answers the 911 call can input all the required information without transferring the caller. Due to the C2C interface, programming the CAD incident is directed to the correct PSAP. It is common to find numerous PSAPs clustered in metropolitan service areas, such as Santa Clara County, the City of Denver, the Phoenix-Mesa metropolitan area, and the Portland, Oregon metropolitan area. These areas are excellent prospects for C2C

projects.The Department of Homeland Security (DHS) selected these agencies for the purposes of the Computer Aided Dispatch Interoperability Project, as these regions were "the closest to implementing multi-jurisdictional CAD interoperability solutions in a real-world environment."[75]

Currently, if one of the dispatch centers receives a call for service in another jurisdiction, it interrogates the caller to determine the location of the event, the caller's name, the caller's telephone number, and obtains a brief description of what is occurring. Once determined that the caller is outside the call-taker's jurisdiction, the caller is transferred to the correct agency and the destination call-taker will begin the same line of interrogation, which wastes precious minuses and frustrates the telephone caller. The transferring of 911 callers from PSAP to PSAP occurs on a daily basis.

The Santa Clara project is currently in the pilot phase to connect disparate fire CAD systems across San Jose, Milpitas, and Santa Clara County, and when fully implemented, will connect 13 fire agencies in the region. The goal is to send the closest, most appropriate fire responders to medical emergencies and structure fires, irrespective of the home jurisdiction. This project should improve response times and patient care.

The Phoenix-Mesa Metro Area project is currently sharing event information and unit information for fire agencies across separate CAD systems. A CAD-to-CAD interface using the same CAD system with an integrated interface is most likely to succeed, as both agencies share the exact system components and standards. These interfaces are based on similar CAD systems avoiding conflicting and proprietary operating systems that utilize the same geographic system and database structure. While robust and dependable, these systems work as long as all agency CAD systems remain constant and on the save software version. Denver 911 and the Denver International Airport Communication/Dispatch Center is a good example of the use of this interface.

The benefit of this type of interface is that irrespective of where the 911 telephone for service is received, the answering 911 call-taker handles the call from start to finish,

---

[75] "Computer-Aided Dispatch Interoperability Project: Documentation of Regional Efforts," Department of Homeland Security, August 2008, http://www.npstc.org/documents/Computer AidedDispatchDocumentationofEfforts.pdf.

and when done, enters the incident information into the CAD system. The system recognizes the geographic location of the event and sends the call automatically to the correct dispatch center and the correct dispatcher within the center with no inconvenience to the telephone caller; inconvenience being measured in having the telephone call transferred to a different government agency.

The third type of C2C interface utilizes a translation bus that requires each jurisdiction to write system code to the common operation platform. The translations between the various CAD systems is done on the bus, a mechanism that acts as a black box to translate the disparate CAD commands, information and data, and is considered to be more robust that the hard-wired interfaces, but not as robust as the point-to-point C2C using similar hardware, firmware, and software versions. The bus was the solution put into place in the Portland Metropolitan area. The bus was designed to manage data traffic from seven PSAPs and four CAD different systems through two states along a 56-mile corridor.

Each agency in the region relies on differing technologies to support its public safety needs. The proposed solution must be able to adapt to changing hardware, operating system, and software platforms, as well as varying data communications methods. The annual cost to maintain the project exceeded $1.1M with no dedicated funding mechanism; it was not a sustainable project.

VII. CONCLUSION

C. TECHNOLOGY ADVANCEMENTS

The need for public safety interoperability and data sharing came to the forefront following the attacks in September 2001. Government reports, academic studies, and the media were all critical that nobody noticed that the lights were blinking but no one took any action. It is encouraging that technology and the concept of the "need to share" have begun to weave their way into the objective to protect the homeland. The federal decision makers have taken far too long to recognize that the public safety sector can play a large role in the protecting the country. However, that role is also beginning to evolve.

The technology and ease of using it has improved exponentially and the cost for implementing commercial-off–the-shelf (COTS) hardware has made advances in information sharing easier on budgets. Proprietary systems on the other hand may have become more affordable, but in lean economic times, these systems are generally not sustainable and studies have found that industrial usage of personal handheld devices is not effective.

D. THE BEST REASON TO SHARE INFORMATION: SITUATIONAL AWARENESS

Situational awareness is a term that simply means understanding the dynamics in the current situation. It is the ability to look at a huge variety of data, determine what is relevant, synthesize the data, and act on it. In a mass-casualty event or public health emergency, "situational awareness is the ability to collect the correct information, analyze it, and project what will come next so the appropriate actions can be taken."[76]

> To achieve situational awareness, we have to get that right information to the right person who's prepared to receive it, who can analyze it and do something with it.[77]
>
> —Eric Toner, Pittsburgh Medical Center

76 "Computer-Aided Dispatch Interoperability Project: Documentation of Regional Efforts."

77 Institute of Medicine, "Medical Surge Capacity: Workshop Summary," The National Academies Press, 2010, http://www.ncbi.nlm.nih.gov/books/NBK32860/.

THIS PAGE INTENTIONALLY LEFT BLANK

VIII. RECOMMENDATIONS

E. THE MOST EFFECTIVE RETURN ON INVESTMENT INFORMATION SHARING TOOL

The desire to share information with adjacent agencies and public safety stakeholders, such as businesses and schools, is a decision that agency leaders must make. If the agency chooses not to share information, it is a conscious business decision and is the agency's prerogative. Agencies that desire to share information with their partnering agencies and public safety stakeholders must determine the business needs of the communities. In moderately dense metropolitan areas, a C2C interface may produce the best results for the first responders and the communities they serve, and recognize that costs are associated with the collaboration.

The best opportunity and cost effective information-sharing model from PSAPs is the CAD report generating application developed for the Colorado Information Analysis Center. The project cost less than $600 to implement and according to the deputy manager at the CIAC, "the information coming from Denver 911 closed the informational gaps and effectively shared information across the public sectors and peer to peer. The Denver 911 CAD generated SAR reports have helped the CIAC analysts solve eleven crimes that would have otherwise been classified as cold calls.[78] "The Denver 911 SAR reports have helped investigators to recover weapons used in felony crimes, recover drugs and stolen property."[79]

F. OPPORTUNITIES FOR FUTURE RESEARCH

If mutual interest warrants enhancing the CIAC SAR project, the teams may want to include adding intelligence channels or helping customize existing operational dashboards to include additional performance metrics. The CIAC management is interested in finding ways to determine how Denver collects data and is interested sharing

[78] Tracie Keesee, Ph.D. (Deputy Director, Colorado CIAC), in discussion with author, August 28, 2014.

[79] Ibid.

it with other law enforcement agencies in the region, ultimately to combine that effort with the "see something, say something" programs that urge citizens to report suspicious activities.

LIST OF REFERENCES

American Public Power Association. "Strengthening and Enhancing Cyber-security by Using Research, Education, Information, and Technology Act of 2012." Accessed September 8, 2014, www.publicpower.org/files.

Association of Public-Safety Communications Officials (APCO), The. "Standards to Download." 2014. https://www.apcointl.org/standards/apco-standards-for-download.html.

Bipartisan Policy Center. Homeland Security Project, National Security Program. "Cyber Security Task Force: Public-Private Information." 2012. http://bipartisanpolicy.org/sites/default/files/Public-Private%20Information%20Sharing.pdf.

Bratton, William J., and Zachary Tumin. *Collaborate or Perish!: Reaching across Boundaries in a Networked World*. New York: Crown Business, 2012.

Brown, Karen H., Deputy Director. "National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce before the Committee on Government Reform, Subcommittee on Government Management, Information, and Technology." National Institute of Standards and Technology, March 9, 2000. http://www.nist.gov/director/ocla/testimony/brown-030900.cfm.

Chegg.com. "Rational Choice." 2014. http://www.chegg.com/homework-help/definitions/rational-choice-49.

Cresswell, Anthony M., G. Brian Burke, and Theresa A. Pardo. "Advancing Return on Investment Analysis for Government IT: A Public Value Framework." *Center for Technology in Government*, 2006. http://www.ctg.albany.edu/projects/proi.

Davenport, Thomas, David DeLong, and Michael Beers. "Successful Knowledge Management Projects." *Sloan Management Review* (Winter 1998): 43–57. https://www.ischool.utexas.edu/~i385q/readings/Davenport_DeLong-1998-Successful.pdf.

Dawes, Sharon S., Anthony M. Cresswell, and Theresa A. Pardo. "From "Need to Know" to "Need to Share": Tangled Problems, Information Boundaries, and the Building of Public Sector Knowledge Networks." *Public Administration Review* 69, no. 3 (May/June 2009): 39–402. http://onlinelibrary.wiley.com/doi/10.1111/j.1540-6210.2009.01987_2.x/full.

Department of Homeland Security. "9/11 Commission Recommendations, Progress Report." 2011. http://www.dhs.gov/xlibrary/assets/implementing-9-11-commission-report-progress-2011.pdf.

———. “Computer-Aided Dispatch Interoperability Project: Documentation of Regional Efforts.” August 2008. http://www.npstc.org/documents/Computer AidedDispatch DocumentationofEfforts.pdf.

———. “If You See Something, Say Something™.” August 20, 2013. http://www.dhs.gov/if-you-see-something-say-something%E2%84%A2-campaign.

———. “Information Sharing Strategy.” 2008. http://www.dhs.gov/xlibrary/assets/dhs_information_sharing_strategy.pdf.

———. “National Strategy for Information Sharing, Successes and Challenges in Improving Terrorism-Related Information Sharing.” Information Sharing Environment, October 2007. http://www.ise.gov/sites/default/files/nsis_book.pdf.

Department of Justice. “What is the Patriot Act?” 2002. http://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf.

Federal Bureau of Investigation (FBI). “Information Sharing and Safeguarding Report 2012.” 2012. http://www.fbi.gov/stats-services/publications/national-information-sharing-strategy-1/fbi-information-sharing-and-safeguarding-report-2012-2.

———. “Updates on Boston Marathon Bombing.” August 2013. http://www.fbi.gov/news/updates-on-investigation-into-multiple-explosions-in-boston.

Federal Communication Commission. Public Safety and Homeland Security Bureau. “9-1-1 Call Centers/PSAPs.” Accessed May 14, 2014. http://transition.fcc.gov/pshs/psaps.html.

Federal Emergency Management Agency (FEMA). “National Incident Management System. Resource Management and Complex Incidents.” 2010. http://training.fema.gov/EMIWeb/IS/IS703A/06_IS703_SM_Aug2010.pdf.

———. “National Response Framework.” 2013. http://www.fema.gov/core-capabilities#IntelandInfo.

Foreman, Tom. “A Timeline of the Colorado Theater Shooting.” *CNN.com*, July 20, 2012. http://www.cnn.com/interactive/2012/07/us/aurora.shooting/index.html.

Gerencser, Mark, Reginald Van Lee, Fernando Napolitano, and Christopher Kelly. *Megacommunities: How Leaders of Government, Business and Non-profits Can Tackle Today’s Global Challenges Together*. New York: Palgrave Macmillan, 2008.

Government Accountability Office. *SOCIAL MEDIA: Federal Agencies Need Policies and Procedures for Managing and Protecting Information*. GAO-11-605. Washington, DC: GPO, 2011. http://www.gao.gov/products/GAO-11-605.

Herman, Peter, and Clarence Williams. “Confusion Marred Police Response to Navy Yard Shooting.” *The Washington Post*, July 11, 2014.

Institute of Medicine. “Medical Surge Capacity: Workshop Summary.” The National Academies Press, 2010. http://www.ncbi.nlm.nih.gov/books/NBK32860/.

International Organization for Standards. “ISO 9001 Quality Management System: Business and Quality Management.” 2011. http://www.standards.org/standards/listing/iso_9001.

Kraatz, Matthew S. “Interorganizational Networks and Adaption to Environmental Changes.” *Academy of Management Journal* 41, no. 6 (1998): 621–43.

Lahneman, William J. *Keeping U.S. Intelligence Effective, The Need for a Revolution In Intelligence Affairs*. Maryland: Scarecrow Press, 2011.

Landsbergen, David Jr., and George Wolken Jr. “Realizing the Promise: Government Information Systems and the Fourth Generation of Information Technology.” *Public Administration Review* 61, no. 2 (2001): 206–20.

La Porte, Todd R., and Daniel S. Metlay. “Hazards and Institutional Trustworthiness: Facing a Deficit of Trust,” *Public Administration Review* 56, no. 4 (1996): 341–47.

Louisiana National Emergency Number Association. “9-1-1 History.” Accessed July 10, 2014. http://www.louisiananena.org/911history.asp.

Lowenthal, Mark M. *Intelligence: From Secrets to Policy*, 5th ed. Los Angeles: SAGE/CQ Press, 2012.

Martin, Phillip. “‘Self-Deployment’ May Have Caused Confusion during Boston Marathon Bombing Manhunt.” WGBH Online, October 16, 2014. http://wgbhnews.org/post/self-deployment-may-have-caused-confusion-during-boston-marathon-bombing-manhunt.

McConnaha, Michelel. “Week Recognizes Hard Work of County’s 911 Dispatchers.” *Ravalili Republic*, April 15, 2014. http://ravallirepublic.com/news/local/article_1e3cab92-c508-11e3-b7d1-001a4bcf887a.html.

Miller, Robert, Ph.D. “Hurricane Katrina: Communications & Infrastructure Impacts.” In the 2006 Conference *Threats at Our Threshold*. Washington, DC: National Defense University, 2006.

National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report: Final Report*. New York: W.W. Norton & Co., 2004.

National Institutes of Standards and Technology. “NIST General Information.” Updated April 2013. http://www.nist.gov/public_affairs/general_information.cfm.

National Security Council, The. “Sharing Information with the Private Sector.” Accessed August 25, 2014. http://georgewbush-whitehouse.archives.gov/nsc/infosharing/sectionV.html.

Nelson, Gary. “Hurricane Sandy Causes “Failure to Communicate.” *CBS Miami*, October 30, 2013. http://miami.cbslocal.com/2012/10/30/hurricane-sandy-causes-failure-to-communicate/.

Nicholson, Kieran. “Columbine: Training Before Massacre ‘Flawed.’” *Denver Post*, September 23, 2000. http://extras.denverpost.com/news/col0923.htm.

Odell, Pete. *Silver Bullets: How Silver Bullets: How Interoperable Data Will Revolutionize Information Sharing and Transparency*. Bloomington, IN: AuthorHouse, 2010.

O’Donnell, Darrell. “Enabling Information Sharing.” Slideshare, 2013. http://www.slideshare.net/ForgeRock/how-do-get-police-fire-paramedics-and-others-to-share-information-built-trust-into-the-system.

Office of the Director of National Intelligence. “The National Intelligence Strategy.” 2009. http://fas.org/irp/offdocs/nis2009.pdf.

PC Magazine. Encyclopedia. “Definition of API.” Accessed August 15, 2014. http://www.pcmag.com/encyclopedia/term/37856/api.

Police Chief, The. “Law Enforcement Information Technology Standards Council (LEITSC).” 2014. http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=1199&issue_id=62007.

Powell, Walter W. “Hybrid Organizational Arrangements: New Form or Transitional Development?” *California Management Review* 30, no. 1 (1998): 67–87.

Russo, Chris. “Information Sharing in the Era of Social Media.” 9-1-1 Magazine.com, July 2011. http://www.9-1-1magazine.com/ELERTS-Russo-Information-Sharing.

Sims, Jennifer E. *Transforming U.S. Intelligence*. Washington, DC: Georgetown University Press, 2005.

Starr, Barbara, Catherine E. Shoichet, and Pamela Brown. “12 Victims Slain in Navy Yard Shooting Rampage; Dead Suspect ID’d.” *CNN.com*, September 16, 2013. http://www.cnn.com/2013/09/16/us/dc-navy-yard-gunshots/index.html.

State of Colorado. Official State Web Portal. "Colorado Information Analysis Center." Accessed July 13, 2014. http://www.colorado.gov/cs/Satellite/StatePatrol-Main/CBON/1251594440125.

State of Minnesota. Metro GIS Policy Board. "Addressing Workgroup." Accessed July 16, 2014. http://metrogis.org/teams-governance/addressing-work-group.aspx.

Stone, Andrea, and John Rudolf. "9/11 Commission Recommendations on First Responder Network, Civil Liberties Unmet 10 Years after Attacks." *Huffington Post*, September 9, 2011. http://www.huffingtonpost.com/2011/09/09/911-commission-recommendations-unmade_n_950896.html.

Wenger-Trayner, Etienne. "Communities of Practice: A Brief Introduction." Wenger-Trayner. Accessed November 14, 2013. http://wenger-trayner.com/theory.

White House, The. "National Strategy for Information Sharing and Safeguarding." December 2012. http://www.whitehouse.gov/sites/default/files/docs/2012 sharingstrategy_1.pdf.

———. "The National Framework for Strategic Communications." 2009. http://www.fas.org/man/eprint/pubdip.pdf.

Wirtz, James J. "The Sources and Methods of Intelligence Studies." Naval Postgraduate School, Center for Homeland Defense and Security, 2012. https://www.chds.us/coursefiles/NS4156/lectures/intel_sources_methods/player.html.

Zucker, Lynne G., Michael R. Darby, Marilyn B. Brewer, and Yusheng Peng. "Collaboration Structure and Information Dilemmas in Biotechnology: Organizational Boundaries As Trust Production, NBER WorkingPaper No. 5199. *National Bureau of Economic Research*, July 1995.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California