5-2013

Three Essays on Law Enforcement and Emergency Response Information Sharing and Collaboration: An Insider Perspective

Joseph Treglia
Syracuse University

ABSTRACT

This dissertation identifies what may be done to overcome barriers to information sharing among federal, tribal, state, and local law enforcement agencies and emergency responders. Social, technical, and policy factors related to information sharing and collaboration in the law enforcement and emergency response communities are examined. This research improves information sharing and cooperation in this area. “Policing in most societies exists in a state of “dynamic tension” between forces that tend to isolate it and those that tend to integrate its functioning with other social structures” (Clark, 1965). Critical incidents and crimes today cross jurisdictions and involve multiple stakeholders and levels. Law enforcement and emergency response agencies at federal, tribal, state, and local levels, including private sector entities, gather information and resources but do not effectively share this with each other. Despite mandates to improve information sharing and cooperation, gaps remain perhaps because there is no clear understanding of what the barriers to information sharing are. Information sharing is examined using a multi-method, primarily qualitative, approach. A model for information sharing is presented that identifies social, technical, and policy factors as influencers. Facets of General Systems Theory, Socio-technical Theory, and Stakeholder Theory (among others) are considered in this context. Information sharing is the subject of the first work of the dissertation: a theoretical piece arguing for use of a conceptual framework consisting of social, technical, and policy factors. Social, technology, and policy factors are investigated in the second essay. That essay introduces a new transformative technology, "edgeware," that allows for unprecedented connectivity among devices. Social and policy implications for crisis response are examined in light of having technological barriers to sharing resources reduced. Human and other factors relevant to information sharing and collaboration are further examined through a case study of

the Central New York Interoperable Communications Consortium (CNYICC) Network, a five-county collaboration involving law enforcement, public safety, government, and non-government participants. The three included essays have a common focus vis-à-vis information sharing and collaboration in law enforcement and emergency response. The propositions here include: (P1) *Information sharing is affected by social, technical, and policy factors, and this conceptualization frames the problem of information sharing in a way that it can be commonly understood by government and non-government stakeholders.* The next proposition involves the role of technology, policy, and social systems in information sharing: (P2) *Social and policy factors influence information sharing more than technical factors (assuming it is physically possible to connect and/or share).* A third proposition investigated is: (P3) *Social factors play the greatest role in the creation and sustaining of information sharing relationships.* The findings provide a greater understanding of the forces that impact public safety agencies as they consider information sharing and will, it is hoped, lead to identifiable solutions to the problem from a new perspective.

THREE ESSAYS ON LAW ENFORCEMENT AND EMERGENCY RESPONSE INFORMATION SHARING AND COLLABORATION: AN INSIDER PERSPECTIVE

By

Joseph V. Treglia

B.A. Syracuse University, 1988
M.S. Syracuse University, 1993

DISSERTATION

Submitted in partial fulfillment of the requirements for the degree
of Doctor of Philosophy in Information Science and Technology in
the School of Information Studies of Syracuse University

May 2013

Acknowledgements

I thank my wife Yvonne, and our children Emily, Connor and Austin for their tremendous support and for graciously sharing their time to allow me to achieve my goals. I also recognize my parents Guy and Karol Treglia who were instrumental in encouraging me to always pursue my dreams.

I thank my advisors and committee members for their participation and guidance; Dr. Lee McKnight, Dr. Joon Park and Dr. Steve Sawyer, Dr. Carlos Enrique Caicedo Bastidas, Dr. Michelle Kaarst-Brown, Dr. Anthony Cresswell, Dr. Murali Venkatesh, Dr. Kevin Crowston, and Professor Pat Longstaff.

I also appreciate and thank my family and friends not specifically named here but who were also supportive of and important to me throughout.

Support for this dissertation has been provided through the National Science Foundation (NSF) Public Safety Networks Study (PSN) (projects #IIS-0534877 & #IIS-0534889) and NSF Partnership for Innovation (PFI) grant for the Wireless Grid Innovation Testbed (WiGiT) (projects #0227879 & #0917973), the Jeffrey Katzer Memorial Dissertation Support Grant, and the James O. Marshall Farms Foundation.

Table of Contents

List of Illustrative Materials

Figures

List of Illustrative Materials

Tables

I. CHAPTER - INTRODUCTION

THREE ESSAYS ON LAW ENFORCEMENT AND EMERGENCY RESPONSE INFORMATION SHARING AND COLLABORATION:
AN INSIDER PERSPECTIVE

1. Introduction and Cohesion of Works

This dissertation of three essays examines factors related to information sharing and collaboration in the law enforcement and emergency response community, which may be referred to collectively as public safety. A contribution in this area comes in the form of describing and framing the broader issues, environment, and influences that operate across the law enforcement and emergency response community. A framework for examination and study of information sharing is proposed in the first essay and utilized to organize the overarching problem, and as a means for investigating and proposing solutions to the other problems identified. The second essay introduces a new technology for collaborating across communication and electronics devices and investigates current technical, social, and policy factors related to information sharing in emergency response. A case study in the area of multi-jurisdictional interagency collaboration and cooperation in the public safety area involving the emergence and activities of an emergency communications (E-911) radio consortium is included. This case is significant in that it is representative of the situation of many other law enforcement and emergency services providers across the United States, and lessons learned from this case will apply to other similar environments regarding information sharing and collaboration.

The included essays have a common theme surrounding information sharing and collaboration in organizations with a current focus being on the law enforcement and emergency response community (public safety). A multi-method, primarily qualitative, approach is taken throughout. A model for information sharing is presented that identifies social, technical, and policy factors as influencers. Facets of General Systems Theory and Socio-technical Theory are considered in this context. The three essays included in this dissertation are:

1) "A Framework for Conceptualizing Barriers to Intelligence Information Sharing in Law Enforcement: An Insider Perspective"
2) "Towards More Rapid and Effective Communication Between Responders to Emergency Situations"
3) "Identifying Factors that Support Collaboration in a Multi-jurisdiction Environment: A Case Study of the Central New York Interoperable Communications Consortium"

In this dissertation of three essays, each individual essay makes a contribution to the field of information science and together they collectively add to the knowledge in this area. The three essays described are included in the following chapters. At the end is a conclusion chapter that discusses the broader context, reflections and implications of the research, and proposes a direction and focus for future work.

2. Law Enforcement and Emergency Response Context

Public safety agencies in the United States, as used in this dissertation, include law enforcement and emergency response entities at the federal, tribal, state, and local levels to include special districts or functions. Emergency response entities include fire departments, ambulance, rescue services, and dispatch centers. Law enforcement agencies are considered emergency responders as well. Law enforcement agencies are responsible for upholding the laws of their jurisdictions and protecting people and property. They are information repositories, a source for documentation of incidents and events generally. Fire departments and rescue services are responsible for responding to fires, accidents, and other threats or incidents that may endanger life or property. Ambulance services are responsible for stabilizing injured or ill persons and transporting them to treatment facilities. Dispatch centers, which include 911 centers, are responsible for communicating with emergency response agencies and the public during critical incidents. This includes anyone that is involved in a crisis event or incident. Dispatch centers typically are the intersection of most all of the public safety agencies and stakeholders. Dispatch centers coordinate with, but do not control, the individual actions of the emergency responders.

Public safety agencies have varying roles and responsibilities in regard to crisis incidents or criminal activity. When police, fire, EMS (Emergency Medical Services) and other municipal entities respond to crisis incidents that involve danger to life and property their interests and responsibilities converge. Public safety agencies have a history of separately gathering data and information relevant to their roles and purpose and have not, to date, combined or integrated this information resource in a way that can be universally shared and used for improving public safety.

Although they share a common purpose of preservation of life and property, public safety agencies are autonomous, responsible to their local needs and interests, and there are many of them. There are 17,876 state and local law enforcement agencies operating in the U.S.: 12,766 local police departments, 3,067 sheriffs' offices, 49 state agencies, 1,481 special jurisdiction agencies, and 513 other agencies (BJS, 2007). Additionally, there are 26,464 fire departments registered with the US National Fire Administration as of February 9, 2011, with 23,120 of them volunteer or mostly volunteer agencies (USFA, 2011). In addition to those, there are an estimated 6,121 public safety answering points (PSAP), or communications centers that handle 911 or emergency calls. There are 225 counties that have no 911 service (Dispatch, 2012). There are multiple layers of governance with overlapping jurisdictions, responsibility, and authority. These include village, town, city, county, tribal nation, and other special jurisdiction agencies such as the park police that further overlap with jurisdiction and authority (see Figure 5, p. 82). The United States is fairly unique with this structure. Each public safety agency has its own rules, policy, regulations, and cultural norms. The village, town, city, county, state, tribal, federal, and special jurisdiction agencies each have their own leadership, policies, procedures, and resources. Governance, coordination, and information sharing in this multi-interest and dynamic environment are difficult to say the least.

Public safety agencies are responsible for defined geographical jurisdictions or areas where they have responsibility and control. The jurisdictions do not always follow municipal boundaries and many share or overlap in their jurisdiction. This is discussed in detail in later sections of this dissertation. For a given crisis incident, there may be multiple law enforcement agencies at different levels of government, multiple fire and rescue departments, several ambulance services, and more than one communications dispatch or 911 center involved in addition to other government and non-government stakeholders. Additional stakeholders are discussed in the second essay of this dissertation.

Historically, public safety agencies in many cases were formed and operated independently of each other. The law enforcement agencies dispatched themselves and created and maintained their own databases of information. Fire, rescue, and ambulance services did the same. Dispatch centers, communications centers, or 911 centers as they are commonly known, were formed as neutral entities or affiliated with law enforcement, fire or ambulance service providers. This independence created gaps in information collection and dissemination. Some example descriptions are provided below to aid in understanding this environment and the attendant conditions and issues created.

In some states, the fire departments are responsible for investigating the cause and origin of fires and may conduct criminal investigations separate from, or in parallel with, law enforcement agencies. Determination as to which agency is responsible for follow up is typically linked to whether or not the fire or explosion is believed to be accidental or done with criminal liability. Law enforcement and fire departments in these cases overlap in their responsibilities and record keeping.

Dispatch centers or 911 centers do not generally have control or authority over the agencies with which they communicate. 911 centers relay information that comes to them and provide information as requested. This does vary across the country. An example of how a dispatch center may have control over responders would be the case of a Metropolitan police department that operates its own 911 center. In that case, the dispatch center may have personnel with command authority over its responding department members. 911 centers are not generally in command during a crisis, even though they may be the ones with the most information and clearest view of the overall incident. Other public safety agencies control their individual forces through the 911 centers or directly through other means of communication. This creates an environment where it is difficult to capture and retrieve all relevant information in a crisis or incident.

Information comes from many sources to public safety agencies. People or agencies may call in complaints or provide information on crimes or incidents to the 911 centers, law enforcement agency, fire, or ambulance service. This data does not automatically get combined, related, or shared across agencies. One would think that the communications centers would act as a natural bridge for information across agencies. As not all calls for service or complaints go to a 911 center, one cannot rely on that agency for an account of all complaints or requests for service in an area. Police gather a great deal of information on people, locations, incidents, and events when they respond to calls for service, or in the course of investigating offenses. Ambulance and fire crews respond to incidents and gather information on people, locations, and incidents as well. Law enforcement agencies do not always respond with fire and ambulance agencies on their calls for service. This potential information is missed.

Each of the public safety agencies has different purposes for gathering information. Although it may be useful for the police to know where a particular person lives or who their associates are, the fact that the ambulance responded to the person’s residence does not mean that this type of information will be captured or even that it would be sharable with another agency due to privacy or other issues. In another example, the fire department may be called to a gas leak and then find evidence of a crime such as an illegal chemical laboratory. There are several possibilities in this example. The responders here may not recognize the information as significant for reporting to the law enforcement agencies and not capture or share it. The firemen may be intimidated or threatened by the participants to not disclose. Firemen may feel bad for the parties involved and not wish to get them into trouble. The firemen may even report the information to the proper authorities. There is a disconnect between police, fire, and other emergency responders in the information that could be shared.

Public safety agencies do not always work well together. There is an insider versus outsider atmosphere in many agencies. By way of example, an agency at the federal law enforcement level may not work well with a particular local-level agency. Law enforcement agencies may view non-agency personnel as outsiders and withhold information or simply choose not to interact. Law enforcement agencies, especially, are responsible for policing others and have sensitive and secret information, operations, and methods that cannot be shared, even with other government agencies. Other public safety agencies have sensitive and private information that must be protected as well. This issue will be discussed in greater detail in the sections following.

It is important to understand the law enforcement and emergency response environment in considering the factors examined in this dissertation.

3. Problem

> *"To prevent acts of terrorism on American soil, we must enlist all of our intelligence, law enforcement, and homeland security capabilities. ... We are improving information sharing and cooperation by linking networks to facilitate federal, state, and local capabilities to seamlessly exchange messages and information, conduct searches, and collaborate." — President Obama's National Security Strategy, May 2010.*

According to the National Security Agency (NSA), barriers continue to impede information sharing, particularly between state and local agencies (United States, 2007, 2007c). The National Intelligence report concluded that the United States is currently facing persistent and evolving terrorist threats (Lieberman, 2007). Crimes continue to proliferate across jurisdictions, and cyber investigations may be the largest challenge to modern law enforcement (Lee, 2008). The government Information Sharing Environment (ISE) report states, "the biggest impediment to all-source analysis—to a greater likelihood of connecting the dots—is the human or systemic resistance to sharing information" (McMamara, 2006).

Despite mandates to improve information sharing in the law enforcement and emergency response communities, gaps still remain perhaps because there is not a clear understanding of what the barriers to information sharing are that can be acted upon or changed by agencies and policy makers. Law enforcement and emergency response agencies in the United States are not yet effectively sharing information. This conclusion is reflected in a report to congress (Kshemendra, 2010).

Law enforcement and Emergency management are complex environments where surprises occur. According to Longstaff, 2003, “systems are said to become ‘complex’ when they have intricate interdependencies among their various parts and many variables operating at the same time.” Taking action in one area can cause unpredictable effects on other areas due to the interrelatedness of the components (Longstaff, 2009).

Research into understanding the dynamics will lead to identification of actionable barriers to law enforcement and emergency response information sharing and collaboration across the federal, tribal, state, and local levels, and ultimately lead to the creation of strategies to address the problem. By identifying a conceptual framework for understanding factors of information sharing in this environment, researchers may provide focus for discussion and research in this area. Much work has been done addressing technological aspects of the information-sharing problem (Akbulut, Kelle, Pawlowski, Schneider, & Looney, 2009; Akbulut, 2003; Gil-Garcia, Chengalur-Smith, & Duchessi, 2007; IT.OJP, 2010; Jacobs & Blitsa, 2008; USDOJ, 2004; 2006) and so there is a need to move beyond the technological aspects of the problem. The issue of sharing involves factors including trust, governance, and participation for members and stakeholders. Trust and governance have significant meanings and contexts in this dissertation and in the three included essays; they are explained in detail in the sections following.

Alternative approaches in these and other areas may be considered to improve information sharing behaviors among involved agencies and potentially extend the degree and quality of information sharing across the law enforcement and emergency response communities. Creating a shared conceptual framework, looking beyond the technological factors, and seeking out alternative and creative means for engaging and retaining participants in the information sharing processes, is necessary and an objective of this research.

Information sharing in this context involves the transfer of information obtained that relates to an actual or impending occurrence of any incident, criminal, or terrorist act. This conceptualization includes the range of information that can be considered data related to events, activity, or resources to information that can be used for strategic decision making or new knowledge generation. Intelligence information, as used in this thesis, is a special set of information related to sensitive issues, resources, or other information related to decision-making.

Knowledge of people and other resources that are involved in crisis or natural disaster response is also information that must be shared. Included as intelligence information are suspicious activity reports regarding incidents or observations, which are of a less obvious nature but which may be supportive of, or related to, criminal or terrorist related activity. The term knowledge may also be substituted here as a way to bridge across disciplines from outside the intelligence community (Forrest, 2006; Kulkarni, Ravindran, & Freeze, 2007).[1] An incident of suspicious nature could be considered suspicious activity (intelligence information) or information, depending upon the circumstances. The determination as to whether an event is considered and captured as “suspicious activity” or “intelligence information” is subjective and often left to the discretion of the observer of the condition involved.

One aspect of the problem of agencies sharing information and collaborating – within the United States – may come from the structure of the political system, agency jurisdictions, and agency responsibility. Law enforcement in the United States remains uniquely decentralized and does not operate under unitary command or control. Recent case studies on knowledge sharing within public sector inter-organizational networks confirm information-sharing difficulties across agencies (Jing & Pengzhu, 2007; Pardo, Cresswell, Thompson, & Zhang, 2006). Agencies overlap jurisdictions and responsibility, each with a duty to their own constituencies. There has been a top-down approach to implementation of information-sharing mandates, typically from the federal level down. The case study included in this dissertation provides support for the notion of a need for both top-level guidance and control, such as in the establishment of broad standards for interoperability as well as providing a degree of autonomy for involved entities at various levels. The case provides evidence of the importance of acknowledging the individual sovereignty of agencies at various levels in cooperative engagements. There are successful alternative governance and collaboration arrangement models that may improve the success, participation, and, ultimately, the sharing of information in mixed-interest environments

[1] Knowledge is defined in the 2011 Merriam-Webster Dictionary as "the fact or condition of knowing something with familiarity gained through experience or association."

(Brafman & Beckstrom, 2006). Brafman and Beckstrom, in their book on leaderless organizations, point to examples such as the Apache Indians as a group that endured under hardship in a distributed fashion through a governance structure that was based on shared purpose and norms that were not tied to a central leader or hierarchy. Tribes are described working together for a common purpose without formal control mechanisms or power over each other. This is a situation similar to that of emergency responders and law enforcement agencies in the United States where there is considerable overlap in jurisdiction, distributed ownership, and control over resources, and a lack of unitary command and control.

Identified below are some of the problems, as identified from the literature and observations in the field, which need to be addressed to improve information sharing and collaboration in the law enforcement and emergency response communities in the United States (Fedorowicz, Markus, Sawyer, Tyworth, &Williams, 2006; Pardo, Gil-Garcia, Burke, 2008; Treglia & Park, 2009:

- Agencies do not have sufficient trust established between them to share information.
- Some information is time-sensitive and this affects the potential for sharing of the information in these situations.
- Technical factors such as incompatibility, lack of standards, and system reliability must be overcome across the law enforcement community.
- Policy is not consistent and, in some cases, may not have kept pace with technology or society and may conflict with sharing interests.

Personnel factors involving social and security concerns may interfere with the information sharing processes in organizations.

4. Research Question

Information sharing in law enforcement and emergency response consists of much more than gathering intelligence on terrorism-related issues. The sharing involved here encompasses sharing information across multiple levels of agencies to enhance the national security of the United States and the safety of the American people more broadly. What may be done to overcome barriers that hinder information sharing among federal, tribal, state, and local law enforcement and emergency response agencies? Could focusing on the problem through a common conceptual framework provide insights that help advance both theory and practice? If current technological barriers to information sharing are removed, what issues remain or emerge? Are there lessons to be learned from successful public safety collaborations that could be applicable to others?

This dissertation suggests possible strategies that may be undertaken to improve appropriate information sharing and collaboration across the law enforcement and emergency response community. The identified propositions here are empirically investigated utilizing multiple research methodologies focusing on a combination of factors, internal and external to the systems studied (law enforcement and emergency response agencies).[2]

[2] "Internal" as used in this context has multiple implications which include, as cited from the Encarta North American Dictionary, 2011: "1.Self-contained or self-generating, existing, evident in, or arising from the nature, structure, or qualities that somebody or something has; 2. Mental, involving or existing within the mind or spirit; 3. Occurring within an organization, working at or carried out within an organization or institution." This conceptualization and understanding captures the broad social and other non-technical aspects that are the focus of this work.

This dissertation examines factors related to information sharing in the law enforcement and emergency response community from an insider perspective. In this case, the researcher is a member of the public safety community and has access to personnel, information, and material that is not available otherwise. Information presented here has been vetted by this researcher and some of the participants in the case study for appropriateness to public dissemination.

The contribution in this area comes in the form of describing and framing the broader issues and describing the environment and influences that operate across the law enforcement community to include emergency services. The overarching question that this work will resolve involves achieving a greater understanding of the workings and dynamics currently involved in the information sharing and collaboration processes, with implications in both the business and government sectors.

This dissertation asserts that information sharing is affected by factors involving social, technical, and policy influencers. The research considers what may be done to overcome internal and external barriers that hinder information sharing among federal, tribal, state, and local law enforcement agencies. The dissertation as a whole addresses the following propositions:

(P1) *Information sharing is affected by social, technical, and policy factors and this conceptualization frames the problem of information sharing in a way that it can be commonly understood by government and non-government stakeholders.*

Intelligence information sharing is the subject and focus of the first work of this dissertation: a theoretical piece identifying a conceptual framework for understanding intelligence information sharing and explaining its structure and use (see Figure 2). An application of the framework is tested using data from a national survey of law enforcement agencies.

The next proposition involves the role of technology in information sharing;

(P2) *Social and policy factors influence information sharing more than technical factors (assuming it is physically possible to connect and/or share).*

Social and policy factors are investigated in the second essay. Here, implications of new solutions to technical barriers to information sharing are considered. By having issues surrounding connectivity and secure access accounted for the focus becomes more on the social and policy factors that impact information sharing systems. This work extends the present understanding of technical, social, and policy factors surrounding information sharing.

A final proposition addressed is that:

(P3) S*ocial factors play the greatest role in the creation and sustaining of information sharing relationships.*

Social factors in public safety information sharing, and their impact on the effectiveness of information sharing systems and practices, are examined through a case study of the Central New York Interoperable Communications Consortium (CNYICC) Network. The CNYICC is a five-county collaboration involving law enforcement, public safety, government, and non-government participants.

These identified propositions are empirically investigated using multiple methodologies including case study, interviewing, and policy analysis. The results to date are reported in this dissertation. The comic shown below depicts one of the assumptions in this research: that there are internal human interests and considerations involved in the process of information sharing that must be understood and addressed. The adage "after you" is a polite expression of human cooperation. This has another side that speaks to the underlying lack of trust in transactions and the belief that there are untold motives that shadow, through informal networks, and influence human interactions. These motives can make it less likely that any one party will be a first mover in a cooperative arrangement.

The findings here will provide a greater understanding of the forces that impact the agencies under study as they consider information sharing, contribute to the academic and professional literature on information sharing and collaboration and will, it is hoped, lead to identifiable strategies to solve the problems from a new perspective.

"I'll show you mine if you show me yours"

Figure 1: Illustrative Cartoon

5. Framework

A multi-method approach was used in this study to identify major problem areas and factors that affect information sharing between law enforcement agencies. The process for this research involved literature review, field observation, and use of soft systems methodology. The methodology and rationale is described further in the methods section. The factor categories identified were chosen following a review the literature and through comments from contacts in the public safety field. Aspects of systems theory contributed to the created factor categories. Sub-categories included here were prominent in both the literature and mentioned frequently by practitioners. The sub-categories presented are not meant to exclusively represent all sub-categories that may be included under a specific factor category. The sub-categories within each major factor category help identify the concepts and types of activity that may be considered within each.

The problems and issues were identified and ultimately grouped into specified areas or factors: Technical, Social, and Policy. The factors influence information sharing individually and collectively. The factors both affect and are affected by each other. This framework is consistent with elements of Socio-Technical Systems (STS) and General Systems Theory (GST), as described below and in the sections following. Important elements include such concepts as the interdependence of the relationships between and across entities. An organizational system described from this perspective is comprised of interrelated interacting parts and relationships that cannot be correctly described without considering their relationship to the whole or larger environment that they operate in (Von Bertalanffy, 1972).

Systems models from the business and management fields also shaped the selection and formation of the three factor categories. Information systems in business and organizational studies typically identify information systems as being comprised of people, procedures, data, software, telecommunications, databases, and hardware that are utilized in combination to support a business purpose (Stair & Reynolds, 2011; O'Brien & Marakas, 2008). Additional sources from Operations management and information systems similarly identify these, or related categories, for system components such as plants, equipment, control procedures and policies (Lewis & Slack, 2003; Gupta, 2000).

The various schemas for categorizing components were considered in consultation with fellow researchers and practitioners and ultimately the three factors of Social, Technical, and Policy were determined to be inclusive of all system components and descriptive enough to provide for a more complete understanding and examination of information sharing systems and processes in the public safety realm. The rationale and descriptions of these are provided in further detail with cognitive maps depicting the concepts and interrelationships in the sections following.

Systems models from the business and management fields also shaped the selection and formation of the three factor categories. Information systems in business and organizational studies typically identify information systems as being comprised of people, procedures, data, software, telecommunications, databases, and hardware that are utilized in combination to support a business purpose (Stair & Reynolds, 2011; O'Brien & Marakas, 2008). Additional sources from Operations management and information systems similarly identify these or related categories for system components such as plants, equipment, control procedures, and policies (Lewis & Slack, 2003; Gupta, 2000). The various schemas for categorizing components were

considered in consultation with fellow researchers and practitioners and ultimately the three factors of Social, Technical, and Policy were determined to be inclusive of all system components and descriptive enough to provide for understanding and examination of information sharing systems and processes in the public safety realm.

Other researchers separately proposed structures for considering the factors in public sector information sharing. Research by Dawes (1996) and Zhang et al. (2005) identify three primary influential factors as technology, management and policy. These are similar to the framework created in this dissertation; technical, social, and policy. Yang and Maxwell (2011) created a model consisting of three identified perspectives (Technological, Organizational and Managerial, and Political and Policy) that influence public sector information sharing. Additional perspectives and factors influencing inter-organizational information sharing in the public sector are shown in Figure 9.

This section provides a detailed identification of the problems that exist in the area of information sharing in law enforcement and the proposed means for addressing these factors through a coordinated plan of research. The conceptual framework is shown in Figure 2 below.

The developed framework for information sharing illustrates the identified problem areas, or conceptual areas, for research focus. The final framework that was produced includes technical, social, and policy factor categories.

These three identifiable factor categories were identified as each having a role in influencing whether or not information is ultimately shared. Technical factors include interoperability issues, responsiveness, and control. Social factors involve trust, informal networks, culture, and importance. Policy factors involve concerns over what can be shared and under what governance model or structure are activities allowed or restricted and include legal/policy considerations. Each area operates in its own sphere and the three spheres independently and collectively impact information sharing. Their relationship and impact on information sharing is being depicted here, and not all of the interrelationships across the identified factors.

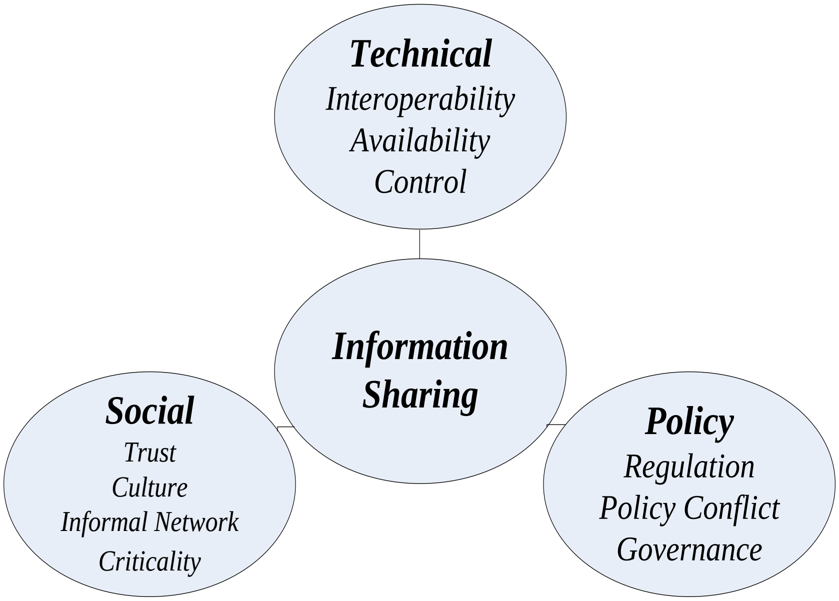


Figure 2: Information Sharing Problem Areas and Research Map

(Treglia & Park, 2009)

Social factors impact and are influenced by technical capability and constraints and policy, social factors, and technology each shape are shaped by one another. A more comprehensive, expanded, version of this framework would depict those influences as well, having bi-directional connections between and across all three factors. A goal here was to create a simple framework that would organize the issues and problems in a way that creates a common ground for discussion and research in this area.

II. CHAPTER - LITERATURE REVIEW

1. Introduction

This chapter will provide an overview of relevant theoretical and empirical literature and research pertinent to the studies in this dissertation. The focus here is on selected theories and topic areas that pertain to aspects of information sharing and collaboration in public safety and to the three essays that are included in this dissertation. This chapter consists of eight major sections: introduction, definitions, research on information sharing, selected theories and concepts, social factors, technical factors, policy factors and a summary of the literature review.

2. Definitions

2.1 Information

Information as used in this dissertation refers to any data, observation or activity, that may be captured and shared for a public, business, or individual purpose. Information is defined here in three parts. The United States Department of Defense defines information as:

1. Any communication or representation of knowledge such as facts, data, or opinion in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.
2. Facts, data, or instructions in any medium or form.

3. The meaning that a human assigns to data by means of the known conventions used in their representation. (U.S. DOD, 2007, p.24)

Information is related in this conceptualization to evidence. Evidence, in the law enforcement community and as taken from the Harvard Law Review, includes “all the means by which any alleged matter of fact, the truth of which is submitted to investigation, is established or disproved” (Thayer, 1889, p142). This is a definition that has been effective to the present day. The definition is meant to be broad and all encompassing.

2.2 Intelligence Information

Intelligence information is defined as any gathered facts or data that relate to an actual or impending occurrence of any incident, criminal or non-criminal. Information such as suspicious activity reports or observations of a less-obvious nature but which may be related to criminal or other activity, and which may be cause for concern are included in this definition. Intelligence information also includes knowledge about resources that an agency or community may have that may be important to crisis responders or criminal investigators. These could be physical, such as the location of alternate fuel resources for emergencies, or non-physical, such as the contact information for important human services providers. This may include what is considered sensitive information by Thompson and Kaarst-Brown (2005). Knowledge and intelligence cross disciplines such as those from outside the intelligence community (Kulkanni, Ravindran, & Freeze, 2007). An incident of suspicious nature could be considered “suspicious activity” or “information” depending upon the circumstances. Deciding whether something is considered and captured as “intelligence information” is subjective. It is up to the discretion of the officer or person involved.

2.3 Collaboration

Collaboration, as used in this dissertation, involves an interaction where two or more parties work together towards a common purpose. Parallel work without an intentional or knowing connection is not considered collaborative work. Individuals and entities may collaborate with each other and across levels. This is consistent with the Miriam-Webster dictionary definition for the term: “1) to work jointly with others or together especially in an intellectual endeavor; 2) to cooperate with or willingly assist an enemy of one’s country and especially an occupying force; 3) to cooperate with an agency or instrumentality with which one is not immediately connected” (Merriam-Webster, 2012). In this dissertation, collaboration is argued to be an element affiliated with cooperation and information sharing.

Collaboration in business has been well studied in the literature (Axelrod & Hamilton, 1981; Mattessich, Murray-Close, & Monsey, 2001). As used in this dissertation collaboration and cooperation have similar meaning and application. Axelrod posits regarding cooperation that reciprocity in interactions between persons creates positive relationships over time that is durable when fully established (1981). The term “Tit for tat” is used in describing this reciprocal interactive relationship that is observed to occur between persons in cooperative activity. Positive cooperation evolving in such an environment would be subject to change where one party defects or acts out of self-interest or taking an advantage, therefore breaking established trust and commitment. These relationships can be repaired (Rocco, 1998). The establishment of behavioral norms among those working together can act as a control measure even where no central authority or structure is in place (Axelrod & Keohane, 1985; Axelrod, 1986; Brafman & Beckstrom, 2006).

Collaboration has been described as a process where “autonomous or semi-autonomous actors interact through formal and informal negotiation, jointly creating rules and structures governing their relationships and ways to act or decide on the issues that brought them together; it is a process involving shared norms and mutually beneficial interactions (Thomson, Perry, & Miller, 2011). This conceptualization of collaboration is one of the few in the literature created through consideration of nine separate studies. It describes collaboration as a multidimensional and variable construct comprised of five dimensions: governance and administration, which are structural in nature, mutuality and norms, which involve social capital dimensions, and organizational autonomy, which involves agency.

Collaboration success can be difficult to quantify or describe. Several studies and approaches have been taken to measure and describe collaboration outcomes and activity (Westphal, Thoben, & Seifert, 2008). Kothari, MacLean, Edwards and Hobbs (2011) note that traditional mechanisms and indicators for measurement of cooperation are not well established. Thomson, Perry and Miller developed a multidimensional model of collaboration using data from a survey of national service program participants (2009). From that study five key dimensions are described that form an overall construct of collaboration. Collaborating with partners is an essential competency for business entities. This is no different in the public safety realm. Kuenzel and Welscher report that there are eight factors important to “Public Safety Collaboration Success” (2009). The eight success factors are explained below and serve as an essential frame-work for analyzing and regulating collaboration processes:

1. Relevance and Sense of Urgency: The need to collaborate can emerge from political strategy; improvement in services; civil society and media exerting pressure on the public sector to change the policies.

2. Incentives and Benefits: The reciprocal benefit from partnership can arise from the interest of each member.
3. People & Roles: The success in collaboration depends directly on establishing a social system wherein the individuals must have interpersonal relationship and a mindset for collaboration.
4. Organizational Structure: It is because of the organizational structure that collaboration from the individuals, having political and social relationships, is mostly sought.
5. Reflection & Learning: It is the changing environment which makes the collaboration process to take place. Collaboration thus demands that all the partners must have a great deal of reflection and knowledge.
6. Skills and Capabilities: A variety of skills are needed for the collaboration to be feasible. These skills pertain management, strategic aptitude, negotiating and communicating capabilities.
7. Resources: The more the resources the more the collaboration. The scope and duration of collaboration determines the amount of resources required.
8. Outside Support & Supervision: when collaboration has admittance to external support it can easily achieve its targeted goals.

The authors suggest that the eight identified success factors (above) must be made part of the design and operation of a collaboration to have the highest probability of achieving its desired public safety objectives (Kuenzel & Welscher, 2009).

Current thinking in the area of cooperation, and it is argued here collaboration, involves extending the basis of cooperation from being focused on longer term relationships and gain than the short term or individual gain focus (Axelrod, 1997). Participants in public safety agencies must cooperate under varied conditions that involve discontinuities of information regarding the other parties they interact with and their degree of control. They may work together for a single incident or have ongoing relationships where they must share information and cooperate in an ongoing basis.

This dissertation proposes to expand the conception of collaboration to involve governments, non-governmental organizations, communities, and individuals in response to crisis incidents. The current conception of resilience[3] includes "inclusive strategies that integrate both resistance (prevent, protect) and resilience (respond, recover) in the face of disasters" (Longstaff, Armstrong, Perrin, Parker, & Hidek, 2010). This is consistent with the notion of involving the "whole community" in preparation and response activities.

2.4 Formalization

Formalization refers to the extent to which tasks or obligations are structured within an organization or entity, and the degree to which these activities are governed by identifiable rules and procedures. Other, early, definitions of the concept of formalization include " … statements of procedures, rules, roles, and operation of procedures which deal with (a) decision seeking (applications for capital, employment, and so on), (b) conveying of decisions and instructions (plans, minutes, requisitions and so on), and (c) conveying of information, including feedback" (Hall, Johnson, & Haas, 1967; Pugh, Hickson, Hinings, Macdonald, Turner, & Lupton, 1963). Measurement of organizational formalization has been operationalized as "… the proportion of codified jobs and the range of variation that is tolerated within the rules defining the jobs, the

[3] Resilience as used here is consistent with the definition used by the multi-disciplinary Resilience Alliance: "*the capacity of a system to absorb disturbance, undergo change, and retain the same essential functions, structure, identity, and feedbacks*" (Longstaff, et al., 2010, p. 3).

higher the proportion of codified jobs and the less the range of variation allowed, the more formalized the organization" (Aiken & Hage, 1966, p. 499; Hage, 1965, p. 295). Change processes become legitimized over time and become stabilized (Kaarst-Brown, 1999).

Sales (2010) suggest that formalization of policy has positive effects on the organization and can improve information sharing. Others see formal systems as potentially less effective in facilitating information sharing than informal ones (Hall & Tolbert, 2004; Kim & Lee, 2006; Willem & Buelens, 2007). It may be that having informal policy leads to increased openness and greater interaction and communication in an organization (Jarvenpaa & Staples, 2000; Kim & Lee, 2006). The case of the CNYICC demonstrates operation of a collaboration having less formal structures in its development stages. For longer term mature operation of collaborations the need for greater formalization may arise.

2.5 Information Sharing

In this dissertation, information sharing, intelligence information sharing and collaboration are discussed. Federal, state, and local enforcement and emergency response agencies have a number of ways to share intelligence and other information: electronically, through paper systems, and through formal and informal personal contacts so the goal of this research is to discern why this does not happen.

The term information sharing in public safety gained popularity as a result of the 9/11 Commission hearings and report of the United States government's lack of response to information that was known about planned terrorist attacks on the New York City World Trade Towers prior to the events. This led to the enactment of several executive orders by President

George W. Bush mandating agencies implement policies to "share information" across organizational boundaries (United States, 2007).

Information sharing can be defined as “making information available to participants (people, processes, or systems)” (USDOD, 2007). The leveraging of this information by parties involved is also included in this broad, simple, conceptualization. Information sharing, in the public sector, has been defined generally as “exchanging or otherwise giving other agencies access to information” (Zheng, 2009, p.27). Researchers clarify that information sharing refers to tacit knowledge as well as to explicit artifacts and codifiable information (Yang & Maxwell, 2011). In the fields of business and marketing, information sharing is defined as “the extent to which the supplier openly shares information about the future that may be useful to the customer relationship” (Cannon, & Homburg, 2001). This indicates a value potential for information, which is sometime paralleled in public safety where agencies share information that may help them solve a case or apply for a funding opportunity. Information sharing is also defined as the degree to which partners proactively provide critical and confidential information to each other (Phan, Styles, & Patterson, 2005). This means that information is provided without one side having to ask for it.

3. Research on Information Sharing

There is a great deal of research that has been done in the area of information sharing and law enforcement since 1990. Prior to the 9/11 tragedy there were fewer than 100 academic articles produced in this area, according to a search conducted through Harzing's Publish or Perish. Publications with "information sharing" and "law enforcement" were tracked from 1990 to 2011 using this same resource (Publish or Perish) resulting in figures showing a steady increase in these publications per year from 99 in 1990 to 1710 in 2009. There is a significant amount of time and resources being devoted to research in this broad area, as the Figure 3 below attest. Within this larger topic area, there are segments of targeted attention and interest, which attract less attention and there remains much work to be done.

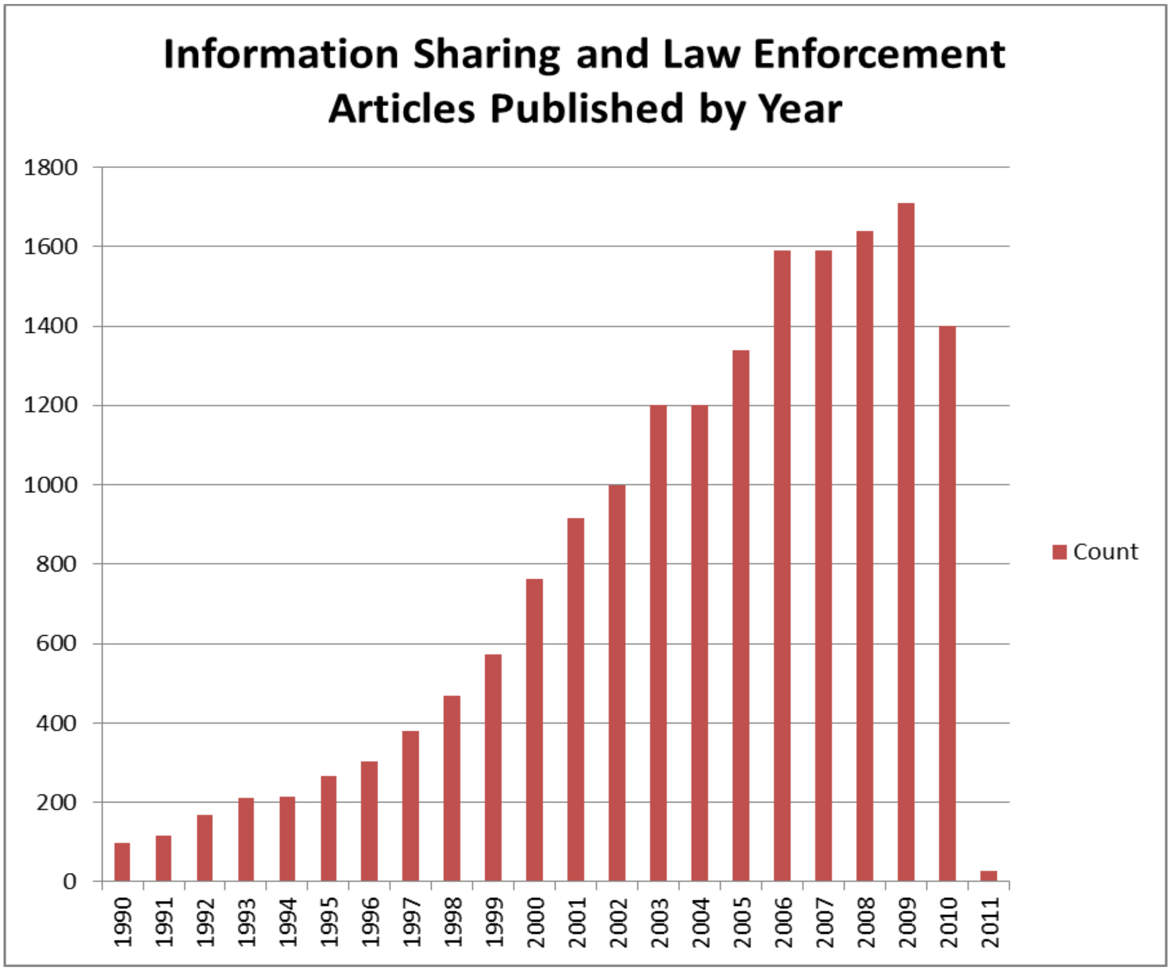


Figure 3: Information Sharing and Law Enforcement Articles

(Created using Harzing's Publish or Perish, January 15, 2011 - Treglia, 2011)

The study of Information Systems "deals with the deployment of information technology in organizations, institutions, and society at large" (Ciborra, 2002). Another definition claims that "information systems are also social systems whose behavior is heavily influenced by the goals, values and beliefs of individuals and groups, as well as the performance of the technology" (Angell & Smithson 1991, p.17).

Identified problems and recurrent themes related to information sharing are grouped here into distinct areas or factors; Technical, Social, and Policy. These factors influence information sharing both individually and collectively, and both affect and are affected by one another. The information-sharing framework described in this dissertation derived from a broad initial focus on information sharing in the law enforcement and public safety communities. This framework is consistent with elements of Socio-Technical Systems (STS) and General Systems Theory (GST), as described in the sections following. Important elements include such concepts as the interdependence of the relationships between and across entities.

Systems models from the business and management fields shaped the selection and formation of the factor categories. Information systems in business and organizational studies typically identify information systems as being comprised of people, procedures, data, software, telecommunications, databases, and hardware that are utilized in combination to support a business purpose (Stair & Reynolds, 2011; O’Brien & Marakas, 2008). Sources from Operations management and information systems identify related categories for system components as plants, equipment, control procedures, and policies (Lewis & Slack, 2003; Gupta, 2000). Various factor categories were considered in consultation with fellow researchers and practitioners and ultimately Social, Technical, and Policy factors were determined to be inclusive of all system components and descriptive enough to provide understanding and examination of information sharing systems and processes in public safety.

Interestingly other researchers have separately proposed similar structures for considering factors in public sector information sharing. Interagency information sharing research by Dawes (1996) and research on knowledge sharing in e-Government by Zhang et al. (2005) identify three primary influential factors as technology, management and policy. These are constructively similar to the framework created and presented in this research; technical, social, and policy. Yang and Maxwell (2011) have recently proposed that three identified perspectives (Technological, Organizational and Managerial, and Political and Policy) influence public sector information sharing and they created a model using those three perspectives (shown in Figure 8).

4. Selected Theories and Concepts

4.1 General Systems Theory

General Systems Theory (GST) is interdisciplinary and involves examining and understanding phenomenon as a system of interrelated components that contribute to overall outcomes (Ackoff, 1971). GST is alternatively referred to as Systems theory, Open systems theory, and as Systemic theory. Ludwig von Bertalanffy is credited with founding this theory (Von Bertalanffy, 1972). In GST, the emphasis is on the interaction of the identified elements of a system with their situated environment. Research is most typically done at the system level of analysis. GST is a holistic approach that recognizes action or influence as specific to a given environment where multiple forces interactively affect outcomes.

The systems approach is described by Churchman as “a set of parts coordinated to accomplish a set of goals” (Churchman, 1979). He identified five basic considerations for conceptualizing the meaning of a system:

1. The total system objectives, and more specifically, the performance measures of the whole system.
2. The system's environment; the fixed constraints;
3. The resources of the system;
4. The components of the system, their activities, goals, and measures of performance;
5. The management of the system. (Churchman, 1979, p. 29)

He also emphasizes that systems are always embedded within larger systems and that the entirety is encompassed within or situated in an identifiable environment. The environment is not under the control of the systems within it. Systems are also viewer and problem-dependent in the view of Churchman. Various observers may describe a system and each interprets it differently, possibly due to their individual purposes. This is not to say one is more correct than another (Alter, 1999).

In regards to systems, Kuhn identifies a common element as the relationship of any given part to the others. Kuhn notes that "knowing one part of a system enables to know something about another part" (Kuhn, 1974). He adds as well that, "the information content of a 'piece of information' is proportional to the amount of information that can be inferred from the information" (Walonick, 1993; Kuhn, 1974). It is anticipated that this interrelatedness will be found as well in the law enforcement and emergency response information sharing realms.

Systems are generally studied following cross-sectional or developmental approaches: looking at the interaction between two systems and looking at systems over a period of time (Walonick, 1993).

This dissertation involved comparing systems to known or other entities as well as looking at the operation of these systems in the law enforcement and emergency response arenas over time. Public safety agencies interact as a group with many interrelated parts and interdependent elements in response to crises. They have a shared or common purpose. They can act and be observed as a complex whole. Later in this dissertation this behavior is also described as stigmergic. Approaches for evaluating subsystems include using a holistic approach, looking at the entire system and relationships, which in this case involve social, technical and policy implications. The law enforcement and emergency response community is well entrenched with technology and that relationship is worthy of additional special attention.

4.2 Socio-technical Systems Theory

Socio-technical Systems Theory looks at systems in organizations as comprised of people using tools, processes and knowledge to create something of value or for a defined purpose (Bostrom & Heinen, 1977; Mumford, 2000; Trist, 1981). An important consideration in this theory is recognition that "every socio-technical system is embedded in an environment that affects the way it behaves" (Mumford, 2003). The emphasis is on understanding the two-way relationship that exists between the technology and users, recognizing that each impact or influence one another. This includes technology and society (Bijker, 1997). This is a critical distinction in STS.

Many authors are associated with writings in this area. Bostrom and Heinen (1977) wrote on Management Information Systems (MIS) problems and failures: A socio-technical perspective. Cherns provides principles of sociotechnical design in “The principles of sociotechnical design” in 1976 and updated this work in “Principles of Sociotechnical Design

Revisited," in 1987. Bijker (1997) describes his theory of sociotechnical change , including that technology and society are both human constructs, in 'Of Bicycles, Bakelites, and Bulbs: Toward a Theory of Sociotechnical Change (Inside Technology).

Other authorship includes Davenport (2008), Social informatics and sociotechnical research—a view from the UK; Lamb, Sawyer, & Kling (2000), A Social Informatics Perspective on Socio-Technical Networks; Emery (1997), The next thirty years: Concepts, methods and anticipations. Social informatics involves interdisciplinary study of the creation and use of information technology while taking into account its interaction with institutional and cultural contexts (Sawyer & Rosenbaum, 2000; Lamb, Sawyer, & Kling, 2000).

Additional early authors include Heller (1997), Socio-technology and the Environment; Leavitt (1965), Applied organization change in industry: Structural, technical, and human approaches; new perspectives in organizational research; Mumford and Hawgood (1980), Training the Systems Analyst of the 1980's: Four New Design Tools to Assist the Design Process; Trist & Murray (1993), The Social Engagement of Social Science: A Tavistock Anthology (vol. II). This is not comprehensive, but does identify some associated authors and works in the area of socio-technical systems and related perspectives such as social informatics.

Under the heading of socio-technical theory task, technology, structure, and people are critical components of a work or information sharing and communications system. Bostrom and Heinen identified this as a matrix of interaction with the people and work or organizational structures as the social system interacting with each other and with the Technical system, including the technology and tasks as shown in Figure 4 below (Bostrom & Heinen, 1977).

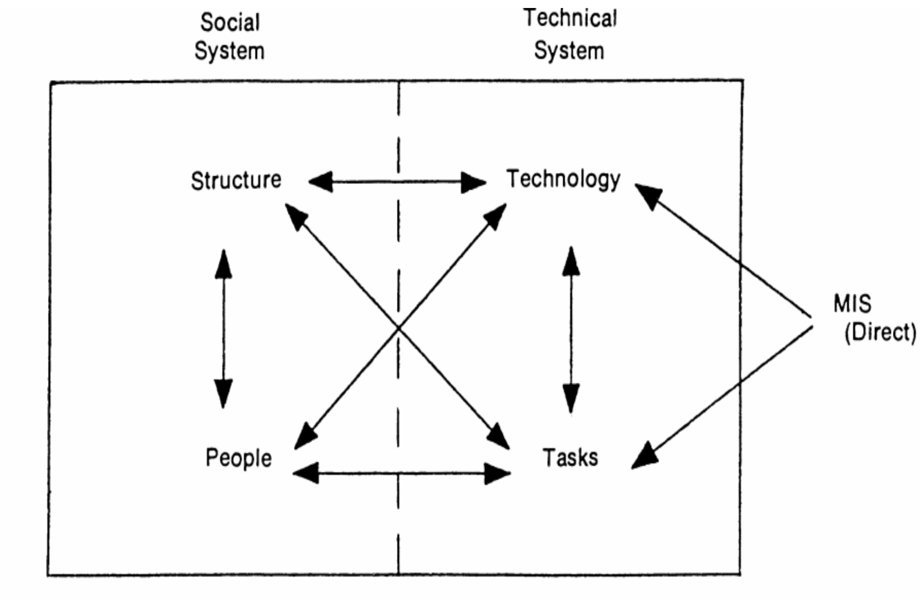


Figure 4: The Interacting Variable Classes within a Work System

(Bostrom & Heinen, 1977)

This early conceptualization is relevant today although, in the time of its origin, they may not have conceived of the vast technological linkages and capacity of today. Still, the interplay of people, technology and process were becoming evident then and there is, perhaps, a more common understanding of this now.

Dawes investigates governance in the digital age and includes in this work consideration of socio-technical principals in the e-government sector (Dawes, 2008). Dawes proposes that borders will be less defined and that "technological aspects become embedded in a more organic notion of governance" improving service delivery through a "more holistic understanding and better informed policies and decisions" (Dawes, 2008).

What is notable here is the specific identification by Uzzi (1997, 2007) that critical transactions depend on social connections and relationships. Social aspects of information sharing are an important part of the conceptual framework referred to in Part IV this dissertation

(Treglia & Park, 2009). This is but one study that acknowledges this element in the context of information sharing. Technology alignment with the organizations structures and individual roles has been examined (Barley, 1990). Collective capability for information sharing was studied by Orlikowski (2002). More recently socio-material practices in the workplace were investigated by Orlikowski in 2007. As previously identified, the social impacts on actual practice and use of information and communication technologies is important in this investigation. This is consistent with the socio-technical notion of both technology and humans simultaneously exerting agency over the system (Rose & Jones, 2005). Researchers must look not only at the processes and structures in law enforcement and emergency response, but include the technology and individual's reaction to or changes based on it.

In the law enforcement and emergency response area, one can expect to gain a richer understanding of information sharing issues by looking at the environment through this perspective and GST.

4.3 Stakeholder Theory

Stakeholder theory is a paradigm for understanding the operation of business, or organization, as it relates to various stakeholder interests. This was initially proposed by R. Edward Freeman in Strategic Management: A Stakeholder Approach (1984) (Freeman, Harrison, Wicks, Parmar, & De Colle, 2010). Stakeholder theory has a managerial focus looking at how one understands what goes into decisions, and thereafter actions, by people in organizations. Stakeholders are an expanded group that includes owners, employees, investors, customers, suppliers, communities and others (Hosseini & Brenner, 2009). The inclusion and participation of stakeholders and stakeholder groups in solving system-wide problems has been recognized and important and proposed in the literature (Freeman, 1984 & 2010). The self-interests and motivation of the participants and stakeholders in an organization, or a system as argued here, impact the operation of the organization but are not well predicted. The organization seeks to fill the needs of the stakeholders. Looking at “the relationship between a business and the groups and individuals who can affect or are affected by it” is an approach of Stakeholder theory (Freeman, Harrison, Wicks, Parmar, & Colle, 2010, p.4). Individual interests may not always align with overall organizational goals. A broadened view encompasses the notion of humans, institutions and organizations as stakeholders in humanity, the natural environment being a stakeholder as well (Waddock, 2011).

The Integrated Non-Filer Compliance System used by the State of California Franchise Tax Board was used to study barriers to inter-organizational information sharing. In that study researchers drew upon stakeholder theory (Fedorowicz, Gogan, & Culnan, 2010). They proposed a four stakeholder group typology including: data controllers, data subjects, data providers, and secondary stakeholders that they used to mitigate participant concerns about privacy. Authors posit that privacy concerns act as a barrier to information sharing and that by improving the perception of the systems fairness greater adoption will be achieved. Accounting for stakeholder concerns over things such as perceived fairness was identified as impacting system success (Fedorowicz et al., 2010).

Other studies examine government agencies and public safety agencies as points of interest. A case study of the New York State Department of Public Service was conducted that investigated regional telecommunications incident response, which produced a model of coordination that recommends new business and communications processes be established that better account for stakeholder needs (Canestraro, Pardo, Raup-Kounovsky, & Taratus, 2009).

4.4 Knowledge Networks

A combined study of multiple public management projects in New York State was conducted that focused on identifying information sharing and knowledge network problems and issues. Authors identify and describe creation of “public sector knowledge networks” (PSKNs) that “treat information and knowledge 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” (Dawes, Cresswell, & Pardo, 2009, p.392).

PSKNs are also sociotechnical systems having mutually influential human, organizational, technical, and institutional aspects related to processes, practices, software, and other information technologies. Knowledge networking, as a form of information sharing, requires particular skills and attitudes. Findings from the literature include that network development processes emphasizing an interactive dialog with stakeholders are likely to succeed (Dawes et al., 2009). The system development processes should be free from the bias of having a pre-defined solution. In the case study of the CNYICC included in this dissertation, it is also argued that social factors are most important to collaboration relationships. In addition to those factors having innovative leadership, access to resources, and authority for the action was found to lead to greater sustainability. Again, these are social characteristics. PSKN’s involved in the study by Dawes, Cresswell, and Pardo included those for: homeless shelters, real property assessment, geographic information coordination, central accounting, justice information sharing (several state-level justice agencies – police, corrections, parole, and central coordinating agency - developing e-Justice New York – information portal), and municipal finance oversight (Dawes, Cresswell, & Pardo, 2009).

4.5 Cross Boundary Information Sharing

A specialized research area within information sharing known as cross-boundary information sharing is significant to understanding collaboration activity. This conceptualization involves law enforcement, emergency response personnel, government, and non-government entities sharing information across their respective domains with each other. Having the capability to access, digest, and apply data and knowledge from the multitude of potential sources during critical incidents and crisis has been called paramount for decision makers and responders. According to Steven Ramage, Executive Director, Open Geospatial Consortium (OGC), cross-boundary information sharing is about overcoming various boundaries between: "Industry, government, academia and the public; Disciplines, professions and industries; Levels of government, local jurisdictions; Nations, languages and regions; Different technologies and different vendor products; Legacy systems and new components and solutions."

Improving information sharing across agencies is cross-boundary information sharing.[4] The U.S. Department of Justice created a series of podcasts in 2010 through the Bureau of Justice Assistance (BJA) which includes a video on information sharing across agencies and boundaries: "The Role of Information Sharing in Counter-Terrorism Investigation and Prevention." The multi-media presentation includes a discussion on federal, state, and local anti-terrorism activities (IT.OJP, 2010). From 2008, international level efforts were underway at the Center for Technology in Government, together with the University at Albany, to create an "International Research program in Cross-boundary Information Sharing" (Mulki, Lei Zheng, Yang & Pardo, 2008). This program is focused on gaining new knowledge regarding cross-

[4] Works that may be considered in this area include: Gil-Garcia et al., 2010; IT.OJP, 2010; Pardo, 2006; Pardo & Tayi, 2007; Pardo, Gil-Garcia & Burke, 2008; Zheng, Dawes & Pardo, 2009.

boundary information in international contexts, and draws on current research in this area with an aim towards new theory development.

Trust is a concern in cross-boundary information sharing. Here, three types of trust are observed by researches: calculus-based, identity-based, and institution-based (Dawes, Cresswell, & Pardo, 2009; Rousseau, Sitkin, Burt, & Camerer, 1998). For calculus-based trust, the participant must have the means to assess trustworthiness of the other party to make a decision. This is not always possible in transactions. Identity-based trust is based on having established relationships with the other party. Institution-based trust is based on the organizational culture, norms, policy, and institutional structures of the entity itself that form the basis of trust or distrust. Actions based on trust are affected by personal and organizational influences and perception. Other aspects of trust are identified and examined in the section following below.

The well-respected MITRE research corporation is exploring technical aspects of cross-boundary information sharing. The Cross-Boundary Information Sharing (XBIS) Laboratory at MITRE provides an unclassified integration and demonstration lab capturing state-of-the-art technologies and processes in the field of cross-boundary information sharing. The goal of the Lab is to show what can be done presently with a focus on the future potential (MITRE, 2009) as social and technical factors in cross-boundary information sharing initiatives are investigated. Ultimately, the goal is to improve information sharing across the law enforcement, emergency response and other communities.

Most scholars recognize the great potential rewards that use of information and communication technologies for integration of information across organizational boundaries can provide (Pardo & Tayi, 2007). According to Pardo & Tayi (2007) true interorganizational information integration and networking has the potential to radically transform organizational structures and communications channels across agencies and geography; it does, however, entail human and organizational, technical, and organizational process and behavior changes (Pardo & Tayi, 2007). Doing so includes benefits, such as improved information sharing and decision-making, as well as presents new challenges.

"Information integration as well as information sharing offers organizations a greater capacity to share information across organizational boundaries, to discover patterns and interactions, and to make better informed decisions based on more complete data" (Dawes,1996). Dawes (1996) described a three-category classification of benefits: technical, organizational, and political (Pardo & Tayi, 2007). Gil-García et al. created what they call an Information Integration Complexity Matrix to look at issues and complexity in cross-boundary information sharing initiatives (Gil-García & Pardo, 2005). Network measurement, quantification, political, economic, and other benefit analysis has been investigated (Milward & Provan, 1998; Rethmeyer, 2005; Young-Ybarra & Wiersema, 1999). These studies provide different means or tools for measuring and reporting the value or contribution of information sharing within organizations. They also provide a method for assessing complexity so that decisions regarding system implementation or use may be better informed.

4.6 Interorganizational Networks

Interorganizational networks can play a critical role in the response to crises and are essential to law enforcement and emergency operations. "When government, communities, foundations, or regional industry groups think about how they can improve their economy, disaster preparedness, competitiveness, health and well-being of citizens, and so on, collaboration through an interorganizational network is an approach that is increasingly utilized" (Provan, Fish, & Sydow, 2007). Public safety networks operate similar to interorganizational networks. Anticipated outcomes are more encompassing than that which could be achieved through independent action.

4.6.1. Public Safety Networks

The formation of Public Safety Networks (PSNs) as information sharing networks was studied (Sawyer et al., 2007; Williams et al., 2009). That study focused on Public Safety Networks (PSNs) created for use at the state-level in the United States and involved a mix of law enforcement and other emergency response and support agencies. Using factors derived from both rational choice and institutional theories, the authors describe the size and maturity of state-level PSNs and propose a set of factors that may predict public safety collaboration (Williams et al., 2010).

Preliminary work exploring conditions for cooperation between emergency management agencies has been done where perceived information assurance of others and having information sharing standards were found to be more strongly related to information sharing than were cultural norms in emergency contexts (Lee & Rao, 2007). Aspects of Public Safety Network (PSN) formation and continuation, as collaborations that share information at the state level, were studied (Sawyer, Schrier, Fedorowicz, Dias, Williams, & Tyworth, 2012). A finding regarding PSN development included that institutional factors provided the most significant coefficient indicating a state's culture of endorsing technological advances, collaboration, transparent sharing of data, or other administrative reforms (Williams, Fedorowicz, & Tomasino, 2010; Sawyer & Fedorowicz, 2012). Some reasons various level (local or regional) public safety networks formed include: a galvanizing critical incident or public safety need, governmental order or mandate, and an identified funding source supporting the initiative (Sawyer, Fedorowicz, Tyworth, Markus, & Williams, 2007; Williams, Dias, Fedorowicz, Jacobson, Vilvovsky, Sawyer, & Tyworth, 2009). A finding of this dissertation includes that at least in one North American case study public safety officials formed a consortium for interoperable communications based not on those reasons but for higher-order interests such as the public good (Treglia, 2012).

These proposed factors do not directly address information sharing issues solely within the law enforcement community; rather they pertain to public safety networks which have law enforcement participants. The PNSs are important to consider as they represent collaborations that involve several types of agencies, structures, and cultures. Lessons learned on collaboration and information sharing apply to the law enforcement and emergency response communities.

5. Social Factors

Social factors as a focus area is comprised of sub-categories of trust, social issues, culture, informal or "shadow" networks, criticality, and quality. The categories elaborated on in this section were chosen following a review the literature and through comments from contacts in the public safety field. The sub-categories were prominent in the literature and mentioned frequently. The sub-categories help identify the types of activities and concepts that fit within this category. The categories do not exclusively represent all of the sub-categories that could be focused on in the social category. The categories identified are further elaborated on in the following section.

5.1 Trust

Trust is placed within the Social factor category. Trust literature “distinguishes trustworthiness (the ability, benevolence, and integrity of a trustee) and trust propensity (a dispositional willingness to rely on others) from trust (the intention to accept vulnerability to a trustee based on positive expectations of his or her actions)" (Colquitt, Scott, & LePine, 2007, p.909).

Trust is a significant factor in information sharing and collaboration. It has special meaning in the context of public safety. As used here, trust manifests itself in agencies through human action. Persons can trust, or not trust, agencies or individuals. It will be identified later as well that trust can apply to a process. A user's sense of trust is not strictly binary and can be understood as involving levels of greater or lesser trust (Rasavi & Iverson, 2009). Trust can be earned and in the case of emergency responders it is also the case that trust can be an essential attribute that is attached to a person or agency by nature of their being a "fellow" officer or department that may have to work together in a critical event or investigation at present or in the future. Reciprocity describes trust as a social exchange process where, even though a contribution may be provided by one party without an identified return, there is an implicit understanding that there will be some (reciprocal) reward in the future (Ostrom & Walker, 2005, p. 232). A more detailed consideration of trust, trust categories, and its use in this dissertation is included in this section, as well as in different contexts in the individual essays. It should be noted that in this dissertation trust is also looked at specifically within and across law enforcement and emergency response practitioners.

Members of agencies may refuse to share information because they do not trust other participating agencies who may gain access to or control over the information (Carter, 2005; Drake, Steckler, & Koch, 2004). This can be a bias due to reputation of the organization or of one or more individuals within the organization. Issues of trust and acceptance of existing or proposed information sharing systems are continuing concerns for organizations (Cresswell, Pardo, & Hassan 2007; Schoorman, Mayer & Davis, 2007). At the organization level, different agencies may not individually trust other agencies that participate and have access to the information that is shared on a collaborative information system. Agencies may choose not to submit their data into an information system, or to participate meaningfully in its governance, where they do not trust or approve of the owners of the system. Agencies may not trust one another as they compete for recognition, funding, or other resources and this has an impact on their motivation for information sharing as they each may be looking out for their own constituencies and special interests. This competitive aspect of trust is discussed in greater detail in later sections.

The problem of trust may stem in part from instances of corruption that have been shown to occur at all agency levels (Butterfield, 2009; Fjeldstad, 2004; Newburn & Webb, 1999; O'Neill, 2006). Agencies maintain confidential and personal information both in their systems and employees. Agencies also maintain and share information as to who their undercover officers are and where they operate so various agency investigations and enforcement activities do not overlap or interfere with one another. Information such as locations of sting operations or law enforcement fronts for illegal operations is shared at appropriate agency and organizational levels to ensure officer and operational safety and reduce the possibility for overlaps. Information such as this can have the gravest of consequences if not properly protected. A Sheriff (Chief Law Enforcement Officer for the county) in the state of Virginia was one of several officers engaging in corrupt behavior that included a department captain, three sergeants, and other agency personnel. According to the indictment, the Sheriff tipped off targets of the investigation, lied to investigators, and helped the suspect in the investigation launder drug profits (O'Neill, 2006). Another public example involved John J. Connolly Jr., an FBI Agent convicted for secretly aiding organized crime leaders in Boston. This became the subject of the 2006 crime film "The Departed” and became well known to all levels of law enforcement. In the area of the country where Connolly worked, other law enforcement agencies suspected a source in the FBI was disseminating information when wiretap operations against certain targets consistently failed. As a result of those suspicions poor relations developed between the Boston office and other law enforcement agencies (Butterfield, 2009). In another case, a top official of the U.S. Central Intelligence Agency (CIA), Harold Nicholson, was charged with selling United States secrets to the Russians; in 1994, another CIA official, Aldrich Ames, was convicted of selling secrets to Russians, which may have resulted in the execution of persons inside the Soviet Union (Nicholson, 1996). These are but a few representative examples of the misuse of information by members of the law enforcement community. It is naive and unrealistic to build policy on a foundational notion that all law enforcement agencies should automatically be trusted simply because they are public safety entities.

Some agencies may not trust the security of the information systems available to them or the networks that support those systems. The security of a system as used here is taken from the United States Code (44 U.S.C. § 3542) and refers to (Zargar, Weiss, Caicedo, & Joshi, 2009):

> "Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide; (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity; (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary

information; and (C) availability, which means ensuring timely and reliable access to and use of information. "

Trust is a significant factor in regards to information sharing and collaboration. It has been introduced here as an identified problem area. The range of factors that affect trust and the various forms of trust are examined in greater detail in the literature section.

5.1.1 Trust Described

Trust is a key influencer of sharing behavior. Trust, in various forms, is well recognized in academic and professional literature as a major component to building and sustaining sharing relationships among agencies (Gil-Garcia, Guler, Pardo, & Burke, 2010; Akbulut et al., 2009; Canestraro et al., 2009; Dyer & Chu, 2003). Trust at the personal and agency levels was identified as one of the most significant factors related to successful collaboration by public safety partners (Treglia, 2012). In this dissertation, trust refers to the degree in which a person with information is willing to share this directly or indirectly with another. This conceptualization includes transfer both within the agency and outward to another. Indirect sharing would involve such things as making data available through a system that is accessible to others.

Trust has been identified as an area of concern in much of the information systems and management research.[5] Trust works that were made part of this research include those

[5] A list of trust works considered in this research include: Gao, 2005; Humenn, Chin, Kosiyatrakul, Older & Northrup, 2004; Ostrom & Walker, 2005; Jing & Pengzhu, 2007; Koufaris & Hampton-Sosa, 2004; Lee, 2006; Lee, Huynh & Hirschheim, 2008; Xiong & Liu, 2004; McKnight, Choudhury & Kacmar, 2002; Niu, 2007; Razavi &

focusing on user-level issues, organizational considerations as well as models for technology adoption such as Task Technology Fit (TFF) and theory on Individualism and Collectivism (Gao 2005; Goodhue 1995; Koufaris & Hampton-Sosa 2004; Lee 2006; Niu 2007; Pardo et al., 2006; Sass 2006; Vaughn, Henning, & Siraj, 2003; Xiong 2005; Zhang 2005). Terms of interest in these works included trust, individual, user, fit, initial trust, and individual relationships. The works cited include those from the fields of social science, social psychology, public administration, policy studies, management information systems (MIS) and computer science. They investigate and report on aspects of trust.

Recent work that addresses different aspects of trust in business and government interactions points to trust as having a greater influence than was previously typically accepted (Booth & Wheeler, 2007; Colquitt et al., 2007; Gerdes, 2010; Morris, Tanner, & D'Alessandro, 2010; Staples & Webster, 2008; Venezia, 2010). In these publications, trust is identified as a factor that is considered in the process of sharing information. Trust is also identified as a critical element for collaborative work, especially in information technology development projects, where it was determined to depend on the rate of knowledge sharing among those involved (Luna-Reyes et al., 2008).

Trust is conceptualized in many ways. The definition is problematic due to the wide variety of approaches to the concept. Risk is but one construct in the conceptualization of trust (Boon & Holmes, 1991). The concept of interdependence is also at the functional core of understanding trust. Interdependence is described as “the extent to which a person’s outcomes in an interaction are contingent on or determined by another’s actions” (Boon & Holmes, 1991, p.

Iverson, 2006; Ruppel, Underwood-Queen & Harrington, 2003; Schoorman, Mayer & Davis, 2007; Zhang, 2005; Rocco, 1998; ISAC, 2004; Li et al., 2008; Ray & Chakraborty, 2004; Chakraborty & Ray, 2006; Park, Suresh, An & Giordano, 2006; Park, An & Chandra, 2007.

191). It is the degree of interdependence between parties that impacts the relevance of trust for the encounter such that the greater the interdependence the more critical is the need for and impact of faith in the expected outcome. This is to say that when the interests of the parties involved are in harmony the level of trust is less of an issue than where each has different preferences or expectations for the outcome.

5.1.2 Risk and Trust

A risk-based method to considering trust is finding increased acceptance among theorists. Trust includes accepting the attendant risk and vulnerability inherent in participating in an information sharing system, personal, or interorganizational exchange, which is not your own (Luna-Reyes, Black, Cresswell, & Pardo, 2008; Zaheer et al., 1998). Trust is differentiated from other risk because it involves beliefs regarding the motivations of others.

In the public safety arena, multiple agencies are separately responsible for their information and physical resources. Agencies do not have direct control over what happens to their assets or information after it is transferred or accessed by others and this can be a source of distrust. Having external forces such as a third-party enforcement capability can improve perceived trustworthiness among businesses (Raiser, 2008). Such an arrangement may be useful to consider in the public safety case.

Trust has predicted risk taking and counterproductive behaviors in organizational settings (Colquitt, Scott, & LePine, 2007). It remains unclear whether the risk is “antecedent to trust, is trust, or is an outcome of trust” (Mayer, Davis, & Schoorman, 1995, p.711). Trust itself is imperfect and generally necessary for cooperation to occur. Cooperation as used in this dissertation involves agents, to include individuals, firms and government entities, agreeing on rules, which are then observed across their interaction (Binmore & Dasgupta, 1986). Gambetta asserts that “Trust uncovers dormant preferences for cooperation tucked under the seemingly safer blankets of defensive-aggressive revealed preferences” and that being wrong about a particular choice is always a possibility (Gambetta, 2000). Progress depends on taking these chances in some cases.

Trust also involves issues of agency. Reliance on others or turning over control regarding an action or decision involves risks. The principal-agent problem, also known as agency problem or principal-agency problem, is a concern in economics, business, political science, and public safety. It relates to the conflict that arises where agents (people or an entity) responsible for looking after the interests of principals (others) use their power for their own interests ahead of the interests of the principals (Gailmard, 2010; Miller, 2005). The focus of positivist researchers has been on governance, identifying situations where a principal and agent may have conflicting goals and describing oversight or control mechanisms that mitigate the self-interested actions (Eisenhardt, 1989). This principal-agent role conflict can be a source of tension over information sharing and shared management of resources in public safety. In public safety especially, command personnel must depend on agents who may or may not directly report to them to complete tasks. There is risk that responders will act autonomously where there is limited contact or control with the supervisors, where there is conflicting information such as the stated condition at a scene versus the firsthand observations, and where individual interests may conflict with those of the command personnel (Rauchhaus, 2009). Agencies use measures such as monitoring technologies, providing incentives for good behavior, punishing non-compliant behavior, promoting their goals and objectives clearly to regulate employee action. Providing for effective accountability and control mechanisms remain issues to be addressed in the law enforcement and emergency response context.

5.1.3 Trust and Context

The meaning of trust varies by situation or context. According to Ross and LaCroix, trust may be considered according to one of three orientations: cooperative motivation, patterns of predictive behavior, or having a problem-solving focus. They also identify that individual predisposition to trust or not trust influenced behavior. In negotiation, those with higher trust were more likely to give the benefit of the doubt to the other party absent clear evidence of untrustworthiness (Ross & LaCroix, 1996). In the legal community, internalized notions of trustworthiness, versus external market forces, are found to be important in corporate sharing relationships (Blair & Stout, 2001). Predisposition and context are important to considering trust behavior (Sales, 2010; Winkler, 2008). In the public safety realm, it is typical for the first reaction to be towards trust in another agency, absent evidence that it should be otherwise.

Jeffries observed that perception of others’ behavior has significant influence on trust following a time of interaction between participants (Jeffries, 2002). The role of attributions in shaping employees' trust in their supervisors was also investigated. Findings include that when employees make sense of negative events, they consider whether the supervisor's behavior was appropriate based on the context in which it occurred (Krosgaard, Brodt, & Whitener, 2002). This has implications as to actions that seem harsh but are necessary at the time. In emergency response, and law enforcement especially, there are times when direct action is necessary and little time is available for introduction or explanation by those in charge.

5.1.4 Trust Level

Trust occurs at the individual and organizational level. It includes other law enforcement officers and extends to the other staff or persons who may gain access to information, were it made available to them and assumes that there is a means for sharing this information (Scott, 2006). Individual agencies may handle information security differently. One agency may require a higher standard than another and not share information based on that. It is also a fact that corruption in a given agency may occur and at any level (Ivkovic & Shelley, 2005). The person responsible for sharing intelligence information may have personal knowledge of individual employees who they do not trust or a general impression or bias, correct or not, of the security within the agency in general terms. Personal impression does influence their decision to share information on the unified system or not. Trust may weigh heavily on the decision to provide information as well (Niu, 2007; Pardo, Cresswell, Thompson, & Zhang, 2006). In the case of a very trusting person, he or she is more likely to freely provide information to the system than someone who is more apprehensive or who has some specific concerns as above.

Trust was identified as a contributing factor to user adoption of new technology systems in a study by van de Wijngaert and Bouwman (2009). In their study of potential adoption of new wireless grids, communications technology, willingness to share, and potential use of the technology, was found to be related to trust. Authors were referring to trust in the partner, trust of the social context, and trust in the technology itself. This same study provided some of the initial support used in the creation of the information sharing framework. It identified here that in emergency situations people are more willing to share information (van de Wijngaert & Bouwman 2009).

Trust as it relates to information sharing was investigated as well by Young-Ybarra and Wiersema (1999). The authors were able to model the weight of the influence of trust in interactions across organizations. They suggested that in accordance with social exchange theory communication, attachment, and having shared values had a significant influence on trust.

5.1.5 Trust and Sharing

Trust and a reason to share are required for information sharing to occur. An obvious comment comes up regarding the need for a channel or means for sharing if, in fact, the decision is made to share information. This is addressed in the framework as a hygiene factor, the capability to share, as well as time to do so, are important factors, but not controlling ones, regarding the decision to share or not to share.

In the process of information sharing, the actor is posited to follow an order of operation in thought that considers trust of the other party involved and the criticality or significance of the information and its potential result, either good or bad, on the actor or another party or group, in determining whether or not to share the information. Without this preceding process to actually share the information, issues of time sensitivity or ability to share, or channel, are not relevant. If an actor has chosen not to share information, there is no meaningful consideration for channel availability or time constraint. Time and channel impact the actions, but do not play the prominent role in the decision itself.

5.1.6 Determinants of Trust

Three determinants of trust– having clear roles and responsibility, knowledge of the other organization, and the way in which authority is exercised– were identified as important determinants of trust relative to cross-boundary information sharing (CBI) initiatives in government. The study involved one county and two state-level criminal justice as well as five state and local public health agency initiatives (Gil-Garcia, Guler, Pardo, & Burke, 2010). Having clear roles and responsibilities speaks to limiting what authority or scope of action one may be giving over by trusting in a transaction. That is consistent with the understanding and context of how trust is expressed in this dissertation. Personal factors that include the way in which authority is exercised are observed in the CNYICC case study and in the literature. This further supports the assertion that observed actions and behaviors influence trust.

5.1.7 Legitimacy and Trust

Legitimacy building in business networks, which is much related to trust studies, is the focus of a study by Human and Provan (2000). Legitimacy is described as referring to "the status and credibility of the network and network activities as perceived both by member firms and outside constituents like funders and customers" (Human & Provan, 2000, p.328). In that study, three dimensions of legitimacy formation are identified: network as form, as entity, and as interaction. These dimensions of legitimacy are reported to be related to future success or failure of a cooperative business network, operationalized as achieving sustainment or demise. That study reported that "achieving success and sustainment depends on a long process of building legitimacy across three conceptually distinct dimensions and being able to overcome significant challenges based on critical legitimacy deficiencies" (Human & Provan, 2000, p.361). Agencies networking in the public safety community build legitimacy over time and may not automatically endow each other with complete trust. That being said, there are also many times in the public safety context where the urgency of a situation demands blind faith in another officer or agency. Officers or responders who do not know each other *do* help each other in life-and-death situations unquestioningly when necessary. The notion of a "brotherhood," in this way, among law enforcement and firefighters is real and necessary in situations where urgency and teamwork are essential. There are times where "blind faith" is needed to get a job done.

Interorganizational networks include interaction in dyads. Dyads, defined here as a group of two, are also considered networks. They involve exchange of information or resources between two or more participants (Arino & Reuer, 2006). The need for legitimacy establishment in larger networks applies to these more intimate interactions as well.

5.1.8 Reciprocity and Trust

It is common in public safety for personnel to extend favors in the form of information, services, or use of resources as professional courtesy. According to Ostrom and Walker "all reciprocity norms share the common ingredients that individuals tend to react to the positive actions of others with positive responses and to the negative actions of others with negative responses" (2005, p.42). This type of exchange may be part of doing one's job or outside the standard operating procedure or protocol. This may not always occur without expectation of a return of some value or reciprocity. Oakerson explains that, "in a reciprocal relationship, each individual contributes to the welfare of the other with an expectation that others will do likewise, but without a fully contingent quid pro quo" (Oakerson, 1993, p. 143). An example may involve a person from a state agency providing information on a subject's address without having the requestor complete the formal written request protocol. These exchanges, which typically do not involve a pre-identified favor in the future, occur based the notion that there is an unstated but understood reciprocal treatment return favor in the future.

Different agencies typically have related activities and investigations at times. This type of reciprocity of trust is a social exchange process without necessarily an identified future return (Ostrom & Walker, 2005, p. 232). This type of social capital is defined as "shared knowledge, understandings, norms, rules, and expectations about patterns of interactions that groups of individuals bring to a recurrent activity" (Dasgupta & Serageldin, 2000, p.177). This understanding is prevalent in the public safety community (although there remains distrust across some agencies and individuals as well). In the public safety community, this is a shared norm. Ostrom notes that a group with more evolved generalized reciprocity, that without a specific quid pro quo relationship, can achieve more than when such developed social capital is not present (Ostrom, 2009). Information sharing and collaboration in public safety is therefore improved where these relationships are fostered.

5.1.9 Trust and Assurance

Consistent with the use of information assurance in this dissertation, assured information sharing is defined by Thuraisingham (2008) as information that is shared between organizations while enforcing security and integrity policies. Research on emergency services reported that technical environments, such as other agencies' information assurance level and having technical standards, seemed to encourage information sharing systems use (Lee & Rao, 2007). This is consistent with findings in the CNYICC case study; agency personnel are more comfortable with information that is known to be "vetted" through an established technical or policy system. Having established standards for systems was said to make them more acceptable and trusted. The first essay addresses additional categories that relate to information systems assurance.

5.1.10 Trust and Technology

Trust has been identified as an area of concern in much of the information systems and management research as it relates to the technical systems as well as in the personnel, cultural, or social aspects of interaction and exchange (Dawson, Reid, Salim, & Burdon, 2010; Gil-Garcia, Chun, & Janssen, 2009; Headayetullah & Pradhan, 2009; Levin & Cross, 2004; Zaheer, McEvily, & Perrone, 1998). On the technical side, information systems must be adequately *trustworthy* and *available* to the agencies that wish to collaborate (Zargar, Weiss, Caicedo, & Joshi, 2009). As used here, trustworthy refers to physical or structural characteristics of the system such that it is considered accurate, available as needed, free from intrusion or alteration of data, and that access is restricted to appropriate entities. There is related work from the field of organization science that identified the importance of access and safety as features impacting on sharing information. Access is related to availability and safety to concerns over the security of the system (Cross, Parker, Prusak, & Borgatti, 2001). Trustworthiness is said to reduce transaction costs in information exchange (Dyer & Chu, 2003).

5.2 Culture

In this study culture is used to describe the accumulated experience, knowledge, values, beliefs, attitudes, meanings, structures and concepts acquired by an identifiable group of people and expressed through their actions. While there is no universally accepted definition of culture there are elements that are commonly accepted. Culture is socially constructed, holistic, historically determined and difficult to change (Hofstede, Neuijen, Ohayv, & Sanders, 1990). Public safety personnel, such as law enforcement and fire fighters, have a history of being strongly socialized. Culture in this distinctive area of public safety has been studied at various bureaucratic and operational levels (Paoline, 2003, Farkas & Manning, 1997).

5.2.1 Social Factors

Socially, the culture within a particular organization will influence the degree of information sharing that occurs. Presently, distrust and lack of knowledge of the other parties involved may hinder information sharing (Glomseth, Gottschalk, & Solli-Saether, 2007). This involves agency culture and even personal ties or connections with other involved agencies, which includes informal or shadow networking ties outside the workplace to include family and friends or other associations that involve one member having some other contact or relationship with someone associated with another agency. A ready example is family, friends, or participation in clubs or activities that involve others apart from the work environment. External contacts can have a positive influence on the likelihood of information sharing. Shared training and joint operations such as the U.S. Marshals fugitive roundup with local agencies in Florida can have positive effects on sharing (Clark, 2008).

5.2.2 Cultural Factors

Research has been conducted on cultural influences on information sharing behaviors in the public sector (Dawes et al., 2009; Treglia & Park, 2009; Wilson, 2010). Agency culture will impact whether or not a person working within a particular agency shares information or not (Drake, Steckler, & Koch, 2004). Apart from the policy of the agency, each agency has a recognizable organizational culture (Pardo, Cresswell, Thompson, & Zhang, 2006). There are unwritten rules for behavior in organizations, and they may restrict or encourage the sharing of information across agencies. A study by Dawes identified three subcultures within the public sector (scientist, politician, and bureaucrat) as a framework to examine benefits and barriers associated with interagency information sharing. Additionally, four types of systems (social, constituency, technical, and organizational) that influence information-sharing processes within and across agencies have been identified (Drake et al., 2004). Making changes to organizational culture is difficult as elements that cause the formation of culture occur over time and emerge from a variety of sources within, and outside, the agency (Doney, Cannon, & Mullen, 1998).

A culture fearful of information technology may be overly cautious or avoid innovation that could improve communication (Kaarst-Brown & Robey, 1999). Research done in 2003 using the Rocheleau Data Sharing Model on North Carolina Law Enforcement agencies found that respondents shared data with those organizations having shared goals and common interests, which supported their core functions. Rocheleau (1996) developed nine hypotheses about public sector information sharing from management literature on both the private and public sectors. The hypotheses are organized into three main categories: facilitating forces, internal facilitators, and inhibiting forces with 13 independent and two dependent variables developed from the hypotheses (Rocheleau, 1996; Vann, 2005). The study by Vann (2005) used an instrument developed to measure correlations between variables (Vann, 2005). Six independent variables were found to have significant correlation with computerized data sharing in the law enforcement agencies here: "common goals, core functions, organizational survival, top management, Internet applications, and organizational autonomy (Vann, 2005)." A further finding from this work was that although top management support is important to sharing, it was influence by top managers within law enforcement that mattered to a greater degree than management or political leadership outside the agency. These findings are especially significant in relating this work to the information sharing factors model of the first essay and the case study of the CNYICC, both in this dissertation. Facilitators and detractors as applied to information sharing and collaboration are discussed in the first essay. In the CNYICC case study, factors such as common goals, autonomy, and top management influence were found to be important to establishing cooperation in emergency communications projects.

Examples of studies done on information sharing in agencies outside the United States include those by Glomseth et al., 2007 and Jing and Pengzhu, 2007. Glomseth found knowledge sharing relative to police investigations, which is a form of information sharing, was affected by the extent of team culture in an agency. Team culture was described as a dimension of occupational culture. In a team culture, members share a group orientation over individualism and tend to cooperate with each other. This study, however, was conducted in Norway. The law enforcement culture in Norway is not necessarily consistent with agencies in the United States.

Jing and Pengzhu studied information sharing behaviors of eight agencies in China that had responsibility for identifying unlawful business activity such as false accounts, forged trade documents, money laundering, and tax evasion. Findings include that inconsistency of policy hindered government-to-government information sharing in China. They note that the government in China is more vertical, with more clearly defined leadership, whereas the U.S. is observed to have a more horizontal structure without common executive leadership. In the Chinese cases, organizational compatibility was found to be more of an issue negatively affecting information sharing than were technical factors. The government environment and culture are not the same as the U.S.; however, the finding that culture and policy factors matter more than technical factors are consistent with the propositions and findings of this dissertation: that social and policy factors matter more than technical factors in information sharing relationships. Such studies may not generalize to the U.S. environment in many respects as culture and policy differ significantly.

There is work done in the U.S. on social and cultural influences of information sharing behaviors in the public sector (Luna-Reyes, Andersen, Richardson, Pardo, & Cresswell, 2007). A dynamic theory of the socio-technical processes involved in defining problems in integrating information was created. The study involved a Criminal Justice Information Technology group at the state level. The created model shows the importance of social accumulations such as trust, understanding, commitment, and engagement in managing information-sharing projects. This process is in line with the approach taken in this dissertation. Social factors, which include trust issues, are important to understanding information sharing behaviors in law enforcement and emergency response (Treglia, 2012).

Police agencies were the subject of a study on patterns of informal communication ties between agencies and the influence of the network contacts on adoption of innovations and change in agency practices (Roberts & Roberts, 2006). Findings there included that agencies tended to choose agencies larger than themselves and agencies of the same type for contact and guidance (Roberts & Roberts, 2006). The preferred networking in that study occurred at or above the level (relative size) of the initiating agency. Larger agencies, according to the study, generally do not communicate as readily with those considered smaller.

5.2.3 Interorganizational Networks

Literature in the area of interorganizational networks includes findings relevant to the interest here in information sharing problems, especially as they pertain to risk and trust in information sharing exchanges. Most conceptualizations of interorganizational networks refer to themes of social interaction, relationships, connections, collaboration, trust, collective and cooperative action (Provan, Fish, & Sydow, 2007). The significance and role of trust is discussed in (Ekbia & Kling, 2005; Uzzi, 1997). Podolny and Page (1998) include varying forms of cooperation, strategic alliances, collaboration, joint ventures, and consortia within their definition (Provan, Fish, & Sydow, 2007).

5.2.4 Informal Networks

Informal networks (also referred to here as shadow networks) involve the situation where a personal or agency connection, in or outside of the workplace, creates a conflict of interest and the organization or individual may not act in a non-biased, objective manner. This may involve personal friendships, affiliations or family ties and connections through other activities or interests outside the workplace. This can have positive and negative effects for organizations (Ingram & Lifschitz, 2006). Information that may negatively impact an agency or key individuals or associates may be withheld and not shared by the organization involved. This is where conflicts of interest are at play. The stigma or interpersonal links behind the scenes plays a role in interaction and sharing decisions (Kulik, Bainbridge, & Cregan, 2008).

Observers must account for these interpersonal connections that may exist in the law enforcement environment; there are times where sensitive information comes too close to home for those involved to remain non-biased (Huijboom, 2007). A law enforcement officer is not going to give his or her own mother a ticket, and similarly agencies and officers may have personal and other ties that influence or bias their information-sharing behavior. Threats to the security and assurance of information sharing systems that are driven by even adversarial or other ulterior motives must be anticipated and understood. Edward Norris, who served as New York City Deputy Police Commissioner, Superintendent of the Maryland State Police and Baltimore Police Commissioner, was indicted for corruption in 1993, which included allegations of thefts of money from secret funds (Levitt, 1993). The fact that humans are imperfect is not in question; the concern is that systems must be in place that account for such a condition and which can still be effective in this environment.

5.3 Criticality

Criticality relates to the potential harmful impact of the information and its urgency. It can also include a potential scarcity of a resource such as something key to an activity or operation (Yound-Ybarra & Wiersema, 1999). Information that, if not acted upon, may cause specific harm, plays a critical role in the likelihood that it will be shared. Studies show that officers are more likely to share information where there is a clear and present danger to life or property (Lee & Rao, 2007).

The criticality of the information itself, and its potentially harmful impact if not disclosed, is a key influencer of action in sharing information. The rules and expectations seem to be different where exigent circumstances come into play. On a day-to-day basis, the information and collaborations must be effective and rehearsed so that when the emergency does occur and the various agencies must come together and collaborate, there are channels, systems, data, and other resources readily available for this, which cannot happen effectively without prior preparation.

In a direct way, there is no sharing of information without a *channel* or technological means to do so. If there is no possible way to share information then there is no constructive value to considering whether or not to share the information; it is a moot point. If the actor knows in advance that there is no way to share information, the activity of making the sharing determination is not necessary. The two events are separate; the decision as to share or not share information itself, and the other, whether or not this is possible or not, due to physical capability and time.

The matter of time playing into the decision process is more complex. Criticality may involve the pressure of time playing into the decision of whether or not to share information. An actor may have information to share regarding an incident, but hold off and, as a deadline approaches, feel pressured to act because the situation did not change or no other person stepped in to provide the information. In this case, it appears that time played a role in the decision to share or not share. A more fine-grained analysis reveals this scenario not to be accurate. Time is forcing the decision process but is not directly involved in the equation of trust and criticality as those elements have been described. Criticality is separate from but related to the issue of time. Criticality involves consideration of things such as importance or danger to others as well as potential benefits that may come from the sharing of the information, among other things previously reported on. In this instance, a person holding off a decision, hoping for some other intervention, is only delaying making the decision. The decision itself of whether to share or not share information remains based fundamentally on trust and criticality. The decision described is based on the possibility of another solution becoming available or not; time affects the dynamic as a deadline for making the decision but not as an element of the decision.

5.4 Quality as Assessed by User

The *quality* of information is also determined by the user's perspective and role. Information that is of high quality for one user's purpose may be considered of low quality to another (Singh, Park, Lee, & Rao, 2009). Information needs for law enforcement at a terror-related explosion may be different than for the responding ambulance crews; both will be concerned with aid to victims and the law enforcement may further have interest in identity and affiliation of victims who may also be participants. It is standard practice for police to investigate all "hostages" that are released or rescued to determine both well-being and affiliation. By its nature, the dimensions of quality information are difficult at times to observe, capture or measure (Singh, Park, Lee, & Rao, 2009).

6. Technical Factors

The Technical domain consists of factors such as interoperability, availability, and control. These are further identified in the following sections.

6.1 Interoperability

Interoperability is a critical issue facing public sector entities that must access information from multiple information systems and sources. Establishing semantic interoperability among heterogeneous and distributed information sources remains a critical issue in research and practice (Park & Ram, 2004). There are many disparate information systems currently being used by law enforcement agencies for data management and communication, such as COPLINK, OneDOJ, N-DEX, ALECS and others (Bulman, 2008; Chen, Zeng, Atabakhsh, Wyzga, & Schroeder, 2003). This lack of standardization creates obstacles for resource sharing and innovation adoption. Having uniform standards in hardware and software would allow for greater innovation and product development (NIST, 2005). Even at the data collection point, problems arise. A 1921 quote from a text on American Police Administration (Graper, 1921), which was written prior to the technology boom, but informative even today, illustrates this issue:

> "Unless the facts upon which information is desired are definitely outlined there will be great variety in the methods of reporting and in the information given. Formerly it was customary for members of the force to make reports much as they pleased." (Graper, 1921, p.287)

This is further complicated by the fact that, as time goes on, agencies become engaged with and invested in different technologies and procedures. This is a technology and process legacy issue. As such, more will be at stake in the future when these agencies are asked to make a change to more universal or standardized method of operation, and the transition costs may be too high (Powner, 2008; Scott, 2006). There are technological solutions emerging that address this need in different ways. Improved security and networking technologies may address some of the current barriers identified.

6.1.1 Wireless Grids and Edgeware

There are alternate means for improved networking. Wireless grids as a new sharing technology and innovation has application potential in the area of law enforcement and emergency response (Treglia, et. al., 2011). Wireless grids are defined as providing "flexible, secure, and coordinated resource sharing among dynamic collections of individuals, institutions, and resources" (McKnight, Howison, & Bradner, 2004, p.26). This includes electronic enabled sharing of voice and data. Resources shared in this context include technological devices and services that are accessible through wired or wireless communication channels. Institutions and individuals that have or use these devices are the users. The public safety arena involves a variety of devices for communication and data access including radios, cell phones, PDA's, alarms, sensors, WiFi networks, and other wired and wireless networks. Services include things such as internet access, databases, public and private networks, and other information resources.

A new class of open standards software that facilitates activity across wireless grids, called edgeware, enables ad hoc connection of people, services, software and services in a personal cloud, is becoming available (Treglia, Ramnarine-Rieks, & McKnight, 2010). Many aspects of the technical barriers to information sharing can be largely set aside in an environment such as that provided through wireless grids edgeware, allowing us to concentrate on other important issues.

This is different from the traditional conception of a shared computational processing resource grid for parallel computing or combining high-end processing resources for computing large tasks. The form of grid computing described here offers a solution to the challenge of "flexible, secure, and coordinated resource sharing among dynamic collections of individuals, institutions and resources"(Foster, Kesselman, & Tuecke, 2001). The grid here allows for the cooperation and coordination of varied devices and platforms that may be wired or wireless. The ultimate vision of the grid is as an adaptive network providing secure, inexpensive, and coordinated real-time access to dynamic, heterogeneous resources (services, application, information, and computational power), that can traverse geographic, political, and cultural boundaries and still maintain the desired characteristics of simple distributed systems, to include stability, transparency, scalability, interoperability, and flexibility while maintaining security and integrity.

Wireless grid applications may be considered in three categories of applications, those that:

(1) Collect or aggregate data;

(2) Take advantage of their location or where they can move to and;

(3) Take advantage of cooperation among a mesh of mobile devices.

Some authors suggest that this emerging infrastructure for a wireless grid will fundamentally change the way society thinks about and uses computing (McKnight & Kuehn, 2011). A broader understanding regarding the nature of the capabilities and options grid computing allows for, as well as the technology necessary to realize the new opportunities, is required (Fichman & Kemerer, 1997). The grid-computing concept provides for the creation of virtual workspaces as configurable execution environments that are created and managed by describing client requirements (Fichman & Kemerer, 1997; Lyytinen & Rose, 2003). Recent work regarding wireless grids includes research on: user and socio-technical perspectives and challenges (Dillinger & Buljore, 2003; McKnight, Katz, & Vaaler, 2001); coordination of user and device behaviors (McKnight, Lehr, & Howison, 2007; van de Wijngaert & Blondia, 2004); future internet applications and bridging communicative channels (Jin, 2002; McKnight & Kuehn, 2011; Rogers, 1995). Wireless grids and edgeware may benefit law enforcement agencies and emergency responders by providing an alternate means to bridge different devices and communication resources.

In the field of radio, wireless distributed computing networks (WDCNs), as wireless grid networks, can transform a group of resource constrained low-cost nodes into a high-performance computing/platform. This area has application to connecting detection equipment and sensors to first responders and investigators in the field. Within each WDCN, the resource requesting node distributes its computing workload to service nodes through a wireless link (Chen, Newman, Datla, Bose, & Reed, 2009). These service nodes compute the allocated workload and send it back to the requesting node. Virginia Tech leads the effort to develop gridlets that structure WDCNs over common wireless devices improving efficiency and stability. Areas of application for this work are related to military scenarios, emergency and disaster response, and mobile gaming.

6.2 Availability

Availability means that the systems must respond in a timely manner and have a sufficient quality for user interface that the users in a given situation will accept them. These systems must have a high degree of survivability and function in mission-critical environments where parts of the network may be compromised but accurate service must be continued

(Schooley, 2007). Network availability impacts acceptance and use of systems (Chan & Teo, 2007; Koroma, Li, & Kazakos, 2003). Information must be kept up to date and in accordance with the users' changing interests and needs. System performance and reliability become taxed as these systems attempt to integrate with the variety of new technologies and protocols that are being used. Systems become more prone to delays or failures as they must incorporate legacy and other protocols into their core programming and functions. Increases in the sophistication of security and authentication processes add to the workload and potential for system delay or failure. Systems that are considered slow or non-responsive according to the expectations of the users will have a hard time being adopted (Chan & Teo, 2007).

6.3 Control

Control over access, use and manipulation of the system and the data as perceived by users is most important for information sharing and systems adoption. Losing control over the information or data, or allowing it to be altered, after it is transferred to another party is a concern for those providing their data. In addition to actual control over resources, it is expected that their perception of having such control is important. Systems must be capable of monitoring and managing all usage and dissemination of information, as well as provenance. This accountability is for tracking purposes and a feeling of assurance, which is required for trust (Powner, 2008). There is no one accepted formula to produce a sense of control. There is no broadly accepted set of minimum security and access control standards and protocols for information systems that have been uniformly adopted for use across federal, tribal, state, and local agencies (Cresswell, Pardo, & Hassan, 2007). Distributed workflow control tasks in these integrated and grid environments become complex and may require both local and remote executions (da Cruz, Chirigati, Dahis, Campos, & Mattoso, 2008). Provenance and user control tasks and capabilities must be suitable to these varied environs.

Acceptance is based on the terms of the individual users and agency culture. Each agency may have different perspectives or requirements for what is considered acceptable (44 U.S.C. § 3542). Issues of broad-based system trust involve identifying and communicating minimum standards for reliability, network security, and program security that can be accepted by all members of the law enforcement community at all levels. There is a range and diversity of confidence needs here from low to high. The problem mimics the initial development of the National Criminal Intelligence Center (NCIC), which began in 1967, and the National Law Enforcement Telecommunications System (Nlets), which links state and many federal agencies for exchange of criminal justice information (Dempsey, 2000). The problem entailed finding a way to meet the needs of multiple and diverse interests in an environment characterized as one of control over resources. Much work was done to identify a minimum set of security protocols, which would be understood and accepted by the greatest number of participants.

There have been a number of agencies looking to address information sharing standards, none of which have garnered universal consensus and some of which are no longer operating. Standards are proposed from agencies such as the Department of Homeland Security and the United States Department of Justice as well as through groups such as the Law Enforcement Information Technology Standards Council (LEITSC, 2009, 2012). LEITSC was comprised of the International Association of Chiefs of Police, the National Organization of Black Law Enforcement Executives, the National Sheriffs' Association, and the Police Executive Research Forum, but has been discontinued. The Global Justice XML Data Model (GJXDM) is part of the Global Justice Information Sharing Initiative's (Global) Infrastructure and Standards Working

Group (ISWG). The ISWG looks to standardize the data sharing of justice organizations through standards specification. Other organizations like the National Center for State Courts Joint Technology Committee, American Probation and Parole Association (APPA), and the Corrections Technology Association (CTA) are also working on shared universal standards (Hicks, 2004). There is still no communitywide consensus.

The most widely known of the United States' information sharing initiatives is the National Information Exchange Model (NIEM). This is an effort to standardize content (data exchange standards), provide tools, and manage sharing processes across entities. The exchange development methodology supports a common semantic understanding across participating organizations striving for data to be formatted in a semantically consistent way. NIEM was created through a partnership of the U.S. Department of Justice, the U.S. Department of Homeland Security, and the U.S. Department of Health and Human Services to develop, disseminate, and support enterprise-wide information exchange standards and processes to better share critical information in emergency situations and in day-to-day operations (NIEM, 2011). Examples of NIEMS implementations include:

> "Colorado Integrated Criminal Justice Information System (CICJIS) - The CICJIS program facilitates the sharing of critical criminal justice data among five state-level agencies at key decision points in the criminal justice process. It created the first technical enterprise sharing architecture in the state and is driven by the business information needs and business process requirements of Colorado's state criminal justice agencies. CICJIS moved forward criminal justice data sharing using the Justice Reference Architecture (JRA) and NIEM" (NIEM, 2011a).

> "Emergency Operation Center--Interconnectivity (EOC-I) - The EOC-interconnectivity (EOC-I) project defined a set of data exchanges for requesting and responding to incident and resource information enacted and acquired during the incident. The NIEM-conformant exchange and prototype system is based on emerging Internet technologies and designed to improve information sharing, situational awareness, and collaboration by regional EOCs during multijurisdictional emergencies to maximize the situational awareness for first responders. The EOC-I project was developed through interactions with state, regional, local, and tribal first responders in the Seattle and Cincinnati regions as well as in coordination with FEMA and NIMS multiple working groups" (NIEM, 2011a).

Recent crises and scenarios such as those referenced above demonstrate that immediate, secure, enterprise-wide information sharing and interoperable communications are required to facilitate tightly coordinated response across multiple agencies, domains, and jurisdictions, and agencies cannot oftentimes securely share critical information in "real time" (NIEM, 2007; NIEM 2011). The NIEM process is designed to create efficient and effective sharing of information using robust information exchange standards (NIEM, 2007; NIEM, 2011).

Technological solutions for improving information sharing between criminal justice agencies have been investigated extensively. The effects of data quality and privacy on limiting information sharing between criminal justice agencies was studied through use of a technological software solution, Entity Analytics Software (EAS). The two cases studied showed that use of technology improved identification of duplicated data across their records systems, thus improving information quality. The study proposes that having better data quality leads to information being more readily shared between criminal justice agencies (Plecas, McCormick, Levine, Neal, & Cohen, 2010). This dissertation posits that agencies are more willing to share information that they trust to be accurate. In another study addressing technology improving information utility, Yang used partial information from shared resources of separate criminal justice agencies to conduct terrorist or criminal social network analysis. A finding here was that even where incomplete information was provided due to security concerns, social network analysis was improved where additional agency information was provided for the system (Yang, 2008). Technological solutions such as described here can enhance available information and improve the sharing of information.

Research conducted at major universities investigated issues of cooperation, information sharing and tools for law enforcement, and emergency response. Roundcount at Saint Louis University demonstrated that county sheriffs and school superintendents found value in use of information sharing through Geographical Information Systems (GIS) in crisis response (Roundcount, 2010). Supporting that conclusion, yet separate from that study, was a 2011 incident in upstate New York involving a shooter near an elementary school. Having GIS information could have been useful to responders there in assessing the situation for containment and evacuation.

In 2009, the White House established the Information Sharing and Access Interagency Policy Committee (ISA IPC) of the predecessor interagency body (the Information Sharing Council) established by IRTPA. It is section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), P.L. 108-485, § 1016, 118 Stat. 3638, 3664 (2004), as amended, that directs the Information Sharing Environment (ISE) to improve the sharing of

Terrorism and Homeland Security Information (ISE, 2011). The IRTPA definition of “terrorism information” includes any terrorism-related information “whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities,” and amended in 2007 to include Weapons of Mass Destruction Information (ISE 2011). Partners include: Critical Infrastructure and Key Resources, Department of Justice - Office of the Director of National Intelligence, Department of Defense, Department of State, state, local, territorial and tribal governments, Department of Homeland Security, and the National Maritime Intelligence Center. The current ISE is to combine policies, procedures, and technologies linking resources (people, systems, databases, and information) at all levels, tribal entities and the private sector; the primary focus is "... any mission process, anywhere, which has a material impact on detecting, preventing, disrupting, responding to, or mitigating terrorist activity" (ISE, 2011). In 2010, the Department of Justice created the "National *Suspicious Activity and Reporting (SAR)* Initiative" (NSI - National SAR Initiative) to assist participants at all levels in sharing and compatibility. Today information sharing involves more than terrorism-related threats and issues, but encompasses sharing information to improve the national security of the United States and safety of the American people more broadly.

There are initiatives sponsored by the federal government that directly impact information sharing efforts at all levels (ISE, 2011). These issues involve federated or delegated control over assets and resources. Detailed information on these entities and activity is provided in Appendix A (Federal Initiatives on Information Sharing).

It is important to have accepted technical standards for information sharing and exchange if there is to be an environment of resource sharing, albeit difficult with so many competing standards and entities involved.

6.4 Technical Quality of Information

The quality of information remains an important consideration in law enforcement and critical incident response. "Information quality" can be generally defined as the degree to which the information meets the needs of the user, “*fitness for use,*” in both individual and communal/societal uses (Stvilia, Gasser, Twidale, & Smith, 2007). Quality is a technical factor in relation to the framework of Figure 2 (Treglia & Park, 2009). There has been limited work specifically addressing this area as it relates to emergency response. The relationship between information quality dimensions and challenges of coordination in information management activities for interagency crisis response was investigated through a framework by Gonzalez and Bharosa (2009). Other models have been proposed and there is guidance to U.S. agencies from the federal level.

From the knowledge management field, Kulkarni, Ravindran and Freeze (2007) argue that Information Quality measures semantic success, System quality measures technical success, and User Satisfaction measures effectiveness success. Further, the authors see Information Quality and System Quality as independent variables. The information quality measure of the IS success model is focused on relevance of information and precision while information quality itself is comprised of multiple attributes. According to the authors, a more comprehensive approach in this same area assesses quality based on the ability for information to be presented, visually, auditorily, through text or graphics, and in the way most useful to those in need of the information, as it pertains to their specific situation. Value determination is more related to usefulness in the field or tactically.

Quality information is crucial to law enforcement and emergency responders as decision quality can be linked directly to availability of crucial information. Quality information has been identified as having the following characteristics: timeliness, accuracy, completeness, consistency, relevance and fitness for the needed use, format, compatibility, security, and appropriate amount (Kulkarni, Ravindran, & Freeze, 2007). This accounting speaks to the need for the information to be understood by the user, a significant point that must be addressed in cross-boundary and inter-cultural environments. Availability is an important consideration where too much information may be coming in to digest or where communication bottlenecks may occur, hindering the flow of the most needed information.

7. Policy Factors

7.1 Regulation and Legal Factors

The laws and policies governing information security, dissemination and use vary across local, state, tribal, and federal agencies. Where agencies do not have clear guidance on whether or not information may be shared, they may choose to take the safer path of not sharing to protect them from potential liability.

Policy, *Regulation* and legal factors surrounding information sharing are complex (McKay, 2008). This presents a problem for those wishing to share as much information as they can (Carter, 2005). The concerns over privacy and violation of individual rights of citizens must be addressed (German & Stanley, 2008). There is no clear standard or ready guideline for agencies that addresses information sharing issues at the federal and local levels in a readily usable way (Swire, 2006). Civil liberties issues must be addressed (Martin, 2004). If agencies had this resource, they would be in a better position to actively share information and address the concerns over privacy and sharing (Carter & United States, 2004). The notion of these barriers to information sharing acting as a “wall” has been proffered for some time yet arguments can be made that it is lack of knowledge about current statutes and policy and not the statutes themselves that are hindering agencies from sharing (Martin, 2004).

7.2 Governance

The *governance* systems regarding law enforcement collaboration may be a source of the sharing and collaboration problem. Historically, there has been a top down approach to implementing information sharing mandates. Law enforcement agencies in the United States, however, share overlapping responsibilities and jurisdiction with no one unitary command; this creates problems over control and authority in investigations and information sharing and access. Edwin Meese III, 75th Attorney General of the United States and Ronald Reagan fellow for the Heritage Foundation wrote:

> "Federalizing crime undermines the idea that the states should be free to experiment with their own systems, to be in effect laboratories of government effectiveness. Furthermore, it shifts accountability, and as I mentioned, certainly confuses the citizens as to who is in charge" (Meese, 1998).

Agencies independently act in the interests of their constituencies as well as for the broader collective good. Agencies may participate by providing their data in a shared information system or not based on which agency owns or operates the system. The governance structure itself plays a role in how agencies choose to participate in jointly operated or controlled systems or activity. Walker and Ostrom write that “institutions and context play a key role in creating assurance”, building trust (2007, p.33). Having appropriate governance structures can foster better cooperation (Ostrom, 2009; Ostrom, 1994). This is to say that there is a fit between the controlling structure and the individual environment and circumstances that it is operated in. Effective Structures and governance systems for the public safety realm are likely to be different than in education, for example. Governance is sensitive to context.

The Law Enforcement-Private Security Consortium conducts research on and supports development of effective law enforcement-private security collaborations in the U.S. A finding of this consortium is that cooperation between private security and law enforcement is hindered by a lack of an accepted coordinating entity (LEPSC, 2009). Additional factors related to governance include findings that governance structures influence cross-boundary information sharing in criminal justice agencies at the state and local levels. Determinants of effective governance structures supportive of cross-boundary information sharing include having the following: knowledge of information needs, knowledge of the environment, a diversity of participating organizations and their goals, knowledge of participating organizations, enabling legislation, and executive involvement (Pardo, Gil-Garcia, & Burke, 2008).

7.3 Levels

There is research that focuses on interagency information-sharing issues in the law enforcement sector that was done in the United States that involved looking at agencies sharing information at the same levels (Pardo, Gil-Garcia, & Burke, 2008), and sharing information generally (Akbulut, 2003; Fedorowicz et al., 2010; Randol, 2009). Other studies were not conducted with law enforcement agencies and do not differentiate intelligence information from other information gathered and shared (Pardo et al., 2006).

A case study through Rutgers University explored perceived efficacy of fusion centers (formal collaborations between multiple agencies within a state for information sharing), and found the fusion centers continue to struggle with many process, analysis, and other challenges (Graphia, 2010). The study at Georgetown University addressed homeland security collaboration issues among state-level players, using survey data from the Council of State Governments (Rabbit, 2009). They found that having state-level participation in terrorism-related investigations with federal agencies enhanced state-federal collaboration. Research conducted by Thatcher at the University of Arizona investigated individual and organizational antecedent factors to use of knowledge-sharing technologies. In particular, their study highlights that information sharing is affected by organizational context. A finding included that "given the characteristics of a police organization, an increase in the use of the knowledge sharing technology to communicate with external groups results in decreased productivity and job perceptions" (Hauck, 2005). Officers must take time out from other activity to input information into knowledge-sharing systems. Officers in many cases are rewarded or recognized more for individual achievement and passing on information that others could use for their own gain (such as closing a case by arrest) can be seen as counterproductive by individuals. The study supports the notion that law enforcement and other entities must be aware of context and possible unintentional effects of using knowledge-sharing technology.

At the federal level in the United States, the Secret Service (USSS) is one example of an agency, which deals with information sharing policy across all federal, tribal, state, and local agencies and which looks to engage with non-government entities and citizen groups. One of their roles is to participate in "the planning, coordination and implementation of security operations at special events of national significance" (USSS, 2011). Where an event is designated by the Secretary of Homeland Security a "National Special Security Event (NSSE)", the Secret Service takes on a mandated role as lead agency for design and implementation of the operational security plan (the Presidential Protection Act of 2000 became law in 2000 and included in the bill an amendment to Title 18, USC § 3056, which codified Presidential Decision Directive PDD-62 regarding combating terrorism). In this role, the USSS has established policy and procedure for engaging with established and created partnerships between law enforcement and public safety officials as well as other entities to provide a safe environment for all participants and the general public. This entails enormous coordination and contact with formal and informal stakeholders as noted and published in the After Action Report of the National Capital Region (NCR) Project Team "2009 Presidential Inauguration Regional After-Action Report (AAR) Summary" (NCR, 2009). Lessons learned from this and similar experiences provide valuable information on communication and cooperation in mixed environments. Due to the nature of action and agencies involved, much of this is not for public disclosure or outside dissemination. This is an area where is should be noted that not all resources and data that may be available can be shared even across law enforcement entities or other emergency responders.

7.4 Jurisdiction and Overlap

Additional concerns are raised regarding factors of control, governance, and responsibility over information and incidents. As identified previously, the governance structure of law enforcement and emergency response agencies in the United States is primarily decentralized, not operating under a unitary command and control structure.

The problem of shared responsibility and overlapping jurisdiction affects the ability of law enforcement entities to cooperate effectively. At the federal level, there are crimes that are clearly violations of specified Federal statutes, yet they may have State, Tribal, or local equivalents. This makes jurisdiction unclear in many cases. Across federal agencies such as the FBI, DEA or others, they too may have overlapping jurisdiction and/or responsibility for a crime or the accompanying co-occurring incidents or offenses.

Crimes surrounding acts involving illegal drug (or controlled substances) possession, creation, and smuggling by an organized gang is a fair example of crime that may cross several federal and local agencies authority. Local law enforcement has clear authority in this regard where the incident, or part of it, occurs in their designated geographical jurisdiction, but they are not alone. By way of example, if this incident took place on the railroad track of a town within a county in a state, the town police, railroad police, county and state police may all have similar authority to investigate it. There are other agencies such as the DEA and/or FBI who could also be involved. The Federal Drug Enforcement Administration (DEA) mission is to:

> "...enforce the controlled substances laws and regulations of the United States and bring to the criminal and civil justice system of the United States, or any other competent jurisdiction, those organizations and principal members of organizations, involved in the growing, manufacture, or distribution of controlled substances appearing in or destined for illicit traffic in the United States; and to recommend and support non-enforcement programs aimed at reducing the availability of illicit controlled substances on the domestic and international markets" (USDEA, 2011).

The FBI mission is to "to protect and defend the United States against terrorist and foreign intelligence threats and to enforce the criminal laws of the United States" (FBI, 2011). The FBI priority areas include: organized crime, violent crime, and major thefts. There would need to be a discussion as to whose resources and responsibility would ultimately be used. Other examples include crimes having specific federal statutes that apply, but these, too, may have local level legislation in place that can be applied. Larceny is defined generally as stealing property or service, which has broad application, including things such as cash, drugs, animals, plants, and phone service.

One observes that state and local government entities and other law enforcement agencies have clearly defined borders and jurisdiction, albeit overlapping. The overlap refers to both geographical jurisdiction and authority to act regarding a particular event. Such is the case where village, town, county, and state police share authority for investigation and arrest where the incident occurs in a location such as a village. Agencies do have defined geographical boundaries that they may be responsible for, such as the city limits, fire protection district, or a school district (which may cross village, town, and county boundaries) with legally defined boundaries. The model provided below shows states having jurisdiction and responsibility that overlaps with lower-level units of government. This is in regard to their geographical jurisdiction and authority to investigate incidents. It impacts their ability to intervene in crisis situations and make arrests among other tasks. The cities are separate from towns or villages although they are located within a county and state. The figure is broadly representative. Not every state has all of these layers or contains this specific structure. The Figure below useful to understanding the relationships and environment that law enforcement, emergency response, and other governmental officials operate in. It is organized to depict in a visual way the responsibility and interest various entities have in responding to an incident or event.

The dynamics involved in this environment of shared responsibility are complex. Creating a better understanding of the forces and motivations of the various entities involved will help practitioners and policy makers better understand the forces and influences involved in achieving cooperation and service provision in multi-agency emergency response events. Identifying policy and practice insights and recommendations that can be effective in this environment are important goals in this research.

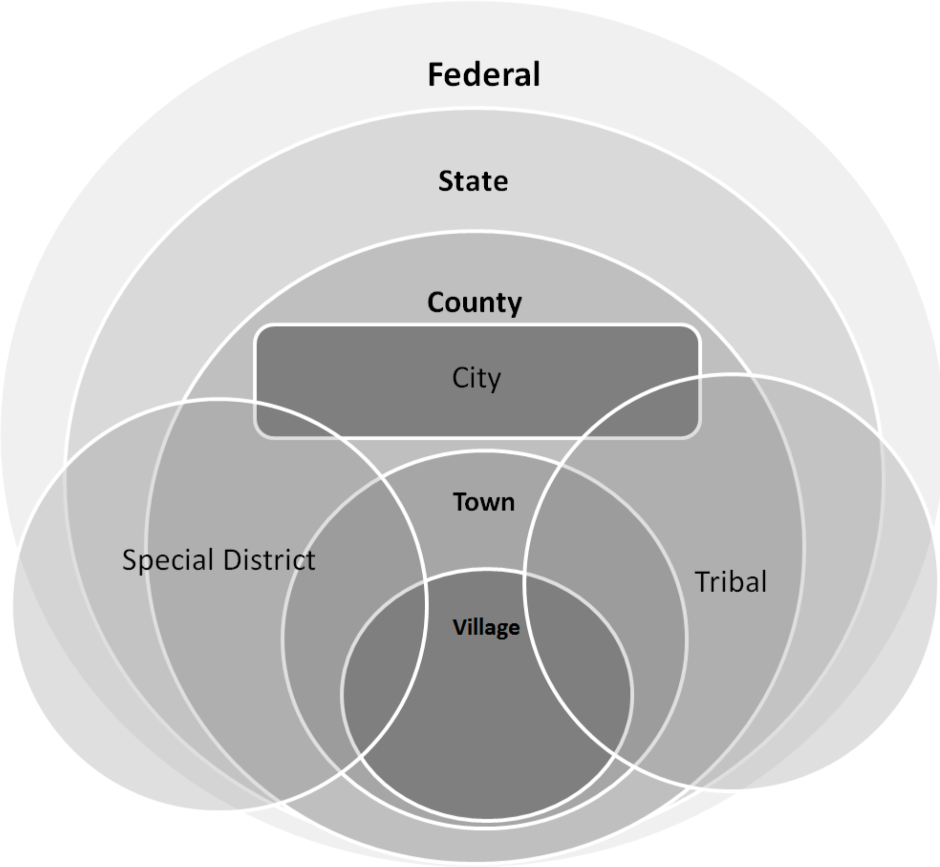


Figure 5: Overlapping Responsibility and Jurisdiction in United States

(Treglia, 2010)

Law and policy may be enacted at each of these levels by various governing bodies. Other issues such as “home rule” states, “Dillon’s Rule,” and the “Cooley Doctrine” grant or propose varying powers to the local governments (Barron, 2003). A town ordinance may prohibit something, such as smoking in public, and the village within the township may not a have law for or against this. In this case, as the village is within the town, the town's prohibition applies in the village as well. A fire-protective district may include sections of several town or village boundaries. Other levels interact in a similar fashion.

7.5 Financial Factors

Agencies at the federal-to-local levels are political entities and must justify their budgets to their constituencies and oversight entities. Many of these agencies are directed by elected officials such as Sheriffs or other municipal leaders. This makes them accountable to their constituents. As such, they have interests that are localized and perhaps not congruent with interests of other jurisdictions or the broader, higher interest or needs elsewhere. To hold their positions, they must be responsive to their own constituents and higher ups. Others in authority may be hired or appointed to positions of leadership. In any case, these persons become responsible to the agency they work for and whose mission and purpose they are to represent. They all must report on their activities and demonstrate that they are doing the job effectively.

These agencies also compete for limited financial resources and, again, must respond to the interests of their individual constituencies (Drake, Steckler, & Koch, 2004; United States, 2007). There is limited funding for programs and support for disaster preparation, response and recovery – and agencies compete with each other for access to these resources. As competitors, there is reason for them to consider not sharing such things as information on programs, services, and how to apply for grants or resources, because that might reduce the chance that their own agency will get the award. By way of a state-level example, a request for proposals went out in New York State to provide funding for implementing tele-conferencing for county agencies. There are 62 counties in New York State and it was announced that there would be funding for up to 10 of these projects. In this case, counties directly compete with each other. The incentive to not help the competition, or to look for ways to show your application, is the most worthy of support is high. Agencies were to include quantitative figures and qualitative arguments to justify their projects in terms of return on investment (ROI) and need (Cresswell, 2004). This created an environment where each agency must show that they were the one doing the most work. The implication here is that there is a risk to the competitive advantage of an individual agency if they fully share information with their counterparts. This may result in an agency choosing to not make their processes and data available to others or to agencies making competing claims over activity figures such as arrests stemming from joint or shared investigations or response to incidents. A federal report from the U.S. Government Accounting Office acknowledges that these figures are considered by funding agencies when making award decisions:

> "In general, agencies use investigation and arrest statistics as indicators of agency work and as output measures in performance plans, budget justifications, and testimonies. In some cases, these data are considered in making promotion, bonus, and award determinations. However, investigation and arrest statistics are not emphasized in any of these activities, but are one of many factors that are considered."

> "All of the agencies GAO reviewed counted the same investigations and arrests when more than one of them participated in the investigative and arresting activities. This practice seems appropriate because many investigations and arrests would not have occurred without the involvement and cooperation of all

> the agencies that participated. If agencies were not allowed to count investigations and arrests in which they participated, agencies would be less likely to work together, cases would be much smaller, and the desired disruption of high-level criminal organizations would be hampered."
>
> (United States, 2004)

Under the present policy structure, many law enforcement agencies are put in a position of being in competition for statistics and resources with other agencies. As described above, "statistics" such as arrest figures can lead to greater funding and agencies seek to claim ownership of arrests and incidents that make them score higher in some state and federal formula-based funding programs. The Department of Justice alone distributed $2.396 billion dollars of assistance to law enforcement and other agencies based on formula and competitive grant requests and other programs (USDOJ, 2008).

7.6 Uniform Crime Reporting (UCR)

Most law enforcement agencies report on selected incidents and arrests to the Department of Justice through the Uniform Crime Reporting (UCR) Program. This program began in 1927 and has now grown to include about 17,000 agencies voluntarily participating. The Local Law Enforcement Block Grants, of the Department of Justice, provide formula-based funding to agencies as determined by crime rate voluntarily reported through the UCR system (USDOJ, 2008). The Edward Byrne Memorial Justice Assistance Grant, or "JAG" program, merged the Edward Byrne Memorial Grant Program with the formula-based Local Law Enforcement Block Grant (LLEBG), follows a formula for funding eligibility and distribution (USDOJ, 2011). BJS calculates the JAG award amounts based on a formula calculating allocations for states and territories based on violent crime as reported in the UCR and their census reported population.

Not all agencies report to the UCR. The information reported through the UCR, although instructions provide much detailed guidance, have room for discrepancies in local interpretation of the status of the crime and for matters such as who is able to report ownership of a statistic where multiple agencies or jurisdictions are involved. In this environment, reportable Part I UCR crimes, called "index crimes," and include: murder and non-negligent manslaughter, forcible rape, robbery, aggravated assault, burglary, larceny-theft, motor vehicle theft, and arson have value as agency statistics. One example of potential subjectivity or ambiguity in reporting is shown in the case of a motor vehicle theft, which may be recorded as a stolen vehicle (UCR Part I crime), not entered at all by the agency, or entered as Unauthorized Use of a Motor Vehicle (not a UCR Part I crime).

Where joint or overlapping investigations into crimes occur, there is not clear guidance as to who gets to report the statistics as their own (who gets the credit for the work). Optimally, the agency that solves the crime gets the statistics, which leads to competition. Anecdotally, state, county, and local agencies have raced each other to the scene of a robbery in part because robbery is a high visibility crime, UCR Part I, and usually has a high solvability rate; in short, a good "stat" or statistic to report as ones responsibility and activity. These statistics are a valuable commodity for a given agency in competing for these funds. Final amounts are distributed through individual state governments split as 60% to the state and 40% to the local agencies within the state; about $.5 billion dollars were set aside for this in 2010. This is a source for conflict over who takes the credit for incidents and arrests.

Sharing of information on things such as how to complete forms and the use of created templates or research into an area that can be used as justification in a grant proposal may not be readily shared across public safety agencies under this system of financial incentives. By helping others who do not have experience or information, they are decreasing their own chances of being selected. There is at least an incentive to keep this explicit and tacit knowledge closely held to maintain advantage for those the agency is most accountable to. A finding in the case study of the CNYICC, included in this dissertation, is that members in the consortium state that they would share all of their information with their members more readily than with those not in the consortium. Being part of a consortium encouraged members to act with a greater sense of trust and willingness to cooperate with each other. This finding was shown through that case study.

7.7 Organizational Capability

Research has emerged on organizational capability assessment for information systems development, which involved criminal justice agencies. This research identified 16 dimensions; Business Model & Architecture Readiness, Collaboration Readiness, Data Assets & Requirements, Provisions for Governance, Information Policies, Leaders & Champions, Organizational Compatibility, Performance Evaluation, Project management, Resources Management, Secure Environment, Stakeholder Identification & Engagement, Strategic Planning, Technology Acceptance, Technology Compatibility, and Technology Knowledge with associated indicators that essentially describe the readiness or success potential for information systems development in a given agency (Cresswell, Pardo, & Hassan, 2007). The dimensions identified may be further categorized as social, technical, and policy factors, in accord with the information-sharing framework described in this dissertation (see Figure 2).

8. Summary of Literature Review

This chapter provided an overview of the relevant theoretical and empirical literature, concepts and research that is pertinent to the study and understanding of information-sharing and collaboration in the public safety area. Eight major sections: introduction, definitions, research on information sharing, selected theories and concepts, social factors, technical factors, policy factors, and this summary were included. Definitions were specified for information, intelligence information, collaboration, formalization and information sharing in this context. Theories and concepts applicable to the three essays in the dissertation included: General Systems Theory, Socio-technical Systems Theory, Stakeholder Theory, Public Choice Theory, Institutional Analysis, Knowledge Management, Knowledge Networks, Cross- Boundary Information Sharing, Interorganizational Networks and included specifically Public Safety Networks. Within Social Factors, Trust, Culture, Criticality, and Quality Issues were discussed. Trust included areas of: Risk and Trust, Context, Levels, Sharing, Determinants of Trust, Legitimacy, Reciprocity, Assurance, Technology and Interorganizational Networks and Trust. Cultural factors examined included: Social Issues, Cultural Issues and Informal Networks. The last major factor section, Technical Factors, included discussion of: Interoperability (which included an example of new sharing technology options and their potential application), Availability, Control, and Technical Quality issues.

Research into understanding these factors and dynamics will lead to identification of the actionable barriers to law enforcement information sharing across the federal, tribal, state and local levels and ultimately potential solutions to the problem.

An outcome of this review and examination is the awareness of the need for further research into the factors surrounding information sharing and collaboration in public safety.

Research has been done, and is being done, that seeks to organize the problems and factors as well as create models for understanding the problem. Different aspects of the research and findings that has been done in this area are incorporated into essays of this dissertation.

III. CHAPTER - RESEARCH METHODOLOGY

1. Introduction

This exploratory dissertation collectively examines factors related to information sharing and collaboration in the law enforcement and emergency response community. This is done through the presentation of three separately prepared essays. Multiple research methodologies are used across the essays. The methodologies are described both in this section and individually in the essays themselves. This section includes discussion of grounded theory, soft systems methodology, policy analysis, interviews, Delphi technique, case studies, threats to validity, and ethical considerations. This dissertation uses multiple methods and a mixed methods approach because the focus area of this study involves law enforcement and emergency response agencies at a variety of levels and the issues and problems are complex.

The first essay involves the creation of a framework for examination and study of information sharing derived from the literature and field experience. It is exploratory and utilized to describe and frame the problem and as a means for proposing solutions to the problems identified. The second research article includes a descriptive essay examining implications for information and device sharing in the realm of emergency services where technology is controlled for such as through the use of wireless grids edgeware (or middleware). This work looks beyond the current limitations on connectivity and security so that other issues, such as social and policy factors, can be investigated absent current technological constraints. The last essay involves an exploratory case study investigating interagency collaboration and cooperation in the emergency services area involving the emergence and activities of a public safety radio consortium, the Central New York Interoperable Communications Consortium (CNYICC)

Network, a five-county collaboration involving law enforcement, public safety, government, and non-government participants. The methodology and application across the essays is shown in the figure below.

	Essay 1: A Framework for Conceptualizing Barriers to Intelligence Information Sharing in Law Enforcement: An Insider Perspective	Essay 2: Towards More Rapid and Effective Communication between Responders to Emergency Situations	Essay 3: Identifying Factors that Support Collaboration in a Multi-jurisdiction Environment: A Case Study of the Central New York Interoperable Communications Consortium
Soft Systems Method (Checkland)	✓	✓	
Grounded Theory (Glaser & Strauss)	✓	✓	✓
Literature Review	✓	✓	✓
Case Study			✓
Document Analysis	✓	✓	✓
Policy Analysis	✓	✓	✓
Field Observation	✓	✓	✓
Interview	✓	✓	✓

Figure 6: Summary of Research Methodology

The research includes activity conducted from an insider perspective. The data collected is from both public and non-public sources. Researchers' accounts here may be considered emic, including accounts from insiders and being observed by an insider. Idiographic research looks to understand a phenomenon in its own context (Franz & Robey, 1984). Idiographic and emic approaches can lead to the development of category systems by investigating a particular context (Headland, Pike, & Harris, 1990). The case study of the CNYICC has a focus on reporting the interpretation and considerations from those within the public safety culture. The factor model of the first essay and various issues identified in the second essay were derived inductively and in part from an insider perspective. The intent is not to limit findings strictly to the public safety context, but to also identify factors and recommendations that have broader impact such as to public and private entities more generally.

2. Multi-Method

To investigate the factors surrounding sharing of information within and across these sensitive organizations a multi-method approach using a research design including literature review, empirical investigation, case studies, interviews, surveys, and mixed-method studies is used. Mingers and others suggest that “research results will be richer and more reliable if different research methods, preferably from different (existing) paradigms, are routinely combined together” (Mingers, 2001, p.240; Cresswell & Plano Clark, 2007; Green, 2008). To understand information sharing and collaborative behavior in this environment, which is impacted by many variables and influences, a multi-method approach is appropriate. Using this methodology, the researcher is able to concentrate on the unique effects of the identified variables in otherwise complex causal environments. The result will provide support for and explain the analytical framework and fundamental concepts proposed within this area.

As previously indicated, this dissertation uses multiple methods for research. These include grounded theory, soft systems methodology, policy analysis, interview, Delphi technique, case study, and interview. Qualitative and quantitative research approaches are undertaken in the conceptualization, data collection and analysis phases. This approach is suggested by several mixed methodology researchers (Tashakkori & Teddlie, 1998; Creswell, 1994; Greene, Caracelli, & Graham,1989). The application of the methods used are summarized Figure 6. Methodologies used are described in greater detail in the sections following.

3. Grounded Theory

A grounded theory approach is undertaken in this dissertation to explore factors and themes surrounding information sharing in the law enforcement and emergency response community. Using this approach, data is gathered and concepts, themes, and propositions based on consideration of the data emerge and evolve throughout the study. The goals include exploration, understanding, and identification of themes, refinement of concepts, and interpretation of meaning for the area of interest (Glaser & Strauss, 1967; Lincoln & Guba, 1985; Padgett, 2004; Strauss & Corbin, 1990). Patterns or possible explanations emerge. As an investigation progresses, theory, propositions or hypotheses may be proposed and evaluated against the available facts and evidence to support or nullify them.

The information sharing framework of the first essay in this dissertation was inductively derived through a process of literature review, and included soft systems methodology, initially focused broadly on information sharing in the law enforcement and public safety communities.

In the second essay, the framework of the first essay is taken as a starting point for exploring factors related to crisis response. Social and policy related factors are explored in light of technology capability that mitigates prior concerns and barriers to sharing. Problems are explored and new ways of understanding the issues are proffered.

The case study, the third essay, used grounded theory and an inductive approach to investigate information sharing and collaboration and to describe the problems, draw attention to the prevailing dynamics in the public safety community, and propose actions that can be taken in this particular scenario.

The CNYICC case is significant in that it is representative of the situation of other law enforcement and emergency services providers across the United States and lessons learned from this case have application in other similar environments. The use of the theory and framework, investigating the technical, social, and policy aspects (Treglia & Park, 2009), allows for these essays to deliver coordinated findings across these different situations and environments and therefore provide researchers with data that can be assessed for broader impacts and more universal meanings. Methods of case study, interviews, field work, literature review, and policy analysis are utilized to thoroughly examine the problems attending information sharing in the law enforcement and emergency services realm.

Grounded theory, interview, case study, and policy analysis as research methods have characteristics not unlike criminal investigation. Patent evidence is gathered and other latent evidence or materials are uncovered through technical means, which may include forensic analysis, interview and observation techniques. These methods share the activity of sifting through the available data to interpret and understand its meaning in the context of the matter under investigation. Criminal investigation involves solving something that has actually occurred and, in a positivist way, there is a concurrent belief, therefore, in the ability to attribute the result to identifiable causative factors. It is an assumption in science research that one can identify causative factors and develop supportable theories regarding some phenomenon if the research is conducted in a cautious and rigorous way.

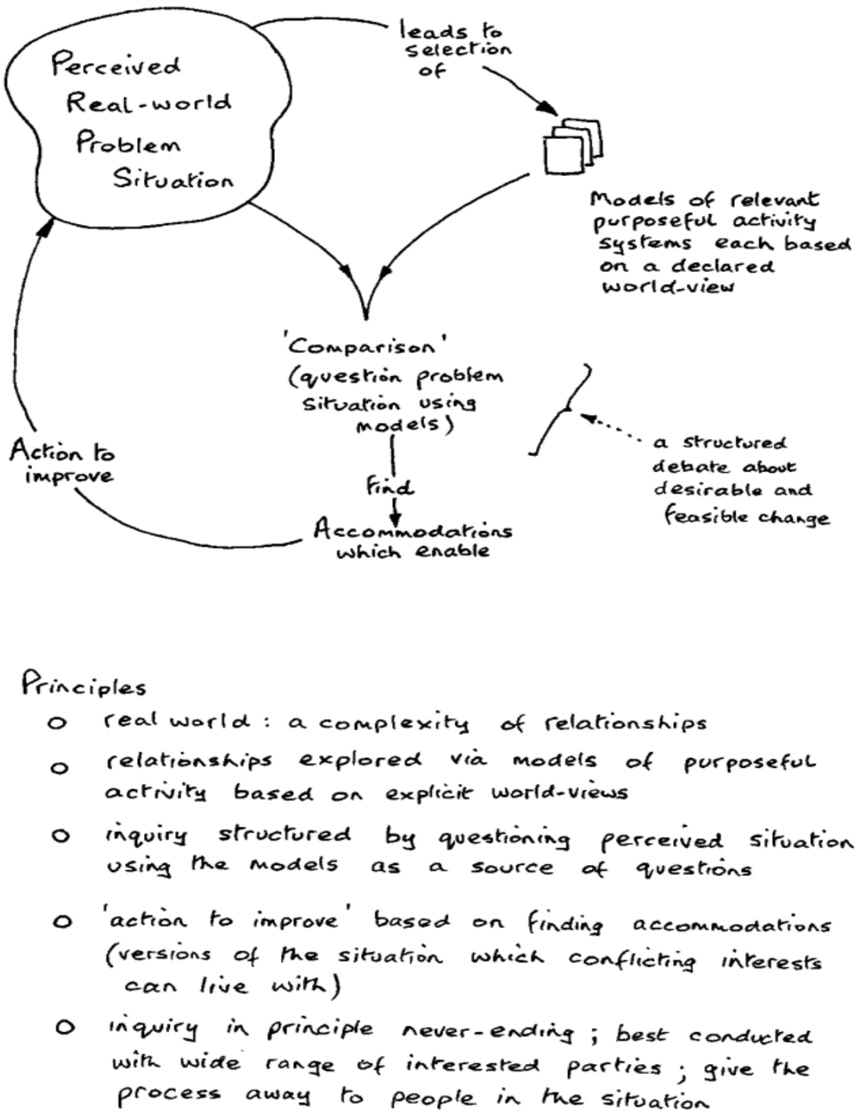
4. Soft Systems Methodology

In the Soft Systems Methodology (SSM), the main dependent construct is a problem solution and the independent construct remains context specific. Soft Systems Methodology is action-oriented and problems are categorized as being either “hard” or “soft,” with unique characteristics and distinct approaches for resolution. Hard problems are defined where the "What" and "How" can be determined in the research or system design methodology early on (Checkland, 1981). Here a solution is expected to exist and specific objectives can be defined in accordance with a positivist orientation.

Soft problems, according to this theory, contain social and political elements that make problem definition and resolution difficult. The question of "How to improve information sharing across law enforcement agencies in the U.S.?" represents a soft problem. The focus of this research involved finding what the constraints to information sharing between the federal, tribal, state, and local enforcement agencies actually are using the soft systems methodology as created by Peter Checkland (Checkland & Scholes, 1999). The soft systems methodology typically involves seven stages (Couprie, Goodbrand, Li, & Zhu, 2007):

1. Find out about the problem situation.
2. Express the problem situation through rich pictures.
3. Select how to view the situation and produce root definitions.
4. Build conceptual models of what the system must do for root definitions.
5. Compare the conceptual models with real world.
6. Identify feasible changes.
7. Recommend actions to improve the problem situation.

The figure below is a diagram of process steps and principles used in Soft Systems Theory.


Perceived Real-world Problem Situation
leads to selection of
Models of relevant purposeful activity systems each based on a declared world-view
'Comparison' (question problem situation using models)
find
Accommodations which enable
Action to improve
a structured debate about desirable and feasible change

Principles

- real world : a complexity of relationships
- relationships explored via models of purposeful activity based on explicit world-views
- inquiry structured by questioning perceived situation using the models as a source of questions
- 'action to improve' based on finding accommodations (versions of the situation which conflicting interests can live with)
- inquiry in principle never-ending ; best conducted with wide range of interested parties ; give the process away to people in the situation

Figure 7: The Inquiring/Learning Cycle of Soft Systems Theory

(Checkland, 2000)

5. Policy Analysis

Policy research is different than many of the other disciplines because it is action oriented and focuses on action-oriented recommendations to fundamental social problems. Karl Marx may have described this best in saying that “the philosophers have only interpreted the world the point is however to change it” (Cohen, 2000). Policy analysis can be divided into two major fields. Analysis of policy is seen as analytical and descriptive; it attempts to explain policies and their evolution and development. Analysis for policy making is prescriptive, involved with formulating policies and proposals such as to improve social welfare (Buhrs, 1993). Another description comes from Ann Majchrzak's book on "Methods for Policy Research." She defines policy research as "the process of conducting research on, or analysis of, a fundamental social problem to provide policymakers with pragmatic, action-oriented recommendations for alleviating the problem" (Majchrzak, 1984). The motivation in this dissertation is to inform and incite actual change.

Policy research typically begins with a social problem, such as lack of communication between law enforcement agencies; this evolves through the research process wherein alternative policy actions for alleviating the problem are developed and communicated as alternatives to policymakers (Majchrzak, 1984). Developing universal principles is more difficult using this kind of research, which is typically directed towards solving a specific problem or set of issues within a specific social and cultural environment.

Policy research is done to produce usable and implementable options for a particular social problem. In addition to the need for scientific practice, researchers must have an understanding of the policymaking arena in which the results will be utilized (Braman, 2008). The results of policy research are but one piece in the mechanism for change. Additional inputs include preconceived attitudes, existing policies, and the views and wishes of constituencies, stakeholders, other experts, superiors, and outside interests. The context of policy research consists of competing inputs, complex problems and may include seemingly irrational decision-making styles.

Eugene Bardach developed an eight-step model for policy analysis that has gained respect in the policy studies and social sciences communities (Weimer & Vining, 1992):

1. Define the Problem
2. Assemble Some Evidence
3. Construct the Alternatives
4. Select the Criteria
5. Project the Outcomes
6. Confront the Trade-offs
7. Decide
8. Tell Your Story

Bardach considers a ninth step could be to simply repeat the process as needed.

These are process steps and different models such as the eight-step model outlined above will include these activities. A common methodology is to: define the problem; establish the evaluation criteria; identify all alternatives; evaluate the alternatives, and recommend the best policy option.

Policy research and analysis can be a multidisciplinary approach and involves many types of data collection and discovery. Policy research can use qualitative and quantitative methods, including, but not limited to, interviews, critical incident, case studies, survey research, and statistical analysis. There are a variety of types of data and information developed in policy research and the choice is up to the researcher in trying to match the discipline and tools to the problem at hand.

Interpersonal and people skills of the researcher are paramount to success, as much of the work will involve working with and understanding diverse interests (Mintrom, 2003). An interesting implementation example related to this area is seen in "Privacy and Information Sharing in the War on Terrorism” (Swire, 2006). The premises offer a useful summary of the context for recent policy debates about information sharing. The author describes the support for increased information sharing and goes on to identify an Information Sharing Paradigm. The premises support expanding information sharing practices to counter terrorism.

Policy analysis is not really a research method in itself but rather, makes use of any of the methods in the sciences, which can help in explaining and solving a real-world problem. Because of this, policy analysis has the broadest application to problem solving and as such is appropriate for this case.

Public policy research typically involves complex social problems, which have, or are composed of, a number of dimensions, causes and effects at various levels. The empirical inductive approach of policy research attempts to empirically induce concepts and causal theories as the study of the social problem progresses. Referred to as empirical inductive, this contrasts with traditional scientific hypothesis testing. The policy research approach has been termed by some as the Grounded Theory approach to research (Majchrzak, 1984). Grounded Theory was first presented in Glaser and Strauss's book, The Discovery of Grounded Theory (1967) and is an inductive approach to studying social activity that tries to create theory from active and compared observations.

It is fair to say that because, in many cases, the process begins with some sort of notion about the end there is a built in bias. By looking for something, a researcher may be less likely to be open to other interpretations or possibilities. As one with experience in law enforcement, there is also a risk of personal bias influencing the research.

The purpose of this research is to identify factors, and problems, regarding information sharing in law enforcement and emergency response organizations and to provide a better understanding of them. This type of environment and problem is well suited to policy research.

6. Interview

Interviewing is a purposive process of finding out what others think and feel about their experiences. The goal is to elicit and understand the meaning of the interviewee without skewing their response. Interviewers must be exceptional conversationalists and listeners as well as possess a great deal of patience (Rubin & Rubin, 1995; Nordin, Pauleen, & Gorman, 2009).

Qualitative research, using in-depth interviews, is suited to the study of organizations (Schutt, 2004). The design is meant to promote candor and provide for a richer understanding of phenomena. This method is effective for gaining insider knowledge from a small number of individuals regarding their actual experience. Explanations have a heuristic function, “stimulating and guiding further inquiry” (Kaplan, 1998). The goal during interviews is to situate the respondents in a prior experience that is known to them which involved, for example, the potential for sharing of information. Retrospective data has been used reliably in social science research (Homey, Osgood, & Marshall, 1995). In this work, the respondents reflect on sharing and collaboration situations and activity which they were part of or personally familiar with to gain insights.

A threat to validity in qualitative interviewing involves the potential for investigator bias (Schutt, 2004). Prior experience of the researcher, here having served law enforcement for many years, would suggest a potential for bias in the collection and interpretation of data (Homey et al., 1995). This is a source for potential subjective validation, expectancy, and bias in the interview and observation process. Triangulation is a process used to verify results that increases validity by incorporating three different viewpoints or by using different research techniques (Blaikie, 1991; Homey et al., 1995). Triangulation, awareness, careful preparation and compliance with interview protocols address concerns regarding issues related to bias and validity.

7. Delphi Technique

The Delphi technique is a process that can be used to obtain a consensus of professional or expert opinion on a particular topic or issue. Linstone and Turoff (1975) define the Delphi technique as "a method for structuring a group communication process so that the process is effective in allowing a group of individuals, as a whole, to deal with a complex problem." It can be used “to correlate informed judgments on a topic spanning a wide range of disciplines” (Delbecq, Van de Ven, & Gustafson, 1975). It is a technique that is used to gather a consensus of opinion from a group of professionals, or experts, in a given area such as for law enforcement officials or emergency communication center directors.

By definition, the technique is a group process that involves interaction between the researcher and the participant experts engaging with a topic, problem, or issue. One version uses a series of questionnaires to gather data from a panel of professionals in a given area. The method may employ multiple iterations of survey, review, and comment to discover a consensus of opinion regarding the topic. The iterations each become part of the feedback process. It may involve a series of rounds where each participant contributes to the data and feeds the results back to the researcher for further examination (Dalkey & Helmer, 1963; Linstone & Turoff, 1975; Young & Jamieson, 2001).

The feedback process encourages participants to reevaluate their judgments and responses from previous submissions. Participants may see their results as well as those of the other participants. This allows for continuous reflection and refinement through the study.

8. Case Study

The Case Study method is valuable for examination of social, policy, and socio-technical factors attending information systems and user behavior. The Case Study method is a widely used method for investigating technology adoption at the organizational level (Choudrie & Dwivedi, 2005).

There is not yet one singularly adopted definition of case study. Robert Yin provides a two-part definition as: "empirical inquiry that investigates a contemporary phenomenon in depth and within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident" and that inquiry "copes with the technically distinctive situation in which there will be many more variables of interest than data points, and as one result relies on multiple sources of evidence with data needing to converge in a triangulating fashion and as another result benefits from prior development of theoretical propositions to guide data collection and analysis" (Yin, 2008, p.18).

This has relevance here. Presented below is a similar definition drawn collectively from Benbasat, Goldstein and Mead (1987), Bonoma (1985) and Stone (1978). The Case Study method examines phenomenon in the native setting, making use of multiple methods for data collection and gathering of information from one or more entities: people, group, or organization. Clear boundaries of the phenomenon are not necessarily apparent in the early stages of the research. Experimental controls and manipulation are not used. The figure below summarizes key elements of case studies (Benbasat, Goldstein, & Mead, 1987; Cater-Steel & Al-Hakim, 2009, pp. 17-18).

- Phenomenon is examined in a natural setting.
- Data are collected by multiple means.
- One or few entities (person, group or organization) are examined.
- The complexity of the unit is studied intensively.
- Case studies are more suitable for the exploration, classification and hypothesis development stages of the knowledge building process; the investigator should have a receptive attitude towards exploration.
- No experimental controls or manipulation are involved.
- The investigator may not specify the set of independent and dependent variables in advance.
- The results derived depend heavily on the integrative powers of the investigator.
- Changes in site selection and data collection methods could take place as the investigator develops new propositions or hypotheses.
- Case research is useful in the study of "why" and "how" question because these deal with operational links to be traced over time rather than with frequency or incidence.
- The focus is on contemporary events.

Figure 8: Case Study Elements

Other important considerations involve such things as case or site selection, single-case versus multiple-case designs, saturation, and representativeness (Benbasat et al., 1987). Means for data collection here involve interviews, documentation, archival records, direct observation, and physical artifacts. The goal here is to obtain the richest data surrounding the research issue and to capture the complexity in context (Benbasat et al., 1987). Site selection is important. The case should have potential to yield rich and informative data. Having the ability to gain research access to a site, resources or community, is critical (Kaarst-Brown & Guzman, 2008). The researcher here is a public safety insider with access to insider information and contacts.

The CNYICC was chosen for this study because it has relevance to the current problems of coordination and interoperability for law enforcement and emergency responders, and it is representative of a critical case in this field. Strategies to identify use cases include processes of random or information oriented selection purpose (Flyvbjerg, 2006). In this case to maximize the utility of data gathered from a case, the CNYICC case was chosen based on an expectation that there is rich content available here that relates to other similar activities and broader impacts. Technical, social, and policy aspects of this collaboration are investigated and include trust considerations. Strategies for selecting samples and cases vary and what seems to fit this situation, looking at law enforcement and emergency response collaboration in communications, is not a random or stratified sample model.   An information-oriented focus with the consortium existing as a critical case is the aim. The purpose for an information-oriented focus is to maximize the utility of information from small samples and single cases based on expectations about the potential information content. In this case, the expectation is to achieve information that permits logical deductions, which fits the critical case definition clearly. The case study of the consortium is not the most or least likely case but rather a critical case that has important elements that include the disparity of partnerships that are brought together, the range of agencies that are involved, and the stage in development that this particular consortium is acting in where tremendous change in telecommunications policy, practice, and technology, for emergency responders is under way. This case involves federal, state, local, tribal, non-governmental and other participants as well as being a typical case where interoperability prior to this time was not achieved, tensions between and across agencies existed, and where lack of cooperation between agencies was the case– similar to other places across the nation and in other countries. This case stands out as well because the group appears to be successful and well organized. One expects to learn and share what is valuable and successful in these collaborations through this process.

Analysis of case study data depends heavily upon the skill of the researcher in identifying, collating, and integrating this data. This is certainly an area where there is potential for bias. Bent Flyvbjerg identifies five misunderstandings regarding case studies and includes "a bias toward verification" as one of these (Flyvbjerg, 2006). He goes on to assert that:

> "The case study contains no greater bias toward verification of the researcher’s preconceived notions than other methods of inquiry. On the contrary, experience indicates that the case study contains a greater bias toward falsification of preconceived notions than toward verification." (Flyvbjerg, 2006, p.237)

Triangulation is a means for validating data and reducing potential effects of bias. Triangulation involves getting several measures and indicators to reference and compare. In the case study of the CNYICC, there is a rich body of data related to the formation and activities of the consortium and participants available publicly. This data comes in the form of legislative action from municipalities, media reports on the consortia and its activities in the press and online, public hearings and minutes of consortium committee meetings, agency annual and/or progress reports and internal memoranda (some of which is not publicly available). The investigator validated what was relayed in interviews with observed events and actions. Interview results were triangulated using information gained by comparison with other interviewees of the consortium. As a further check on the soundness of both the investigators’ interpretation and documentation of the collected data, interviewees were asked to provide direct feedback. The preliminary findings were presented to the consortium core members in writing and in person for comment before being finalized. Results and conclusions were developed following a great deal of introspection and consideration of the data/evidence in its particular context.

Having contacts in the law enforcement and emergency response community facilitated access to these organizations. This relationship was helpful for access but created a situation of potential bias. This potential was addressed as described in the section above. Additionally, several authors who have conducted case studies report that they revised their original hypothesis on essential points as a result of the study and report that their own assumptions, initial views, and conceptualizations were inaccurate (Campbell (1975), Ragin (1994), Geertz (1995), Flyvbjerg (1998, 2001). It is possible for researchers to report on data and findings in an objective way.

The case study plan called for a census of CNYICC members. As there are fewer than 30 members, it was possible to interview all. As the research progressed, other persons such as vendors, prior members and other stakeholders were considered for adding to this study. That decision was based on information derived through the interviews, observations, and document analysis. Assessment was also made as to whether or not the additional sources would be important to the robustness of the study. This would include considerations of the potential value of findings for the research, academic and professional communities. The study continued on until it was felt that saturation was achieved and there was no new information or questions developed. This decision was made in consultation with committee members. Substantive changes in the research process would have been submitted as a requested amendment to the current Institutional Review Board (IRB) research study authorization. In this case there were none.

9. Threats to Validity

Threats to validity in this dissertation research were acknowledged and addressed in a number of ways. As a multi-method and multi-part activity, the different means for addressing issues of validity varied by study. These are described further below.

A good approach to investigating the problem of identification of organizational barriers to information sharing between law enforcement agencies in the United States at federal, state, and local levels involves a mixed methodology. Methods used in this dissertation include case study with in-depth qualitative interviews that include following up with survey elements using a Dephi technique. The in-depth interviews involved one-on-one, researcher-to-person discussion. This form of close interaction can lead to increased insight into people's thoughts, feelings, and behavior on critical and important issues. Interviews were semi-structured and permitted the interviewer to encourage respondents to talk at greater length about the problem of interest and to allow for elicitation of unanticipated information. The Delphi technique is a flexible approach, which aims to allow individuals to explain reasons underlying a problem or practice in this case within their organization. The technique is used for gathering people’s ideas to then use as a basis for further processing across other respondents in similar positions. This process and strategy was used here to investigate the phenomenon within its real-life, work place, and context.

For interviews, a potential weakness is that the interviewer may disturb the process. The interviewer must not influence the respondent by suggesting through body language or by asking leading questions. Respondents may offer guarded responses. There is, however, an expectation that people will be able to accurately relate their motivations, intentions, and experiences to bring light to the problem. Another weakness would be that the range of possible responses or the direction that the interviews take could lead the researchers in too many directions to be of value. The researcher here runs the risk of getting data and information that may not address the problem at hand and of getting a great deal of data that is of questionable value. These concerns were addressed through having an established interview protocol that was both structured and flexible. The researcher conducting the interviews has many years of interview experience. The experience of the investigator was also a mitigating factor to threats to validity in this part of the study.

Another threat to validity in the interview and data analysis process involved the potential for investigator bias (Weiss, 2004). The researcher here had prior experience in public safety and the potential for observing things in a preconceived way had to be accounted for (Diesing, 1992). Awareness of this, engaging with other researchers, and having input and direct feedback from the participants (member checking) reduced this effect. This was a source for potential subjective validation, expectancy, and bias in the data interpretation and observation process. The established interview protocol was used with all participants for guidance and consistency.

Bias in the participant selection process for the case study of the CNYICC was reduced, as there was 100% participation of the core consortium membership.

A concern is that some respondents may not complete the process. In the CNYICC case study, one of the core members was unavailable during a portion of the Delphi technique survey where responses were reviewed and ranked. This member reviewed and accepted the responses and rankings after the others had already completed this. No additional changes were made.

The threat that there may be contamination with others participating in the study would not necessarily have adverse impacts. Networking by the participants was allowed. If respondents choose to discuss the study with each other that was fine because, in real life, they may or may not choose to do so.

10. Ethical Considerations

This dissertation seeks to achieve a better understanding of the impacts and mechanisms underlying and driving interactions across organizations by people. Having a solid framework and understanding of the way that trust is established and maintained can be a tool. Understanding the establishment and creation mechanisms of trust can help society and institutions to work better together, build greater relationships, and improve knowledge and systems that make everyone better. Unfortunately, knowledge of interaction mechanisms as a skill or tool may be used to manipulate trust or create deception in interactions, negotiations and other activities for illegitimate purposes as well.

In terms of the framework, Figure 2, these considerations are primarily social factors. People create standards and interpret ethical behaviors, and these are reflected in the policy created as well as through actions and conduct of those in the organization interpreting these policies. The technology can add to controls or inhibitors to providing an environment that fosters certain types of activity or at least establishes accountability. At the heart of the issue are the people who create it within the organization.

Sharing and interconnection can make entities vulnerable. A disconcerting aspect of the research here on information sharing is that it may be providing information that could be used by persons in illegitimate ways. One could conceivably use a thorough knowledge of the trust process to their advantage. As part of the research, understanding the establishment of mechanisms of trust between entities and individuals considerations such as this must be attendant. If one follows the belief that people benefit most from having complete information in interactions, it would stand as an argument towards full disclosure and sharing of all the tools in a negotiation or information sharing interaction.

The considerations and dynamics involved in sharing trusted information between parties parallels considerations made in other negotiation environments such as international relations and domestic violence incidents. In the case of international relations, nations often negotiate with a "speak softly and carry a big stick" style. In that environment, the parties involved are sometimes at an unequal power level and the side with less capability to defend or attack is at a disadvantage and subject to feeling coercive pressure. Trust in this case is difficult, as the parties are not interacting in a balanced or safe environment. Agreements made where one party has power over another are by their very nature coercive, and so the true wishes of the parties may not be reflected in these cases. The weaker party may formally agree but later take actions in opposition to the agreement because of this discord. As an example, the United States has nuclear capability and other means to compel compliance relative to its interaction with other countries. For a negotiation to be balanced here, the other nation involved would have to have equivalent capability to have a fair negotiation. The belief here is that trust in decisions that are made is more valid where parties have mutual destructive capability. This is a debatable point, however. Where the intent is to have two parties seek out mutually agreeable outcomes that do not involve damaging something, the possibility of violence or use of force cannot be an option. In the range of possible outcomes there cannot be one that involves harm. In this way, there is not coercion but mutual interest in beneficial outcomes and the resulting agreements will be in line with the actual motives and interests of each of the parties involved. The results of negotiation under these conditions have the greatest potential to be acted upon as described by the actors.

A good example of how mutual destructive capability does not promote truthful agreements in communication and negotiation situations can be seen in family domestic violence situations. Police are often called in to intervene in domestic violence cases. In many of these cases, one spouse or party has considerably more weapons at their disposal than the other party; these may include: physical size, weapons, control over assets, or other options for alternate living arrangements. Police are trained to equalize the power between parties so they can facilitate truthful and earnest discussion and negotiation to resolve the issue. Police do not provide weapons to each of the parties to create this balance but instead seek to remove the weapons and create an environment that is free from coercive elements. This follows a belief that for truthful and earnest negotiation and information exchange, there must be a safe environment for all parties involved. This concept is consistent from international to personal levels regarding trusted information sharing.

Having a better understanding of trust itself is not the same as having additional coercive tools in an interaction. In regard to trusted information sharing, the notion of coercive capability is something that influences the trust between parties and the ultimate decisions that are made. Trust is not used as a coercive weapon, but it can be used in a manipulative or subversive way. Having knowledge of the way trust is developed and expressed can provide a party to an encounter with tools to create false trust to advance their own objectives. An example from World War II depicts this process. The bombing of the United States-owned Pearl Harbor by Japan in 1941 is well known. Japan has a proud and respected culture of integrity and this and many other countries have evolved and gone through periods of conflict as well; the selection of this case from the past is but one of many available. In that case, the Japanese government was negotiating with the United States government regarding establishing peace at the same time as they were preparing for the surprise attack. The image of trust can be used for subversive purposes. One could consider that if the Japanese government did not have capability to use force, the negotiations would have had an alternative outcome. Greater understanding of trust also provides tools for evaluating trust as well as identifying the mere portrayal of trust. In the case of Pearl Harbor, the United States would have been well served by tools for interpreting the portrayal of trust by the Japanese government such that they would have been in a better position to assess whether or not there was actual trust or merely the appearance of trust.

Greater knowledge of what creates trust may be used to gain unfair advantage in an exchange, but the likelihood of this is reduced where all parties have the most complete understanding of true trust measures and behavior. In short, it will be harder to deceive or “fake it.” There are many elements that go into creating and evidencing trust and they involve things that are malleable as well as things that are hard or impossible to manipulate.   A party can profess policy and take some actions that are in line with what is understood to be trustful behavior, but it is not possible to change something like recent history of conflicting behaviors. Having greater information can provide more accurate assessments and improve decision making.

Fundamentally, this research proceeds on the assumption that having a greater understanding of trusted information sharing between individuals and organizations is beneficial to the greater society.

IV. CHAPTER - ESSAYS

ESSAY 1: A Framework for Conceptualizing Barriers to Intelligence Information Sharing in Law Enforcement: An Insider Perspective[6]

1. Introduction

The term “information sharing” in law enforcement gained popularity as a result of the 9/11 Commission Hearings and report of the United States government's lack of response to information that was known about planned terrorist attacks on the New York City World Trade Towers prior to the events. This led to the enactment of several executive orders by President George W. Bush mandating agencies implement policies to "share information" across organizational boundaries (United States, 2007c). Information generally, and intelligence information, were included in this broad mandate. Intelligence information sharing is the transfer of tangible or articulable facts or data obtained that relate to an actual or impending occurrence of a criminal or terrorist act. It includes suspicious activity reports regarding incidents or observations which are of a less obvious nature, but which may be supportive or related to criminal or terrorist related activity.

An incident or activity of suspicious nature or that is outside of the norm for a particular environment and circumstance could be considered suspicious activity or intelligence information depending upon the circumstances. The adjudication as to whether an event is considered and captured as suspicious activity or intelligence is subjective and left to the discretion of the officer involved in the report or observation. Where a person of average intelligence and familiarity with the normative environment would believe an act may be a part

[6] This is an expanded version of the original article: Treglia, J. V., & Park, J. S. (2009). “Towards trusted intelligence information sharing.” In Proceedings of the ACM SIGKDD Workshop on CyberSecurity and Intelligence Informatics. Paris, France: ACM. (pp. 45-52).

of the cause or furtherance of a criminal act, it would qualify as intelligence information. An example may be helpful here; a person taking pictures of trains in a train yard may not cause someone familiar with the area to be concerned. Many people collect, model, and photograph trains. However, if one adds to this scenario: 1) the person is not from the surrounding area; 2) the person is taking photos of trains and the facilities; 3) the person becomes agitated when asked about her/his purpose; 4) the person provides inaccurate information about where they are from or inconsistent versions of what they are doing, then perhaps the person is affiliated with a terrorist group or may have criminal intentions. This all may bring the incident to the level of a reportable incident, or suspicious activity report, which would become intelligence information to be shared among enforcement agencies. The combination of activity and circumstance is the trigger. This will also be referred to as intelligence information or intelligence. It is yet another problem, worthy of study, to identify the means by which various agencies collect and manage this type of information.

While millions of dollars have been invested in information technologies to improve information sharing capabilities among all law enforcement agencies, according to the National Security Agency (NSA), there remains a hesitation to share intelligence information between agencies (Lieberman, 2007). Information technologies for the future should provide for ubiquitous and distributed computing and communication systems that deliver transparent and high quality service, without disruption, and while enabling and preserving privacy, security, trust, participation, and cooperation. This paper identifies barriers affecting effective intelligence information sharing between federal, tribal, state, and local law enforcement agencies in the United States. An information-sharing framework is proposed that identifies three major factor areas that impact upon sharing: social, technical, and policy. The paper then provides an application of this categorization in considering an instance of agency information sharing using data from a national survey of criminal justice agencies. It is argued that researching these dynamics will lead to improved understanding of the problems and factors and ultimately to identification of actionable solutions to law enforcement intelligence information sharing across the federal, tribal, state, and local levels.

2. Research Methodology

This article is the result of exploratory research aimed at identifying and defining problems in information sharing in the law enforcement and emergency response community. It is provided from an insider perspective. A researcher involved in this work was also an active member of the law enforcement community. A grounded theory approach and soft systems methodology was undertaken. The overall goal was to identify and refine major themes and concepts in this area and to create a framework for understanding the problems and factors. Using this approach, data was gathered and concepts, themes, and propositions based on consideration of the data emerged and evolved throughout the study.

Goals included exploration, understanding, and identification of themes, refinement of concepts, and interpretation of meaning (Glaser & Strauss, 1967; Lincoln & Guba, 1985; Padgett, 2004; Strauss & Corbin, 1990). A literature review– including primary sources of public data such as research reports, congressional testimony, agency after action reports, academic and professional literature– was conducted.

The data included in the analysis was taken from works primarily from 1995 through 2010. This period contained research and policy both before and after the September 11, 2001 (9/11) attacks in the U.S. That incident arguably had a significant impact on emergency response policy and practice and so covering this period is significant to researchers.

Proprietary data from internal resources, such as internal memos and after action incident reports, were considered. Field observations and interviews with public safety personnel were also included in preparation of this article.[7] Through this process, patterns and potential explanations are uncovered. Over the course of the progression of the investigation, theory and propositions were suggested and evaluated against the available facts and evidence.

The approach taken in gathering and reviewing the available data and literature involved a three-step process with feedback in between. The steps, consistent with recommendations of Webster and Watson (2002) included: 1) Identification of major authoritative sources and initial review; 2) expansion out through a snowball effect from the citations and references of the initial review; and 3) Making use of professional, academic, and public search engines for related resources.

Several search sources and key words were used to gather data. Leading journals in information systems, management, and public administration were targeted for searching. These included Communications of the ACM, MIS Quarterly, Academy of Management Review, Public Administration Review, Journal of Public Administration, Government Information Quarterly and others such as Information Polity. Proprietary resources included the FBI Research Library online and LEO (Law Enforcement Online) resources. Online searches included Elsevier’s Science Direct and Scopus, individual searches within the targeted journals, and online public searches including Google Scholar and Google Web Search. Terms used for searching included “information sharing”, “intelligence”, “collaboration”, “knowledge sharing”,

[7] Field observations were based on the researchers participation as a member of several local law enforcement agencies in New York State from 1982 – 2012. Agencies included: Onondaga and Madison County Sheriff’s Departments, Onondaga County Corrections, Manlius town, Fayetteville village court, Chittenango and Oriskany village police departments. Through this affiliation the researcher had professional contact with Federal, State and Local agencies to include FBI, Secret Service, DEA, BATF, INS, Coast Guard, Customs and Border Patrol, and others as well as regular contact with various fire, ambulance, 911 center personnel, primarily in New York State.

and “data sharing”. Qualifiers for searches included words such as “law enforcement”, “public safety”, “government”, “criminal justice”, “emergency response”, ‘emergency services”, “public administration” and “management”. The review and data gathering was completed when there seemed to be no new conceptualizations for the categories emerging from the various sources.

Information gathered was discussed with fellow university researchers and practitioners in the field to validate that it was contributing to understanding the problem, that it was valid and of sufficient quality.

Identified problems and recurrent themes related to information sharing were grouped into distinct areas or factors; Technical, Social, and Policy. The factors influence information sharing individually and collectively. The factors both affect and are affected by each other. The information-sharing framework proffered in this article was inductively derived from a broad initial focus on information sharing in the law enforcement and public safety communities. This framework is consistent with elements of Socio-Technical Systems (STS) and General Systems Theory (GST), as described in the sections following. Important elements include such concepts as the interdependence of the relationships between and across entities. An organizational system described from this perspective is comprised of interrelated interacting parts and relationships that cannot be correctly described absent its relationship to the whole or larger environment that they operate in (Von Bertalanffy, 1972).

Systems models from the business and management fields also shaped the selection and formation of the three factor categories. Information systems in business and organizational studies typically identify information systems as being comprised of people, procedures, data, software, telecommunications, databases, and hardware that are utilized in combination to support a business purpose (Stair & Reynolds, 2011; O’Brien & Marakas, 2008). Additional sources from Operations management and information systems similarly identify these or related categories for system components such as plants, equipment, control procedures, and policies (Lewis & Slack, 2003; Gupta, 2000). The various schemas for categorizing components were considered in consultation with fellow researchers and practitioners and ultimately the three factors of Social, Technical, and Policy were determined to be inclusive of all system components and descriptive enough to provide for understanding and examination of information sharing systems and processes in the public safety realm.

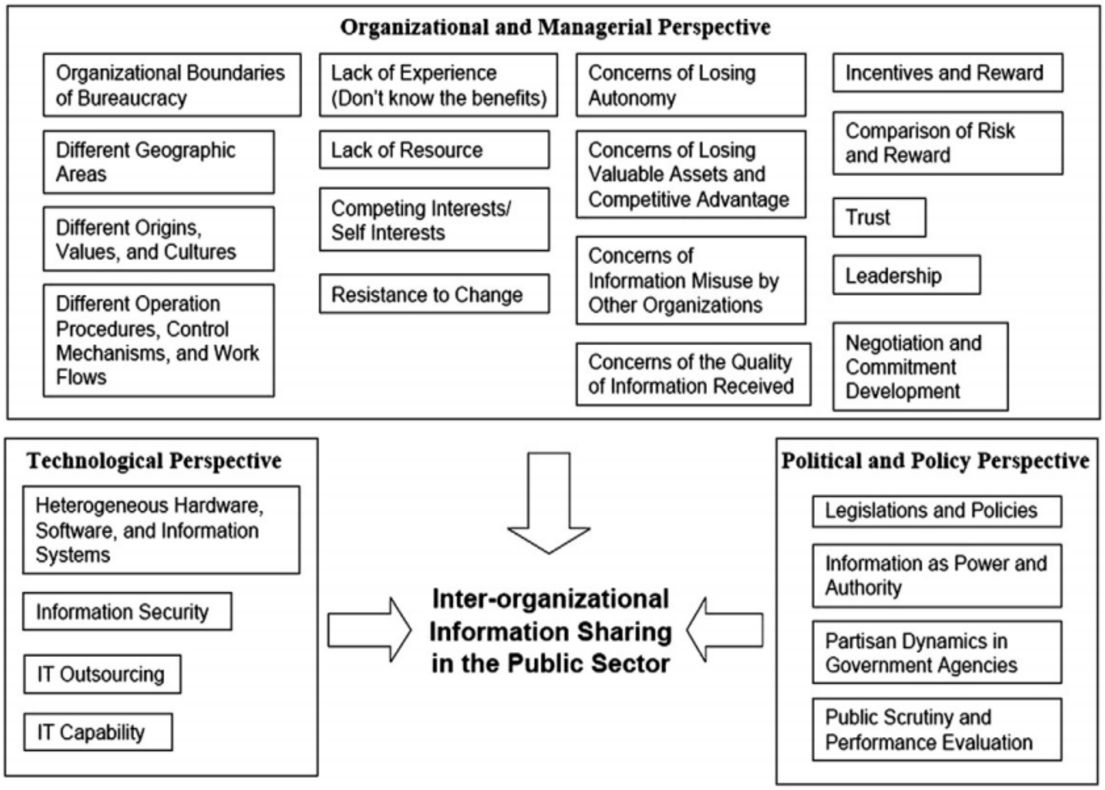

Organizational and Managerial Perspective
Organizational Boundaries of Bureaucracy
Different Geographic Areas
Different Origins, Values, and Cultures
Different Operation Procedures, Control Mechanisms, and Work Flows
Lack of Experience (Don't know the benefits)
Lack of Resource
Competing Interests/ Self Interests
Resistance to Change
Concerns of Losing Autonomy
Concerns of Losing Valuable Assets and Competitive Advantage
Concerns of Information Misuse by Other Organizations
Concerns of the Quality of Information Received
Incentives and Reward
Comparison of Risk and Reward
Trust
Leadership
Negotiation and Commitment Development
Technological Perspective
Heterogeneous Hardware, Software, and Information Systems
Information Security
IT Outsourcing
IT Capability
Inter-organizational Information Sharing in the Public Sector
Political and Policy Perspective
Legislations and Policies
Information as Power and Authority
Partisan Dynamics in Government Agencies
Public Scrutiny and Performance Evaluation

Figure 9: Public Sector Inter-Organizational Information Sharing Factors

(Yang & Maxwell, 2011)

Interestingly other researchers have separately proposed similar structures for considering factors in public sector information sharing. Interagency information sharing research by Dawes (1996) and research on knowledge sharing in e-Government by Zhang et al. (2005) identify three primary influential factors as technology, management and policy. These are constructively similar to the framework created and presented in this research; technical, social, and policy). Yang and Maxwell (2011) have since proposed that three identified perspectives (Technological, Organizational and Managerial, and Political and Policy) influence public sector information sharing and they created a model using the three perspectives. The perspectives and factors influencing inter-organizational information sharing in the public sector are shown in the Figure 9 above.

The rationale and descriptions of these frameworks and models are provided in detail in the pages following with cognitive maps depicting the concepts, elements, and interrelationships.

3. Literature and Related Work

Information sharing is defined as "making information available to participants (people, processes, or systems)" (USDOD, 2007). The leveraging of information by entities involved is included in this broad, yet simple, conceptualization. Information sharing has been defined in the public sector as "exchanging or otherwise giving other agencies access to information" (Zheng, 2009, p.27). Researchers note that information sharing refers to both tacit knowledge and to explicit artifacts and codifiable information (Yang & Maxwell, 2011). In the business field, information sharing is defined as "the extent to which the supplier openly shares information about the future that may be useful to the customer relationship" (Cannon & Homburg, 2001). This information value potential is paralleled in public safety where agencies share information to solve a case or apply for funding opportunities. Information sharing is also defined as the degree to which partners proactively provide critical and confidential information to each other (Phan, Styles, & Patterson, 2005). This means that information is provided without one side having to ask for that, which may be useful to have.

There is limited work available that focuses on interagency intelligence information sharing factors in the law enforcement sector.

Studies done in agencies outside the United States include Glomseth et al., (2007) and Jing and Pengzhu (2007). Glomseth found that intelligence information sharing in police investigations was affected by the extent of team culture. Team culture was identified as being a dimension of the agency occupational culture. Jing and Pengzhu studied agencies in China with responsibility for identifying unlawful business activity. Their findings included that having inconsistent policy hinders government-to-government information sharing.

Recent case studies confirm information sharing difficulties across agencies. The unwritten rules for behavior in organizations may restrict or encourage information sharing between agencies (Pardo, Cresswell, Thompson, & Zhang, 2006). Some studies done in the United States involved looking at difficulties with agencies sharing information across the same levels (Pardo et al., 2006). Organizational culture within the agencies was found to influence sharing there. In another study, four types of systems (social, constituency, technical, and organizational) were found to influence information-sharing processes within and across agencies (Drake et al., 2004). Effective solutions for the issues have yet to be identified.

Inter-organizational systems studied by management information systems researchers have primarily focused on the private sector and do not directly apply to the government sector (Lai & Mahapatra, 1997). Preliminary work involved an exploration of conditions for cooperation between emergency management agencies where perceived information assurance of others and information-sharing standards were more strongly related to information sharing than were cultural norms, in emergency contexts (Lee & Rao, 2007). Research on emergency services reported that technical environments, such as other agencies' information assurance level and technical standards, seemed to encourage information sharing systems use.

There is initial work on cultural influences on information sharing behaviors in the public sector (Luna-Reyes, Andersen, Richardson, Pardo, & Cresswell, 2007). There is recent work on organizational capability assessment for information systems development, which involved criminal justice agencies and included cultural considerations and system complexity issues (Cresswell, Pardo, & Hassan, 2007). Crisis response systems are “complex” systems as they have interdependencies among numerous parts and variables interacting simultaneously (Longstaff, 2003, p. 2013).

Public administration authors concentrate, much of the time, on the structures and delivery of services from public organizations from a variety of perspectives. These works aim to assist public administrators to be more aware of the internal structure which they are intimately part of and of the structures and influences that they may encounter in their external environments.

Charles Handy, a recognized British management writer, classified organizational culture by the power of the roles and functions taken on by individuals within organizations (Handy, 1976). Culturally, organizations are not homogeneous, being consisted of multiple and competing forces. They tend to subdivide into groups, each with the ability to subdivide into further subgroups based on those who compose them. Handy argues here that in order for managers to be successful within a given organization or environment, the manager must be first keenly aware of the different organizational cultures that exist within the organization (Handy, 1976; Handy, 1996). Once aware of these different cultures that are present in the organization, the manger may be effective as a liaison between the different cultures, and improve the chances for influencing processes and norms.

Central to the test will be what works. "Public value" in information sharing and service provision is delivered where management is managing the external authorizing environment and engaging more innovatively with the public to be served (Moore, 1995). While having a voice is seen as a central element in assessment of public value, it is not the only element and one should be wary of an overly ideological interpretation of just one aspect of what is a more involved and complex model.

According to Sparrow, Moore, and Kennedy, law enforcement "has a chance to forge new attitudes of mind and structures of relationships that will help it produce high-quality solutions to society's problems - not just one problem but many problems; not just now but in the future" (Sparrow, Moore, & Kennedy, 1992). Emergency response is added to this as well. In accord with this Longstaff, Armstrong, Perrin, Parker, & Hidek, provide a conceptual framework for assessing community resilience[8] that includes: ecological, economic, physical infrastructure, civil society, and governance subsystems (2010). This is a truly more holistic, systems oriented, picture of the prospects for crisis response and, it is argued here, information sharing processes. Further examination of the influence of perception of technological factors, culture, trust, and legal or policy factors in the law enforcement, emergency response and public sector context is necessary.

4. Framework - Key Influences on Information Sharing

In order to enhance the current intelligence information-sharing services between government entities researchers created a conceptual framework comprised of three major

[8] Resilience as used here is consistent with the definition used by the multi-disciplinary Resilience Alliance: "*the capacity of a system to absorb disturbance, undergo change, and retain the same essential functions, structure, identity, and feedbacks*" (Longstaff, et al., 2010, p. 3).

areas of influence: Technical, Social, and Policy, (this is depicted and summarized in Figure 10 below) through previous research work (Treglia & Park, 2009).

Key Influences on Trusted Information Sharing

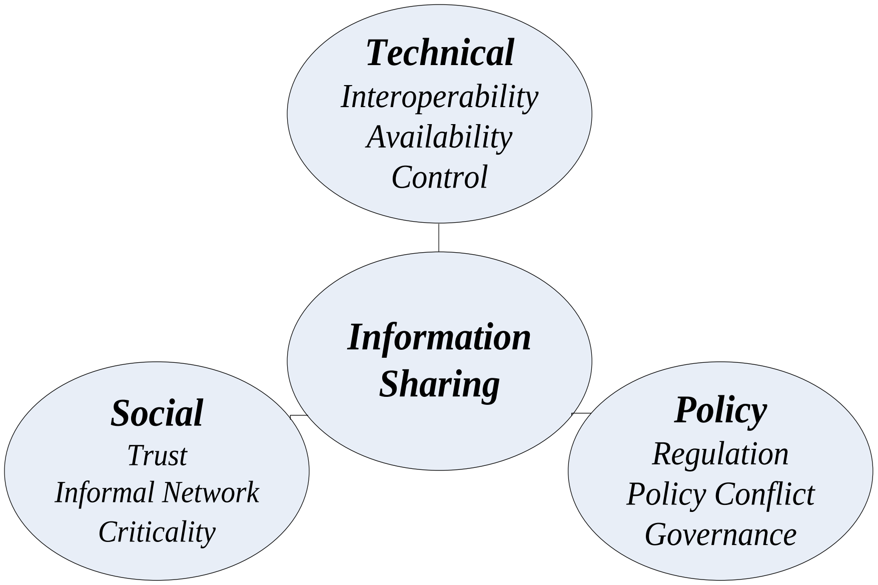


Figure 10: Information Sharing Framework

In this paper the preliminary framework, model and theory of intelligence information sharing are developed through a literature review, experience, and interviews with practitioners in the field. The framework and model is also tested using national survey data. Within each area, individual factors are identified and discussed that play roles in influencing whether or not intelligence information is ultimately shared.

4.1 Technical Influences

4.1.1 Interoperability

The interoperability of information systems and the data elements captured and used was found to be a problematic issue. Tools such as Extensible Markup Language (XML) are widely used in business development of Web services and for Business to Business (B2B) integration and data exchange (Fernández-Medina & Yagüe, 2008; Lampathaki, Mouzakitis, Gionis, Charalabidis, & Askounis, 2009). Although 82% of non-federal law enforcement agencies in the United States use computers for internet access, unified standards for information systems have not been universally accepted by law enforcement entities (USDOJ BJS, 2006). This has led to hardware, software and network inconsistencies, and incompatibility (Chau, Atababhsh, Zeng, & Chen, 2002; United States, 2007b). Interoperability is also related to the definition of fields and data descriptions. With more than 19,000 law enforcement agencies in the United States, each having its own systems and hierarchy, it is no wonder there are issues with compatibility between agencies and systems when you try and collaborate or interconnect (BJS, 2007). As a matter of fact, there are many different information systems currently being used by law enforcement agencies for data management and communication, such as COPLINK, OneDOJ, N-DEx, ALECS, LInX and others (Bulman, 2008; Chen, Zeng, Atabakhsh, Wyzga, & Schroeder, 2003; McKay, 2008).

Furthermore, the inconsistency in regulations hinders trust between agencies. For instance, there are no broadly accepted standards for security clearances and subsequent access across agencies. The federal government has a lengthy process for approving access to intelligence information and there is no provision to readily accept security clearances from other federal or non-federal agencies (Whitehouse, 2007). A state police officer with secret clearance in his agency does not carry this standard or designation with other local or federal agencies. Security clearances even across federal agencies do not automatically transfer and must be reevaluated and reassessed by the individual agency. A justifiable concern is that there are not universal standards for hiring and background checks across the various agencies. The process used to verify a person's credibility in a given agency may not be adequate for a certain level of secure access at another agency. This is a tremendous obstacle to sharing information among agencies and feeds into a perception of mistrust across agencies. This is an area which can be addressed through legislative changes and changes to internal agency processes.

4.1.2 Availability

Availability means that the systems must respond in a timely manner (Zargar, Weiss, Caicedo, & Joshi, 2009). These systems must have a high degree of survivability and function in mission critical environments where parts of the network may be compromised but accurate service must be continued (Park, Chandramohan, Suresh, & Giordano, 2009; Schooley, 2007). For instance, network availability impacts acceptance and use of systems (Chan & Teo, 2007; Koroma, Li, & Kazakos, 2003). Furthermore, information must be kept up to date and in accordance with the users' interests and needs. For the new systems to integrate with the varieties of technology and protocols that are used, the complexity of processing and connections are increased and system performance and reliability become taxed. Systems become more prone to delays or failures as they must incorporate legacy and other protocols into their core programming and functions. Increases in overhead for security also add to the workload and increases the potential for system delays or failure. Systems considered slow or non-responsive according to the expectations of the users will have a hard time being adopted.

4.1.3 Control

Control as perceived by the users is required for information sharing and systems adoption. Information-sharing systems must be capable of controlling, monitoring, and managing all usage and dissemination of intelligence information for tracking purposes to provide assurance, which is required for trust (Li, Hess, & Valacich, 2008). There is no broadly accepted set of minimum security and access control standards and protocols for intelligence information systems that have been uniformly adopted for use across federal, tribal, state and local agencies (Cresswell, Pardo, & Hassan, 2007). Distributed workflow control tasks in these integrated and grid environments may increase the level of information sharing, availability, cost effectiveness, but, on the flip side, they also increase the complexity and control problems (Serra da Cruz, Chirigati, Dahis, Campos, & Mattoso, 2008; Park, Kang, & Froscher, 2001). Therefore, provenance and user control tasks and capabilities must be suitable to these varied environs in a trusted information-sharing system.

4.2 Social Influences

4.2.1 Trust

Trust is a key influencer of sharing behavior. Here trust refers to the degree in which the person with intelligence information may accurately predict the action that will be taken by other people in other agencies who may receive information or have access to it. Trust has been identified as an area of concern in much of the information systems and management research.[9]

[9] Trust research considered in information systems and management includes: Gao, 2005; Humenn, Chin, Kosiyatrakul, Older & Northrup, 2004; Jing & Pengzhu, 2007; Koufaris & Hampton-Sosa, 2004; Lee, 2006; Lee,

Recent work that addresses different aspects of trust in business and government interactions points to trust as having a greater influence than was previously typically accepted (Booth & Wheeler, 2007; Colquitt et al., 2007; Gerdes, 2010; Morris, Tanner, & D'Alessandro, 2010; Staples & Webster, 2008; Venezia, 2010). In these publications, trust is identified as a factor that is considered in the process of sharing information. Trust is also identified as a critical element for collaborative work, especially in information technology development projects, where it was determined to depend on the rate of knowledge sharing among those involved (Luna-Reyes et al., 2008). Fear of information technology may interfere with trust in systems (Kaarst-Brown & Robey, 1999).

Trust occurs at the individual and organizational level. It includes other law enforcement officers and extends to the other staff or persons who may gain access to information were it made available to them and assumes that there is a means for sharing this information (Scott, 2006). Individual agencies may handle information security differently. One agency may require a higher standard than another and not share information based on that. Corruption in a given agency may occur and at any level (Ivkovic & Shelley, 2005). The person responsible to share intelligence information may have personal knowledge of individual employees who they do not trust or a general impression or bias, correct or not, of the security within the agency in general terms. The concern is complex as it can be at the agency or individual level that this assessment is applied. Personal impression influences a user's decision to share information on the unified system or not. The person deciding to share the information weighs trust in this way. Trust may weigh heavily on the decision to provide

2008; Xiong & Liu, 2004; McKnight, Choudhury & Kacmar, 2002; Niu, 2007; Razavi & Iverson, 2006; Ruppel, Underwood-Queen & Harrington, 2003; Schoorman, Mayer & Davis, 2007; Zhang, 2005; Rocco, 1998; ISAC, 2004; Li, Hess & Valacich 2008; Ray & Chakraborty, 2004; Chakraborty & Ray, 2006; Park, Suresh, An & Giordano, 2006; Park, An & Chandra, 2007 ; Walker & Ostrom, 2007.

information as well (Niu, 2007; Pardo, Cresswell, Thompson, & Zhang, 2006). In the case of a very trusting person, he or she is more likely to freely provide information to the system than someone who is more apprehensive or who has some specific concerns as above.

A study by van de Wijngaert and Bouwman (2009) identified trust as a contributing factor to user adoption of new technology systems. In their study of potential adoption of new wireless grids communications technology, willingness to share, and potential use of, the technology was found to be related to trust in the partner, social context and in the technology. This same study provided some of the initial support used in the creation of the information sharing framework here where it identified that in emergency situations people are more willing to share (van de Wijngaert & Bouwman, 2009). Trust as it relates to information sharing was investigated as well by Young-Ybarra and Wiersema (1999). There the authors were able to model the weight of influence of trust in interactions across organizations. Here a connection was made in terms of social exchange theory regarding trust that communication, attachment and having shared values had significant influence on trust (Young-Ybarra & Wiersema, 1999).

4.2.2 Informal Network

Informal, or shadow, networks involve the situation where a personal or agency connection, in or outside of the work place, creates a conflict of interest and the organization or individual may not act in a non-biased, objective manner. This may involve personal friendships, affiliations or family ties and connections through other activities or interests outside the workplace. This can have positive and negative effects for organizations (Ingram & Lifschitz, 2006). Intelligence information that may negatively impact an agency or key individuals or associates may be withheld and not shared by the organization involved. The stigma or interpersonal links behind the scenes play a role in interaction and sharing decisions (Kulik et al., 2008). This is related to the organizational notion of shadow systems, which are described by Stacy (1996) as “the complex web of interactions in which social covert political and psycho-dynamic systems coexist in tension with the legitimate system” (Shaw,1997; Stacey, 1996). There is an obvious link here to personal integrity and to social impacts of potentially damaging information that hits “too close to home.” The personal integrity of the individual member with the information has an influence on whether or not they will share. Integrity is internal to the individual. Trust is focused outward to the perception of another agency by the individual. Integrity is related to the specific character and makeup of the person with the information.   Influences such as policy, trust and personal interests, personal connection, and corruption affect different individuals in different ways based on their personal integrity and interests. A person who demonstrates a high degree of respect for the rules and regulations of the agency would be considered to have a high degree of integrity and would be more likely to follow policy than someone with a record of bending, or not following, the rules. Integrity involves a willingness to place the organizations rules and interests above one’s own.

4.2.3 Criticality

Criticality of the information itself and its potential harmful impact if not disclosed is a key influencer of action in sharing information. Studies by J. Lee and H.R. Rao have shown that officers are more likely to share information where there is a clear and present danger to life or property (Lee & Rao, 2007). The greater the threat, the greater the likelihood that the people involved will cooperate and share information. Preliminary work exploring possible causes and effects of inter-agency information-sharing systems adoption in the counter-terrorism and disaster management domains involved an exploration of environmental and situational conditions for cooperation between emergency management agencies. The perceived information assurance of others and having information sharing standards were more strongly related to agencies sharing than were cultural norms, in emergency contexts. The study of Lee and Rao supports the assertion that during a crisis, where criticality is described as a factor, people are more willing to share information regardless of other influences. The timeliness of the information itself is also related to criticality. The relationship of time to the consequences or effectiveness of the information influences whether or not the information is shared or not. In the case of information obtained too late or after the fact, it may or may not be shared based on what consequence it may have at that point in time. Information of a questionable value may be held in waiting so that it can be verified or supported in some way before sharing. As the time draws near to where the information may become useless if not shared, the decision to share or not share is reevaluated.

4.3 Policy Influences

4.3.1 Policy Conflict, Competition and Confusion

Agency policy also has influence on whether information gets shared or not. In an agency with defined policy as to what is to be shared, it is easier for staff to make the determination to follow through with information that is clearly within the guidelines. Clear and enforced rules for information sharing lead to better sharing of this information (Carter & United States, 2004). Policies also vary and are subject to interpretation.

The legal boundaries surrounding intelligence information sharing are unclear. This lack of clarity in law and policy was reflected in the statement of John McKay, former United States

Attorney for the Western District of Washington, speaking before the subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment on Homeland Security (McKay, 2008). Having uncertainty in what is allowed to be provided presents a problem for those wishing to share as much intelligence information as they can (Carter, 2005). The concerns over privacy and violation of individual rights of citizens must be addressed (German & Stanley, 2008). There is no clear standard or ready guideline for agencies that addresses information sharing factors at the federal and local levels in a readily usable way (Swire, 2006; Thompson & Kaarst-Brown, 2005). Civil liberties issues must be addressed (Martin, 2004). If agencies had this resource, they would be in a better position to actively share information and address the concerns over privacy and sharing (Carter & United States, 2004). The notion of these barriers to information sharing as a “wall” has been proffered for some time, yet arguments can be made that it is lack of knowledge about current statutes and policy and not the statutes themselves that are hindering agencies from sharing information with each other (Martin, 2004).

Furthermore, based on the funding or evaluation policy, agencies may compete for resources and there is a competitive element to doing the job better than other agencies that have shared interests and responsibility. For instance, funding for activities may be based on how many crimes are solved or specific incidents handled by a particular agency. An example of this would be formula grants, which are disseminated based on key reported activities handled by an agency. Actually, the Department of Justice alone distributed $2.396 billion dollars of assistance to law enforcement and other agencies based on formula and competitive grant requests and other programs (USDOJ, 2008). This leads to competition for important cases and an interest in being the agency to close a particular case or handle a particular incident. As long as funding determinations are made in this manner, competition among agencies will likely continue to be an influencing factor. Under the present structure, many law enforcement agencies are put in a position of being in competition for statistics and resources with other agencies because agencies from the federal to local levels each must justify their budgets to their constituencies and oversight entities. There is a belief that showing your agency as the one doing the work, being involved in activity, and bearing the responsibility will all correlate to getting awarded more money and resources.

4.3.2 Governance

Governance structures and systems operating in the law enforcement arena can create conflicts of interest and reduce cooperation. Law enforcement agencies in the United States share overlapping responsibilities and jurisdiction with no one unitary command; this creates problems over control and authority in investigations, information sharing, and access. Officials independently act in the interests of their constituencies as well as for the broader collective good. The approach and expectations for collaboration in this environment must be challenged to be effective in the future. Law enforcement in the US remains uniquely decentralized and does not operate under unitary command or control. Recent case studies on knowledge sharing within public sector inter-organizational networks confirm that there are information-sharing difficulties across agencies (Jing & Pengzhu, 2007; Pardo, Cresswell, Thompson, & Zhang, 2006). Agencies overlap jurisdictions and responsibility; each with a duty to their own constituencies. Each has their own notion and structure for control.

There is not a clear and universal guide to what intelligence information can and cannot be shared across the federal, tribal, state and local levels. The laws and policies governing information security, dissemination, and use vary across local, state, tribal, and federal agencies. Where agencies do not have clear leadership and guidance on whether or not intelligence information may be shared, they may choose to take the safer path of not sharing to protect them from liability. For instance, security clearances for intelligence information sharing and recognition of legitimate rights to access intelligence information by local, state, tribal, and federal agencies remains a process that is not coordinated or acknowledged across agencies.

5. Conceptual Model

A conceptual model based on the impacts of two types of direction or force of influences affecting whether or not sharing occurs: facilitators and detractors is introduces here. The model is based on the key influences on intelligence information sharing that were analyzed in Section 3. This conceptual model is an offspring of Lewin's force field analysis, which is used here for looking at factors or forces influencing the decision of an individual or organization to share intelligence information (Thomas, 1985). It is also consistent with organizational change stages suggested by Lewin (1951) and others (Kaarst-Brown, 1999). Forces may act as facilitators– driving movement toward information sharing– or as detractors drawing momentum away from a choice to share something like intelligence information. Each of the factors depicted under the headings given in the information sharing framework has a potential for facilitating or detracting from a choice by the person or agency to share intelligence information in a given context or not, and to what extent. Facilitators include the positive influences that result from technical, social, and policy factors. Detractors include negative influences resulting from technical, social and policy rules, regulations, actions or perceptions (see Figure 11 below). The combination and interaction of the facilitating and detracting forces leads to a condition of sharing or not sharing information.

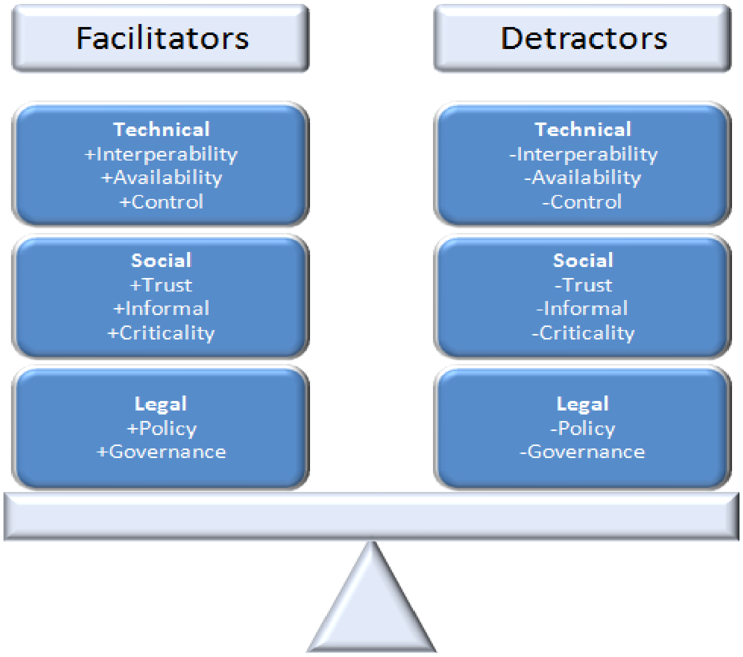


Figure 11: Factors Influencing Information Sharing

As facilitators, technical factors such as having compatible operating systems, software, hardware, data definitions, secure access, control, high usability, and system availability all can work towards improving the potential for information sharing but do not cause information to be shared (Lee & Rao, 2007; Scott, 2006). Regarding technology, picture two young friends who tie two tin cans together on a string to communicate; it is not the technology of the cans that cause the two to talk across the string but their desire to share with each other that controls use of technology. It is therefore the social and cultural aspects of the relationship that matter more than the technology in the equation for information sharing. Today, the two kids from the previous example are texting.

Socially, greater trust and knowledge of the other parties involved may lead to a greater tendency towards intelligence information sharing. This process involves considerations of agency culture and personal ties or connections with other involved agencies, which may include informal or "shadow" networking ties outside the workplace such as connections to family and friends or other associations that involve one member having some other contact or relationship with someone associated with another agency (Drake, Steckler, & Koch, 2004; Marks & Sun, 2007). A common example involves family, friends, or affiliation through participation in clubs or activities that involve others apart from the work environment. These external contacts can have a positive, or negative, influence on the likelihood of intelligence information sharing. Shared training and joint operations such as the U.S. Marshals' joint fugitive round up effort with state and local agencies in Florida were shown to have a positive effect on information sharing (Clark, 2008). Importance to those involved, as described previously, can be a critical factor influencing the sharing of intelligence information as well. Information that is credible and which may result in some specific harm or loss is more readily shared. The pressure to share this information is increased where there may be an approaching deadline or need to act quickly for safety (Lee & Rao, 2007).

In the area of legal influence, having a clear and enforced agency policy regarding intelligence information sharing can lead to a greater likelihood that information will be shared as will increased knowledge of laws and regulations, which allow for intelligence information sharing. Having an established governance system and involving participation by others has also been shown to facilitate collaboration and intelligence information sharing where members and organizations had positive regard for and accepted each other's roles (Cresswell, Pardo, & Hassan, 2007; Park, Sandhu, & Ahn, 2001). It has been shown that people within agencies are more likely to participate in sharing systems that they have choice, investment and control over.

As detractors, intelligence comes from the field or other sources to an agency and the identified factors may negatively affect the degree to which this information is likely to be shared.

Legal factors with a negative influence include having separate security clearances, not uniform or recognized across agencies, laws regarding privacy, secrecy, or sharing of information that are conflicting or not well understood by participants. Social factors here also involve issues of lack of trust, integrity, assurance, or an agency culture, which is geared towards not sharing (Lee & Rao, 2007). Trust is reduced where agencies compete with each other for statistics, media attention, and funding. Informal or outside contacts, which are described as part of the informal network, have great potential to provide a negative influence if the information may be potentially damaging to an entity or person. Criticality also includes timing of information and its potential impact such that where there is little urgency the pressure to share this intelligence is reduced and action may be delayed. Where there is no identified time frame or deadline, the information may not be reacted to in a timely manner and put to the side and not shared. Lack of knowledge or inaccurate knowledge about what actions can be taken regarding sharing of information can hinder information sharing. Matters of jurisdiction, authority, and governance or control over the power or influence also work against sharing (Drake et al., 2004). The means for quantifying or assessing the particular significance relative to other factors and forces remains an important question and subject for further research.

Technical factors can act as detractors as well. Many agencies use different hardware and software programs for communication and information management, and these may not interact together. Systems that are not responsive or show poor performance may not be adopted. Agencies with existing systems may not be financially able to change to more compatible or standardized systems. The costs for retraining personnel on to new services can be high as well. Costs for maintenance and upgrades of the systems must be considered as well.

These social, policy and technical factors can serve as the basis and model framework for further investigation in this field. This paper argues that the inter-relationships between the identified factors influence the degree to which information sharing, and cooperation, is more or less likely to occur. This is proposed to be true for a given circumstance and environment and further that the resulting behavior can be observed, and represented in a conceptual model as the balance of this result. Knowledge of these factors may predict action.

Developed here for consideration is a proposed conceptual model based on the proposed information sharing framework that may be used to describe and to predict information sharing behaviors based on knowledge of the three influencing factors (social, technical, and policy) at a given time and for a given environment. The conceptual model proposed here was suggested from the research, literature, and observations conducted to date. Probable effects from modifying the influencing factors are more readily apparent and easier to identify using such a model. The conceptual model and its use are described in greater detail in the following.

The relationships in the proposition that are being investigated may be depicted conceptually in the form of an information-sharing model (this is an early conceptual approach, and there are not sufficient verified quantitative tools at this time to be able to accurately place specific weighting or values to these elements in advance). The current or end state of sharing or not sharing intelligence information (IIS) is the result of the combined effects of identified facilitators (F) and detractors (D) present or occurring within an agency at the time of consideration, and is shown as $IIS = f\,(F, D)$. As they are used in this research, F is a function of the combination of the resulting facilitating forces for social, technical, and policy factors (F = (S_{tsu} + T_{tirc} + P_{tkg}), and D is the sum of the detractor forces from those same factor headings (D = (S_{tsu} + T_{tirc} + P_{tkg}). Sharing of information, which may also be considered cooperation, occurs where the equation results in an imbalance in the form of a positive, negative, or zero - end state. If there are more forces working *against* sharing than those that work *for* sharing, the balance is tipped towards not sharing. It may also be the case that a stalemate can occur and information will not be shared. If both facilitating and detracting forces are equivalent (F = D) then it is a sum of zero or stalemate and information is not shared. One can alternatively combine summary versions of S for social (cultural) influences, T for technology influences, and P for policy issue influences to show the combined effect for IIS as $IIS = f\,(S_F+S_D,\ T_F+T_D,\ P_F+P_D)$ or more simply $IIS = f\,(S, T, P)$. This model may be further broken down to show how one may include various subcomponent influences and considerations such as i for interoperability, r for responsiveness, c for control, t for trust, s for informal networks, u for importance, k for knowledge, and g for governance factors within the broader categories. Not all of the factors and sub-factors may be present or available for consideration in a given case. The sub-categories are not meant to be exhaustive. The model and some possible components are show in the formulation and table in Figure 12 below:

$$\mathrm{IIS} = f(\, F\,,\, D\,)$$

$$F = (\mathrm{S}_{\mathrm{tsu}} + \mathrm{T}_{\mathrm{tirc}} + \mathrm{P}_{\mathrm{tkg}})$$

$$D = (\mathrm{S}_{\mathrm{tsu}} + \mathrm{T}_{\mathrm{tirc}} + \mathrm{P}_{\mathrm{tkg}})$$

$$\mathrm{IIS} = f\,(\mathrm{S}_\mathrm{F}+\mathrm{S}_\mathrm{D},\ \mathrm{T}_\mathrm{F}+\mathrm{T}_\mathrm{D},\ \mathrm{P}_\mathrm{F}+\mathrm{P}_\mathrm{D})$$

$$\mathrm{IIS} = f(\ \mathrm{S},\ \mathrm{T},\ \mathrm{P}\ )$$

IIS = Sharing	S = Social factors	T = Technical factors	P = Policy factors

F = facilitators
D = detractors
	t = trust
	s = informal networks
	u = importance
		t = trust
		i = interoperability
		r = responsiveness
		c = control
			t = trust
			k = knowledge
			g = governance

Figure 12: Information Sharing Model - V1

The conceptual model illustrated here can be used for understanding, description, or comparison purposes. It can serve as a tool to assess or predict sharing potential or action based on knowledge of inputs stemming from agency and environmental activity or conditions. One can also illustratively and conceptually change or manipulate the influencing factors to consider possible outcomes based on different inputs or actions. The model as a tool may describe a current or desired state, or serve as a predictor for the potential state given certain changes to influencing factors. Effects of the different influencing factors will be more readily apparent and easier to focus on using such a model.

6. Testing the Model

This paper proposes that the act of sharing or not sharing intelligence information can be described by considering conditions in terms of three broad factors: Social, Technical, and Policy as these factors were defined and operationalized previously in this paper. This relationship was shown as a conceptual model where intelligence information sharing (IIS) behavior is a function of the combined result of facilitating and detracting influences from the social, technical, and policy factors as shown previously. To test the model, an alternate version of the conceptual model is used. The alternate model is based on the same assumptions and conditions but allows survey data to be more readily input for demonstration and examination purposes. It is argued that $IIS=f(S,T,P)$ is an equivalent means of representing the relationship $IIS=f(F,D)$. A proposition is that the information-sharing model created is useful for describing and understanding intelligence information sharing behavior among participants in the law enforcement and broader public safety environment.

Intelligence Information Sharing (IIS) = *ƒ* (Social, Technical, Policy)

IIS = *ƒ* (S, T, P)

Figure 13: Information Sharing Model - V2

To demonstrate utility of the conceptual model, survey data were used to show the relationship of these three factors to actual intelligence information sharing behavior. The data used is from a national survey of law enforcement agencies in the United States conducted on behalf of the U.S. Department of Justice (USDOJ) for 2003.[10] There are approximately 19,000 law enforcement agencies in the United States at the local to federal levels. This survey was sent to 3,254 random agencies at the non-federal levels. The response rate was 90.6% for agencies overall and 100% for state agencies; 2,859 surveys were included in the final analysis. Of those, 2,741, or 95.9%, had sufficient data to be used here as the data needed to have sufficient information to verify agency name and be able to correlate to UCR submission information. The 2,741 survey respondents describe this population with 1.75% error at the 95% confidence level. Researchers consider the unusable 4.1% of total respondent data to have an insignificant impact on the findings for comparison purposes.

In the case model, intelligence information sharing (IIS) is represented by the response of agencies as to whether or not they participate in submitting their intelligence information to the

[10] United States Department of Justice. Bureau of Justice Statistics. Law Enforcement Management and Administrative Statistics (LEMAS): 2003 Sample Survey of Law Enforcement Agencies [Computer file ICPSR04411-v1. Ann Arbor, MI: Inter-university Consortium for Political and Social Research [distributor], 2006-05-10. doi:10.3886/ICPSR04411.v1.

Uniform Crime Reports (UCR) of the U.S. Department of Justice. This is a national repository for law enforcement data. Participation in the UCR is recommended for all agencies, but is not required by law. Agencies are considered to be sharing intelligence information if they send data to the UCR and they are considered to be not sharing if they do not send information to this repository. UCR submission is a dichotomous variable (yes or no to submitting intelligence information to the UCR) that is available from the data.

The three factors, Social, Technical, and Policy, are derived through a process of assessing individual survey response items from the national survey and assigning them to these factor categories as appropriate. Researchers identified five relevant questions from the survey for each factor category to build ordinal variables for Social, Technical, and Policy factors from the selected responses. For the factor categories, each question was given a 1 or 0 based on whether a described condition was present or not. Each question response contributed equal weights 1 or 0 to the total possible for each factor category. The result was creation of three ordinal factor categories having scores ranging from a minimum of 0 to a maximum of 5. The following is a listing of the factor categories with their associated questions as taken from the survey. The V# shown is the data item(s) identifier in the dataset followed by the text of the corresponding question number as taken from the survey.

Social

V43 - “Enter the number of ACTUAL part-time paid agency employees: a. Sworn personnel with general arrest powers.” Any number indicated here greater than 0 is assigned a 1.

V70 - “Indicate your agency's minimum education requirement which new (non-lateral) officer recruits must have within two years of hiring." Responses indicating some college or more are assigned a 1, otherwise 0.

V97 - "On average, how many total in-service hours of training are required annually for your agency's NON-PROBATIONARY field/patrol officers? A 1 is assigned for any total hours indicated here and a 0 for none.

V129 - V135 – "Does your agency provide special pay/benefits for any of the following?" A 1 is assigned for checking any of the eight listed incentives (Education, Hazardous duty, Merit/performance, Shift differential, Special skills proficiency, Bilingual ability, Tuition reimbursement, Military service), otherwise 0.

V453 - "Which of the following best describes your agency's written policy for pursuit driving?" A 1 is assigned for indicating either of the following; Judgmental (leaves decisions to Officer's discretion) or Agency does not have a written policy pertaining to pursuit driving, otherwise a 0. (A part of this question involves a written policy issue, however, the response is included here as a Social indicator due to its relevance as an indicator of agency culture and trust, putting greater faith in officers or creating an environment of less strict control.)

Technical

V147 - "Does your agency participate in an operational 9-1-1 emergency telephone system (i.e., your agency's units can be dispatched as a result of a call to 9-1-1)?" Checking yes to having either a basic or enhanced system is a 1, otherwise a 0.

V239 - "Do the public safety agencies operating in or nearby your jurisdiction (including your agency) use a shared radio network infrastructure that achieves interoperability?"

Checking yes is a 1, otherwise 0.

V358- V386 - “Indicate whether your agency's field/patrol officers use any the following types of computers or terminals WHILE IN THE FIELD.” For checking a box for having a computer available in the vehicle or as a portable it is a 1, otherwise 0.

V392 - “Do any of your agency’s field /patrol officers have direct access to the following types of information using IN-FIELD vehicle-mounted or portable computers?” Checking yes for Inter-agency information system is a 1, otherwise 0.

V419 – V436 - “Does your agency maintain its own computerized files with any of the following information? “ Checking any or all of the listed files (Alarms, Arrests, Biometric data for use with facial recognition sytem, Calls for service, Criminal histories, Fingerprints, Incident reports, Illegal attempts to purchase firearms, Intelligence relate to potential terrorist activity, Stolen property, Summonses, Traffic accidents, Traffic citations, Traffic stops, Use-of-force incidents, Warrants) is a 1, otherwise 0.

Policy

V237 - “Does your agency have a written plan that specifies actions to be taken in the event of terrorist attacks? (Include emergency operation plans that would be applicable to such an attack.)” A yes here is a 1, otherwise 0.

V238 - “Does your agency's plan include mutual aid or cooperative agreements between city, county, transit, public works, and/or other agencies?” A yes is 1 a no is 0.

V208 - “Does your agency's mission statement include a community policing component?” A yes here is a 1, otherwise 0.

V213 - “During the 12-month period ending June 30, 2003, did your agency have a problem-solving partnership or written agreement with any of the following?" Checking "Other local law enforcement agencies" is a 1, otherwise 0.

V440 & V451 - "Does your agency have written policy directives on the following? " Checking yes for both "Code of conduct and appearance" and "Interacting with the media" is a 1, otherwise 0.

6.1 Describing intelligence information sharing

It is important to know the factors that lead to an agency sharing intelligence information. This is represented through examining characteristics of respondent agencies who answer the question of do they submit information to the UCR. This example represents the broader question of what are observable behaviors, as agency factors, that impact intelligence information sharing in the law enforcement community. The instrument used to predict whether or not an agency is more or less likely to share intelligence information is comprised of a combination of three identifiable factors: Social, Technical and Policy. The question is whether or not this is a reliable test for identifying the likelihood of those identified elements acting as predictors for agencies sharing intelligence information, in this case UCR data. The goal of this research is to provide evidence of this model's utility for predicting or explaining the outcome of sharing intelligence information by agencies in the law enforcement community.

6.2 Multiple Regression described

Multiple regression is a technique in statistics that allows one to predict expected outcomes based on observed patterns of related variables in the data. It is more than a descriptive technique. Multiple regression rises to a predictive level of investigation of phenomenon. To predict the degree of intelligence information sharing among law enforcement agencies, one may look at variables such as having a written policy on sharing, participation in multi-agency communications systems, internal structures such as computer infrastructures and others. Variables such as these can be captured, such as through observation or survey. As a model, they may contribute to understanding intelligence information sharing by an agency. The model proposed in this article postulates that intelligence information sharing behavior can be understood through created factors of Social, Technical and Policy, as previously identified. To test this proposition, multiple regression analysis is conducted using the U.S. Department of Justice (DOJ) survey data.

From Princeton.edu, multiple regression is: “a statistical technique that predicts values of one variable on the basis of two or more other variables” (wordnet.princeton.edu/perl/webwn, 05/01/2009).

In multiple regression, researchers use “independent variables” to identify variables they expect will influence the “dependent variable” and so when used here they are called “predictor variables” because they are variables that are believed to have an effect on the dependent variable– in this case, intelligence information sharing (which may also be called the “criterion variable” in the literature) and which is operationalized as the agency submitting data to the UCR.

In 1927 the Department of Justice created a nationwide information sharing initiative known as Uniform Crime Reporting (UCR) program. Agencies report certain arrest and incident information to a central repository. This sharing of information with other agencies and the public constitutes an act of information sharing by the participating agency. The majority of law enforcement agencies today voluntarily participate, but not all (USDOJ, 2008). Researchers here argue that sharing information through the UCR is indicative of an agencies propensity to share other information of greater or lesser criticality. Participation in UCR reporting is useful as a criterion variable for investigating information sharing behavior by an agency more broadly.

Multiple regression provides an acceptable way to identify predictor variables, which are useful to estimating an agencies likely degree of intelligence information sharing based on what is known.

6.3 SPSS Example

The example here uses SPSS version 19. The data set comes from the national survey of law enforcement agencies in the United States conducted on behalf of the U.S. Department of Justice (USDOJ) for 2003-2004. There are approximately 19,000 law enforcement agencies in the United States at the local to federal levels. This survey was sent to 3,254 agencies at the non-federal levels. The response rate was 90.6% for agencies overall and 100% for state agencies; 2,859 surveys were included in the final analysis. Of those, 2,741, or 95.9%, of those had sufficient data to be used here as data needed to have sufficient information to verify agency name and be able to connect to UCR submission information.

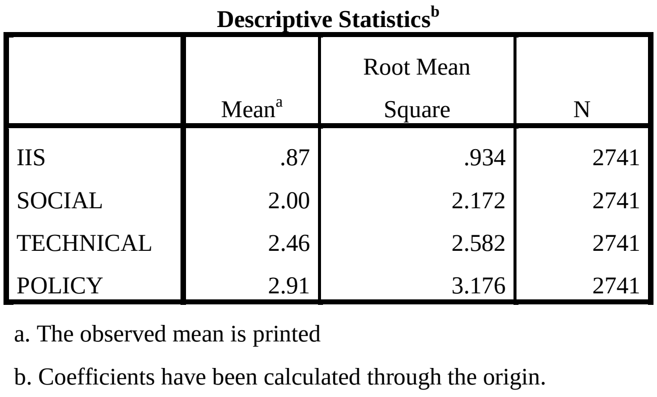
A metric for Intelligence Information Sharing (IIS) was selected to describe whether or not intelligence information is shared by an agency. The IIS response result is the criterion variable. IIS is comprised of the dichotomous response to whether or not the agency submits data to the UCR, a 1 for yes and 0 for no. This metric is used to describe whether or not the agency shares or does not share intelligence information.

Predictor variables for the IIS criterion variable include the created variables: Social, Technical, and Policy, as described above.

There were several other trials of the linear regression conducted. These included the variables identified above and also included other variables such as; population, state, budget and even whether or not having a horse unit had an predictive effect. The alternate trials did not improve the predictive capability significantly over the present model. Interestingly, having a horse unit did show a slight correlation to predicting IIS, as did number of dismissals, but not enough to warrant including them as additional factors. The aim was to test whether the three identified factors could be used to accurately predict intelligence information sharing in accordance with the model and not necessarily to establish that it was the best formulation of all choices. SPSS output is provided below.

6.4 Regression

[DataSet] “LEMA2003_2741.sav”



Descriptive Statistics[b]

	Mean[a]	Root Mean Square	N
IIS	.87	.934	2741
SOCIAL	2.00	2.172	2741
TECHNICAL	2.46	2.582	2741
POLICY	2.91	3.176	2741

a. The observed mean is printed

b. Coefficients have been calculated through the origin.

Figure 14: Descriptive Statistics

The first table was produced by the descriptives option and contains information on means, the root mean square, and numbers of the population. It also tells that the coefficients have been calculated through the origin. Correlations provide a first look at the model as assembled.

Correlations[a]

		IIS	SOCIAL	TECHNICAL	POLICY
Std. Cross-product	IIS	1.000	.873	.896	.868
	SOCIAL	.873	1.000	.905	.882
	TECHNICAL	.896	.905	1.000	.932
	POLICY	.868	.882	.932	1.000
Sig. (1-tailed)	IIS	.	.000	.000	.000
	SOCIAL	.000	.	.000	.000
	TECHNICAL	.000	.000	.	.000
	POLICY	.000	.000	.000	.
N	IIS	2741	2741	2741	2741
	SOCIAL	2741	2741	2741	2741
	TECHNICAL	2741	2741	2741	2741
	POLICY	2741	2741	2741	2741

a. Coefficients have been calculated through the origin.

Figure 15: Correlations

The correlations table provides details of the correlation between pairs of the chosen variables. For a good predictive model, one does not want strong correlations between criterion and predictor variables. The values in the top box are the Pearson Correlation output and all are below 1, which is acceptable. The Sig (1-tailed) section and counts in the N section are also acceptable, well below .05 and complete counts.

Variables Entered/Removed[b,c]

Model	Variables Entered	Variables Removed	Method
1	POLICY, SOCIAL, TECHNICAL	.	Enter

a. All requested variables entered.

b. Dependent Variable: IIS

c. Linear Regression through the Origin

Figure 16: Variables Entered/Removed

The box Variables Entered/Removed shows the result from the “Enter” query, which included all of the variables chosen and so all are show here as being used.

Model Summary[c,d]

					Change Statistics					
Model	R	R Square[b]	Adjusted R Square	Std. Error of the Estimate	R Square Change	F Change	df1	df2	Sig. F Change	Durbin-Watson
1	.910[a]	.828	.827	.388	.828	4379.595	3	2738	.000	1.924

a. Predictors: POLICY, SOCIAL, TECHNICAL

b. For regression through the origin (the no-intercept model), R Square measures the proportion of the variability in the dependent variable about the origin explained by regression. This CANNOT be compared to R Square for models, which include an intercept.

c. Dependent Variable: IIS

d. Linear Regression through the Origin

Figure 17: Model Summary

The model summary shows the result from the choice of predictor variables and method. The R square value is shown here as .828, which means that this model accounts for 82.8 % of variance in the IIS scores. This is a significant percentage for this model. ANOVA is now conducted for further validation and significance information.

ANOVA[c,d]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	1977.837	3	659.279	4379.595	.000[a]
	Residual	412.163	2738	.151		
	Total	2390.000[b]	2741			

a. Predictors: POLICY, SOCIAL, TECHNICAL

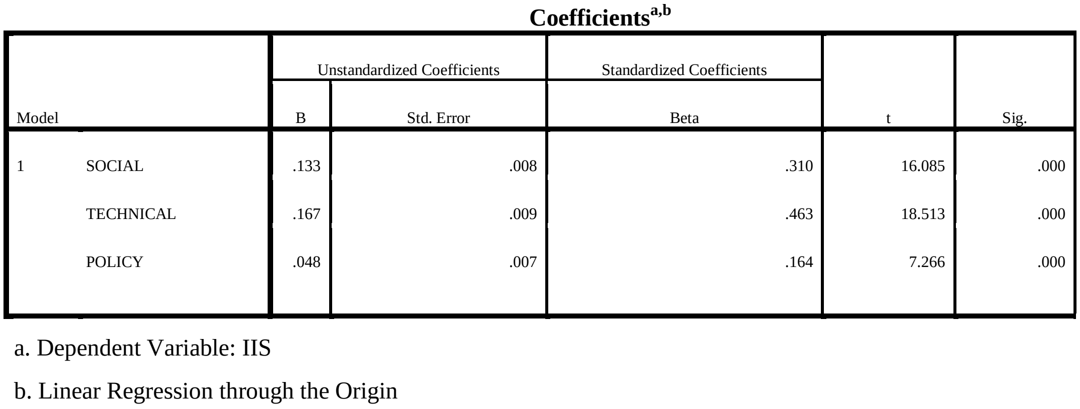
b. This total sum of squares is not corrected for the constant because the constant is zero for regression through the origin.

c. Dependent Variable: IIS

d. Linear Regression through the Origin

Figure 18: ANOVA

The ANOVA reports an assessment of overall significance of the model as an F value of 4379.595 with a (Sig.) p < 0.05 so this model is significant.



Coefficients[a,b]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	SOCIAL	.133	.008	.310	16.085	.000
	TECHNICAL	.167	.009	.463	18.513	.000
	POLICY	.048	.007	.164	7.266	.000

a. Dependent Variable: IIS

b. Linear Regression through the Origin

Figure 19: Coefficients

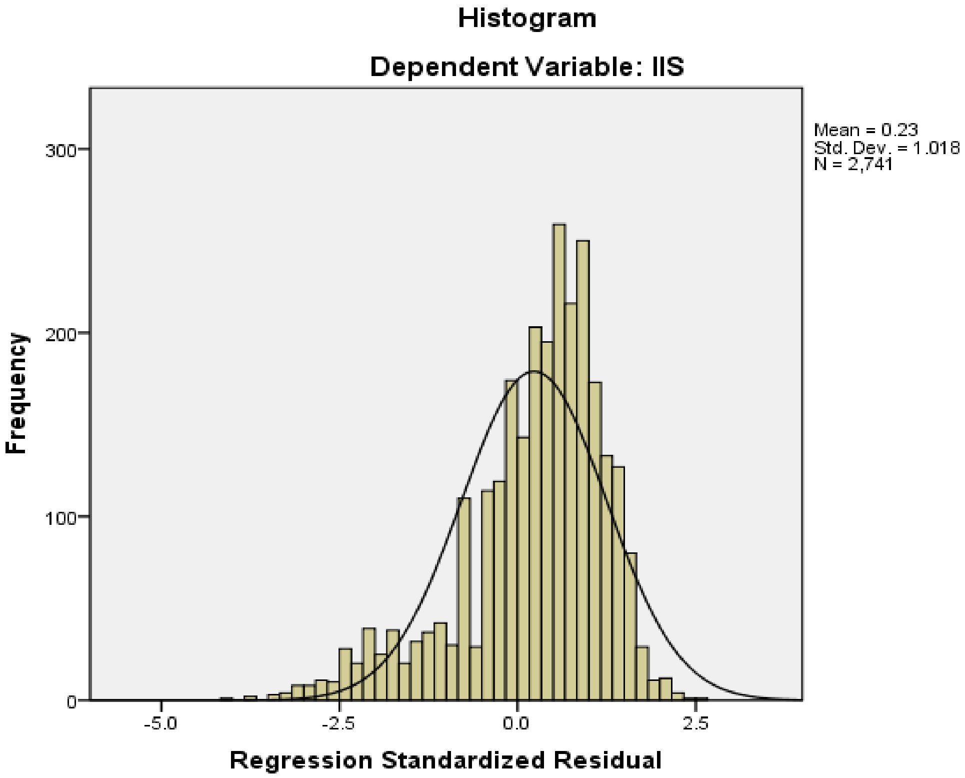
From the coefficient table, the Standardized Beta coefficients show a measure of each variables contribution to the model. These standardized beta coefficients are interpreted in a similar way to correlation coefficients or factor weights. Large values here indicate that a unit of change in the given variable will have a large effect upon the criterion variable (IIS). Signs, + or – of the regression or B coefficients show the direction of the relationship between the variables. If positive, the relationship of this particular variable to the dependent variable is positive or increasing. If negative, the relationship of the particular variable to the dependent variable is negative or declining. For a B coefficient of 0, there is no relationship.

The order of relative importance from the B and Beta figures suggests the order of importance of the independent variables in this model changes slightly from the unstandardized Coefficients to the standardized Beta. The standardized Beta coefficient shows the order from greater influence to lesser: TECHNICAL, SOCIAL, and then POLICY. A greater emphasis is on the standardized Beta because of the comparison that is being made across equations.

As shown, the t and p (Sig.) values provide an indication of the influence of the predictor variables such that a large absolute t with small p value implies greater impact on the criterion variable. These values are also significant: all over 7 and p < 0.05.

A histogram and scatterplot of the model are provided below. Scatter plots show direction and strength of the relationships between variables. The scatter plot shows a strong positive linear relationship with a few outliers. The predictor variables have a positive influence on the criterion variable, IIS. A histogram from SPSS on the regression standardized residual to frequency was produced as well. This shows the data conforming to a normal curve.

The conclusions follow the two figures below.



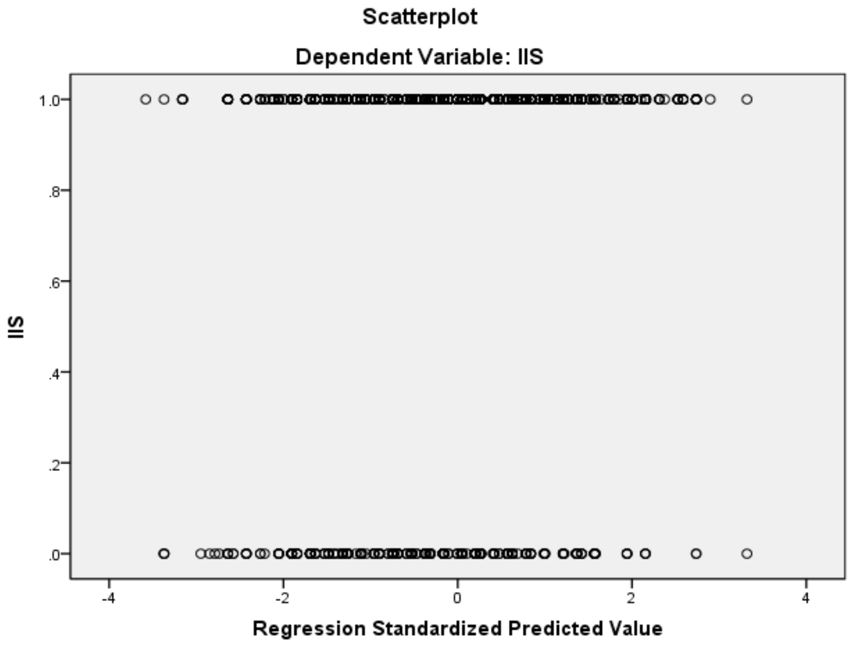


Figure 20: Histogram and Scatterplot for IIS

The statistical package SPSS V.19 was used to analyze data from the 2003 U.S. Department of Justice survey of law enforcement agencies. Using the enter method, a significant model for IIS was established with R square = .828; F3, 2738 = 4379.595, p < 0.000*. Significant variables are shown below:

Predictor Variable	Beta	p
SOCIAL	.310	p < 0.000*
TECHNICAL	.463	p < 0.000*
POLICY	.164	p < 0.000*

**actual value not shown as it is beyond three decimal places*.

The three-variable model strongly predicts the outcome of the IIS metric regarding intelligence information sharing by law enforcement agencies.

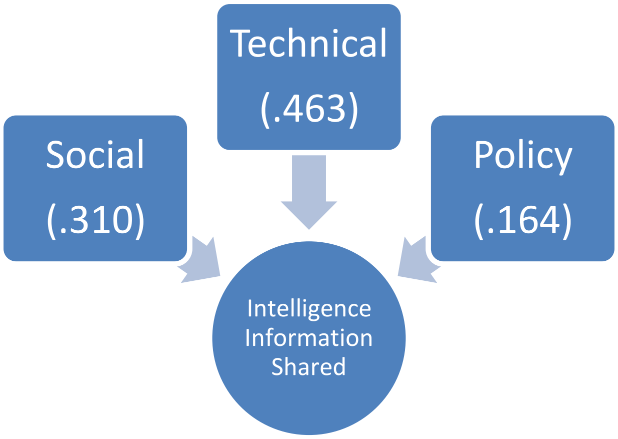


Figure 21: Influence of Factors

The chart above shows the influence of the three factors upon IIS. The investigation of these influences will inform the model for the degree of influence each may have relative to the other so that decision makers can pattern solutions towards the desired end. This one case is not conclusive. This work can serve as the basis and framework for further investigation, which should focus on further quantifying the influence of these elements as well as confirming, or disputing, their impact and relevance in the model.

By using the approach developed, one can visualize the effects of making changes in different areas of influence on the level of information sharing and observe the outcomes. One can see how adjustments in degree of influence for the influencing factors identified determine whether or not intelligence information is shared under the given circumstances.

7. Conclusions and Future Work

While millions of dollars have been invested in technologies to improve intelligence information sharing among public safety agencies at the federal, tribal, state and local levels, there remains a hesitation to share this information between agencies. This lack of coordination has hindered the ability of these entities to prevent and respond to crime, terrorism and to protect the public. The work done to date by others has not produced widely accepted solutions or paradigms for understanding the problem. This research was conducted by investigators including law enforcement personnel and in that way provides a unique insider perspective to understanding the problem. A framework and theory of intelligence information sharing has now been created through a multi-method process involving literature review, document analysis, participant observation, and interviews with practitioners in the field. A model consisting of three major factor areas of influence; Technical, Social, and Policy are identified and successfully tested using data from a National survey of law enforcement agencies. This model and theory should serve as a basic conceptual framework for further academic work that may be used by practitioners and academics alike and lead to additional investigation and clarification of the identified factors and the degree of impact they exert on the system so that actionable solutions can be identified and implemented.

This research has led to the creation of a conceptual framework and model for information sharing that is both descriptive and predictive. It is posited in this research that intelligence information sharing between law enforcement agencies is affected by social, technical, and policy factors, which are comprised of issues and considerations including, but not limited to: interoperability, availability, control, trust, informal networks, criticality, policy conflict, competition, and governance. This was done through a research process involving literature review, field observation, experience, and interviews with practitioners in the field. Researchers involved included members of the law enforcement community, providing for a unique insider perspective to investigating and understanding information and collaboration issues in this community.

Within the broader identified problem areas of technical, social, and policy factors individual identifiable factors were found that play roles in influencing whether or not information is ultimately shared. This research has identified the major areas of influence and posits that these factors work to facilitate or detract from information sharing and cooperative behavior between agencies.

The information sharing model consisting of three major influencing factor areas: Technical, Social, and Policy was successfully tested using data from a National survey of law enforcement agencies.

The UCR is useful as a criterion variable for testing purposes, however, it does not speak directly to other forms of information sharing that may be more difficult or critical. Researchers here argue that agencies who are willing to share UCR information are more likely to share critical information and even innocuous information generally than those who do not participate.

This conceptual model and theory should serve as a starting point for future academic research and lead to clarification of the identified factors and the degree of impact they exert on the system so that actionable solutions can be identified and implemented.

The information-sharing model, for considering the impacts and outcomes from the interaction or manipulation of the identified factors, should be further tested and validated. Additional tools for quantification of the factor components identified will be developed in further extensions of this work. This will help practitioners and policy makers identify new strategies to improve information sharing among all law enforcement agencies and will result in improved law enforcement capability to prevent and respond to crime, terrorist activity, and other emergencies as well as lead to greater effectiveness in overall public service response and delivery across government entities in general.

8. References

BJS. (2007). *US Department of Justice, Bureau of Justice Statistics (BJS) Law Enforcement Statistics*, August 8, 2007. Retrieved May 9, 2008, from http://www.ojp.usdoj.gov/bjs/lawenf.htm.

Booth, K., & Wheeler, N. (2007). *Security Dilemma: Fear, Cooperation, and Trust in World Politics (First* ed.). Palgrave Macmillan.

Bulman, P. (2008). Communicating across state and county Lines: The Piedmont Regional Voice over Internet Protocol Project. *NIJ Journal*, 261. Retrieved February 22, 2009, from http://www.ojp.usdoj.gov/nij/journals/261/piedmont- voip.htm.

Cannon, J. P., & Homburg, C. (2001). Buyer-supplier relationships and customer firm costs. *The Journal of Marketing*, 29–43.

Carter, D. L., & United States. (2004). *Law enforcement intelligence a guide for state, local, and tribal law enforcement agencies*. Washington, D.C.: U.S. Dept. of Justice, Office of Community Oriented Policing Services.

Carter, D. L. (2005). "Brief history of law enforcement intelligence: Past practice and recommendations for change." *Trends in Organized Crime* 8(3):51-62. Retrieved February 15, 2008.

Chakraborty, S., & Ray, I. (2006). Trust BAC: Integrating trust relationships into the RBAC model for access control in open systems. In Proceedings of the 11th ACM Symposium on Access Control Models and Technologies, Lake Tahoe, CA, June 2006.

Chan, H. C., & Teo, H. (2007). Evaluating the boundary conditions of the technology acceptance model: An exploratory investigation. ACM Trans. Comput.-Hum. Interact., 14(2), 9. doi: 10.1145/1275511.1275515.

Chau, M., Atababhsh, H., Zeng, D., & Chen, H. (2002). Building an infrastructure for law enforcement information sharing and collaboration: Design issues and challenges. National Science Foundation. Retrieved February 4, 2008, from http://dlist.sir.arizona.edu/473/01/chau4.pdf.

Chen, H., Zeng, D., Atabakhsh, H., Wyzga, W., & Schroeder, J. (2003). COPLINK: managing law enforcement data and knowledge. *Communications of the ACM*, 46(1), 28-34.

Clark, J. (2008). Remarks by Director John Clark at the Operation Orange Crush Press Conference, September 18. *USMarshals.gov*. Government Agency. Retrieved November 27, 2008, from http://www.usmarshals.gov/news/chron/2008/091808.htm.

Colquitt, J. A., Scott, B. A., & LePine, J. A. (2007). Trust, trustworthiness, and trust propensity: A meta-analytic test of their unique relationships with risk taking and job performance. *Journal of Applied Psychology*, 92(4), 909–926.

Cresswell, A. M., Pardo, T. A., & Hassan, S. (2007). Assessing capability for justice information sharing. *In Proceedings of the 8th annual international conference on Digital government research: bridging disciplines & domains* (pp. 122-130). Philadelphia, Pennsylvania: Digital

Government Society of North America. Retrieved September 18, 2008, from http://portal.acm.org/citation.cfm?id=1248460.1248479 & coll=ACM & dl=ACM & CFID=3249028 & CFTOKEN=78511360

Dawes, S. S. (1996). Interagency information sharing: Expected benefits, manageable risks. *Journal of Policy Analysis and Management*, 15(3), 377−394.

Drake, D., Steckler, N. A., & Koch, M. J. (2004). Information sharing in and across government agencies: The role and influence of scientist, politician, and bureaucrat subcultures. *Social Science Computer Review*, 22(1), 67-84. doi: 10.1177/0894439303259889.

Fernández-Medina, E., & Yagüe, M. I. (2008). Guest Editorial: State of standards in the information systems security area. *Computer Standards & Interfaces, 30*(6), 339-340

Gao, J. (2005). Information sharing, trust in automation, and cooperation for multi-operator multi-automation systems. Retrieved from http://proquest.umi.com/pqdweb?did=1079666781 & Fmt=7 & clientId=3739 & RQT=309 & VName=PQD.

Gerdes, A. (2010). Revealing preconditions for trustful collaboration in CSCL. *International Journal of Computer-Supported Collaborative Learning*, 5(3), 345–353.

German, M., & Stanley, J. (2008). Fusion Center Update - ACLU,July. Retrieved October 19, 2008, fromhttp://www.aclu.org/pdfs/privacy/fusion_update_20080729.pdf.

Glomseth, R., Gottschalk, P., & Solli-Saether, H. (2007). Occupational culture as determinant of knowledge sharing and performance in police investigations. *International Journal of the Sociology of Law*, 35(2), 96-107. doi:10.1016/j.ijsl.2007.03.003.

Gupta, E. (2000). Information System. *Bajaj, Ankit 197 Bakry, Mohamed Abd El Latif 28 Bala, Shashi 414 Baporikar, Neeta 118*, 97.

Handy, C. B. (1976). Understanding organizations. Oxford University Press.

Handy, C. B. (1996). *Beyond certainty: the changing worlds of organizations*. Harvard Business Press.

Humenn, P., Chin, S.-K., Kosiyatrakul, T., Older, S., & Northrup, T. (2004). *A trusted information sharing project*. Syracuse. Retrieved from http://webdev.maxwell.syr.edu/insct/Research/IS%20Page/SU%20Trust-Sharing%20Project.pdf

Ingram, P., & Lifschitz, A. (2006). Kinship in the shadow of the corporation: The Interbuilder Network in Clyde River Shipbuilding, 17111990. *American Sociological Review*, 71, 334-352.

ISAC. (2004). White paper, Vetting and trust for communication among ISACs and government entities. Retrieved October 23, 2008, from http://www.isaccouncil.org/pub/Vetting_and_Trust_013104.pdf.

Ivkovic, S. K., & Shelley, T. O. (2005). The Bosnian police and police integrity: A continuing story. *European Journal of Criminology*, 2(4), 428-464. doi:10.1177/1477370805056057.

Jing, F., & Pengzhu, Z. (2007). A case study of G2G information sharing in the Chinese context.

In proceedings of the 8th annual international conference on Digital government research: bridging disciplines & domains (pp.234-235). Philadelphia, Pennsylvania: Digital Government Society of North America.

Kaarst-Brown, M. L. (1999). Five symbolic roles of the external consultant–integrating change, power and symbolism. *Journal of Organizational Change Management*, 12(6), 540–561.

Kaarst-Brown, M. L., & Robey, D. (1999). More on myth, magic and metaphor: Cultural insights into the management of information technology in organizations. *Information Technology & People*, 12(2), 192–218.

Koroma, J., Li, W., & Kazakos, D. (2003). A generalized model for network survivability. *In proceedings of the 2003 conference on Diversity in computing* (pp.47-51). Atlanta, Georgia, USA: ACM. doi:10.1145/948542.948552.

Koufaris, M., & Hampton-Sosa, W. (2004). The development of initial trust in an online company by new customers. *Inf. Manage.*,41(3),377-397.

Kulik, C. T., Bainbridge, H. T. J., & Cregan, C. (2008). Known by the company we keep: Stigma-by-association effects in the workplace. *Academy of Management Review*, 33(1), 216-230. doi: Article.

Lai, V. S., & Mahapatra, R. K. (1997). Exploring the research in information technology implementation. Inf. Manage., 32(4),187-201.

Lampathaki, F., Mouzakitis, S., Gionis, G., Charalabidis, Y., & Askounis, D. (2009). Business to business interoperability: A current review of XML data integration standards. *Computer Standards & Interfaces*, *31*(6), 1045-1055.

Lee, C. (2006). The role of trust in information sharing: A study of relationships of the interorganizational network of real property assessors in New York State. Ph.D. diss., State University of New York at Albany, In Dissertations & Theses: Full Text [database on-line]; available from http://www.proquest.com.libezproxy2.syr.edu (publication number AAT 3251091; accessed April 23, 2011).

Lee, H. (2008). Cyber crime and challenges for crime investigation in the information era. *In Intelligence and Security Informatics*, 2008. ISI 2008. IEEE International Conference on (pp. xxv-xxvi). doi:10.1109/ISI.2008.4565011.

Lee, J., & Rao, H. R. (2007). Exploring the causes and effects of inter-agency information sharing systems adoption in the anti/counter-terrorism and disaster management domains. *In Proceedings of the 8th annual international conference on Digital government research: bridging disciplines & domains* (pp. 155-163). Philadelphia, Pennsylvania: Digital Government Research Center.

Lewin, K. (1951), *Field Theory in Social Science*, Harper and Row, New York, NY.

Lewis, M., & Slack, N. (2003). *Operations management: critical perspectives on business and management*. Routledge.

Li Xiong & Ling Liu. (2004). PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities. *Knowledge and Data Engineering, IEEE Transactions on*, 16(7), 843-857. doi:10.1109/TKDE.2004.1318566.

Li, X., Hess, T. J., & Valacich, J. S. (2008). Why do we trust new technology? A study of initial trust formation with organizational information systems. *The Journal of Strategic Information Systems*, 17(1), 39-71. doi:10.1016/j.jsis.2008.01.001.

Lieberman, J. (2007). Confronting the terrorist threat to the homeland: Six years after 9/11. 342 Dirksen senate office building, Washington, D.C.: Federal News Service. Retrieved May 8, 2008, from http://www.fas.org/irp/congress/2007_hr/091007transcript.pdf.

Longstaff, P. H. (2003). Can unpredictable systems be managed? Systems, Man and Cybernetics, 2003. *IEEE International Conference on* (Vol. 2, pp. 2013–2020). IEEE.

Longstaff, P. H. (2009). Managing surprises in complex systems: multidisciplinary perspectives on resilience. *Ecology and Society*, 14(1), 49.

Longstaff, P. H., Armstrong, N. J., Perrin, K., Parker, W. M., & Hidek, M. A. (2010). Building resilient communities: A preliminary framework for assessment. *Homeland security affairs*, 6(3), 1–23.

Luna-Reyes, L. F., Andersen, D. F., Richardson, G. P., Pardo, T. A., & Cresswell, A. M. (2007). Emergence of the governance structure for information integration across governmental agencies: a system dynamics approach. *In Proceedings of the 8th annual international conference on Digital government research: bridging disciplines \ & domains* (pp. 47-56). Philadelphia, Pennsylvania: Digital Government Society of North America.

Marks, D. E., & Sun, I. Y. (2007). The impact of 9/11 on organizational development among state and local law enforcement agencies. *Journal of Contemporary Criminal Justice*, 23(2), 159-173.

Martin, K. (2004). “Domestic Intelligence and Civil Liberties.” *SAIS Review* 24(1):7. Retrieved November 14, 2008.

Mckay, J. (2008). Statement of John McKay, Former United States Attorney For the Western District of Washington, Before the Subcommittee on Intelligence, Information Sharing And Terrorism Risk Assessment Committee on Homeland Security United States House of Representatives (Washington, D.C., 2008), Retrieved October 18, 2008, from http://webdev.maxwell.syr.edu/insct/Research/IS%20Page/M cKay%20Testimony.pdf.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-Commerce: An integrative typology. Info. Sys. Research, 13(3), 334-359.

Moore, M. H. (1995). Creating public value: strategic management in government. Harvard University Press.

Morris, B., Tanner, C., & D’Alessandro, J. (2010). Enabling Trust through Continuous Compliance Assurance. Information Technology: New Generations, Third International Conference on (Vol. 0, pp. 708–713). Los Alamitos, CA, USA: IEEE Computer Society. doi:http://doi.ieeecomputersociety.org/10.1109/ITNG.2010.172

Niu, J. (2007). Circles of trust: A comparison of the size and composition of trust circles in Canada and in China. Retrieved from http://proquest.umi.com/pqdweb?did=1276413271

& Fmt=7 & clientId=3739 & RQT=309 & VName=PQD.

O'Brien, J., & Marakas, G. (2008). *Management Information Systems* (9th ed.). McGraw-Hill/Irwin.

Pardo, T., Cresswell, A., Thompson, F., & Zhang, J. (2006). Knowledge sharing in cross-boundary information system development in the public sector. Information Technology and Management, 7(4), 293-313. doi: 10.1007/s10799-006-0278-6.

Park, J., An, G., & Chandra D. (2007). Trusted P2P computing environments with role-based access control (RBAC). IET (The Institution of Engineering and Technology, formerly IEE) Information Security, 1(1):27-35.

Park, J., Chandramohan, P., Suresh, A., & Giordano, J. (2009). Component survivability for mission-critical distributed systems. Journal of Automatic and Trusted Computing (JoATC). In press.

Park, J., Kang, M., & Froscher, J. (2001). A secure workflow system for dynamic cooperation. In Michel Dupuy and Pierre Paradinas, editors, Trusted Information: The New Decade Challenge, pages167–182. Kluwer Academic Publishers, 2001. Proceedings of the 16th IFIP TC11International Conference on Information Security (IFIP/SEC), Paris, France, June 11-13.

Park, J., Sandhu, R., & Ahn, G. (2001). Role-based access control on the Web. ACM Transactions on Information and System Security (TISSEC), 4(1):37–71.

Park, J., Suresh, A., An, G., & Giordano, J. (2006). A framework of multiple-aspect component-testing for trusted collaboration in mission-critical systems. In Proceedings of the IEEE Workshop on Trusted Collaboration (TrustCol), Atlanta, Georgia, November 17-20. IEEE Computer Society.

Phan, M. C. T., Styles, C. W., & Patterson, P. G. (2005). Relational competency's role in Southeast Asia business partnerships. *Journal of business research*, *58*(2), 173–184.

Ray, I., & Chakraborty, S. (2004). A vector model of trust for developing trustworthy systems. In Samarati, P., Ryan, P., Gollmann, D., & Molva, R., editors, Computer Security- ESORICS, Proceedings of the9th European Symposium on Research in Computer Security, September 13-15, 2004, Sophia Antipolis, France. LNCS3193, Springer.

Razavi, M. N., & Iverson, L. (2006). A grounded theory of information sharing behavior in a personal learning space. In Proceedings of the 2006 20th anniversary conference on Computer supported cooperative work (pp. 459-468). Banff, Alberta, Canada: ACM. doi: 10.1145/1180875.1180946.

Rocco, E. (1998). Trust breaks down in electronic contexts but can be repaired by some initial face-to-face contact. In Proceedings of the SIGCHI conference on Human factors in computing systems (pp. 496-502). Los Angeles, California, United States: ACM Press/Addison-Wesley Publishing Co.

Ruppel, C., Underwood-Queen, L., & Harrington, S. J. (2003). e-Commerce: The roles of trust, security, and type of e-Commerce involvement. e-Service Journal, 2(2), 25-45.

Schooley, B. L. (2007). Inter-organizational systems analysis to improve time-critical public services: The case of mobile emergency medical services. Retrieved from http://proquest.umi.com/pqdweb?did=1390309161 & Fmt=7 & clientId=3739 & RQT=309 & VName=PQD.

Schoorman, F. D., Mayer, R. C., & Davis, J. H. (2007). An integrative model of organizational trust: Past, present, and future. *Academy of Management Review,* 32(2), 344-354. doi: Article.

Scott, E. D. (2006). Factors influencing user-level success in police information sharing: An examination of Florida's FINDER system. Retrieved from http://proquest.umi.com/pqdweb?did=1251886251 & Fmt=7 & clientId=3739 & RQT=309 & VName=PQD.

Serra da Cruz, S., Chirigati, F., Dahis, R., Campos, M., & Mattoso, M. (2008). Using explicit control processes in distributed workflows to gather provenance. In Provenance and Annotation of Data and Processes (pp. 186-199). Retrieved February 22, 2009, from http://dx.doi.org/10.1007/978-3-540-89965-5_20.

Shaw, P. (1997). Intervening in the shadow systems of organizations Consulting from a complexity perspective. *Journal of Organizational Change Management,* 10(3), 235.

Sparrow, M. K., Moore, M. H., & Kennedy, D.M. (1992). Beyond 911: a new era for policing. Basic Books.

Stacey, R. (1996). *Complexity and creativity in organizations* (1st ed., p. 312). Berrett-Koehler Publishers.

Stair, R., & Reynolds, G. (2011). *Principles of information systems*. Course Technology.

Staples, D. S., & Webster, J. (2008). Exploring the effects of trust, task interdependence and virtualness on knowledge sharing in teams. *Information Systems Journal*, 18, 617 – 640. doi:10.1111/j.1365-2575.2007.00244.x

Swire, P. P. (2006). “Privacy and Information Sharing in the War on Terrorism.” Ohio State Public Law Working Paper No. 63. Retrieved March 14, 2008 (http://ssrn.com/paper=899626).

Thomas, J. (1985). Force field analysis: A new way to evaluate your strategy. Long Range Planning, 18(6), 54-59. doi: 10.1016/0024-6301(85)90064-0.

Thompson, E. D., & Kaarst-Brown, M. L. (2005). Sensitive information: A review and research agenda. *Journal of the American Society for Information Science and Technology*, 56(3), 245–257.

Treglia, J. (2009). "Two Cans on a String: Technical Social & Legal Barriers to Effective Information Sharing Among Federal, Tribal, State & Local Law Enforcement Agencies in the United States," Poster in proceedings of iConference 2009 - iSociety: Research, Education, Engagement. University of North Carolina at Chapel Hill, NC, February 8-11, 2009.

Treglia, J. V., & Park, J. S. (2009). Towards trusted intelligence information sharing. Proceedings of the ACM SIGKDD Workshop on Cyber Security and Intelligence

Informatics (pp. 45-52). Paris, France: ACM.

U.S. Dept. of Justice, Bureau of Justice Statistics (2006). Law Enforcement Management and Administrative Statistics (LEMAS): 2003 Sample survey of law enforcement agencies [Computer file]. ICPSR04411-v1. Ann Arbor, MI: Inter-university Consortium for Political and Social Research [producer and distributor], 2006.

United States. (2007b). Building the information sharing environment: Addressing the challenges of implementation: Hearing before the subcommittee on intelligence, information sharing, and terrorism risk assessment of the Committee on Homeland Security, U.S. House of Representatives, One Hundred Ninth Congress, Second Session, May 10, 2006 (p. 27). Washington: U.S. G.P.O.

United States. (2007c). Federal support for homeland security information sharing: role of the information sharing program manager: Hearing before the subcommittee on intelligence, information sharing, and terrorism risk assessment of the Committee on Homeland Security, House of Representatives, One Hundred Ninth Congress, First Session, November 8, 2005 (p. 58). Washington: U.S. G.P.O. Retrieved from http://www.gpoaccess.gov/congress/index.html.

USDOD. (2007). *Department of defense information sharing strategy* (p. 24). Washington, D.C.: Department of Defense, Information Sharing Executive, Office of the Chief Information Officer.

USDOJ. (2008). Department of Justice Federal Assistance from U.S. Department of Justice, FY 2008, summary. (n.d.). . Retrieved February 22, 2009, from http://www.usaspending.gov/faads/faads.php?datype=T & det ail=-1 & database=faads & fiscal_year=2008 & maj_agency_cat=15.

van de Wijngaert, L., & Bouwman, H.(2009). “Would you share? Predicting the potential use of a new technology.” *Telematics and Informatics* 26(1):85-102.

Venezia, P. (2010, July 2). Why do we trust Google? | Internet integration - InfoWorld. *InfoWorld. Online News*. Retrieved December 18, 2010, from http://www.infoworld.com/t/internet-integration/why-do-we-trust-google-415?page=0,1

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, 26(2).

Whitehouse. (2007). *Report of the security clearance oversight group consistent with Title III of the Intelligence Reform and Terrorism Prevention Act of 2004*. Retrieved March 16, 2008, from http://www.whitehouse.gov/omb/pubpress/2007/sc_report_to_congress.pdf.

Yang, T. M., & Maxwell, T. A. (2011). Information-sharing in public organizations: A literature review of interpersonal, intra-organizational and inter-organizational success factors. *Government Information Quarterly*, 28(2), 164–175.

Young-Ybarra, C., & Wiersema, M. (1999). Strategic Flexibility in Information Technology Alliances: The Influence of Transaction Cost Economics and Social Exchange Theory. *Organisation Science*, 10(4): 439-459.

Zhang, J., Dawes, S. S., & Sarkis, J. (2005). Exploring stakeholders' expectations of the benefits and barriers of e-Government knowledge sharing. *The Journal of Enterprise Information Managemen*t, 18(5), 548−567.

Zheng, L. (2009). *Leadership Behaviors in Cross-boundary Information Sharing and Integration: Comparing the US and China*. ProQuest.

Zargar, S. T., Weiss, M. B. H., Caicedo, C. E., & Joshi, J. B. D. (2009, December*). Security in Dynamic Spectrum Access Systems: A Survey,* Working Paper. Retrieved October 9, 2012, from http://d-scholarship.pitt.edu/2823/

ESSAY 2: Towards More Rapid and Effective Communication between Responders to Emergency Situations[11]

1. Introduction

That communication and information sharing gaps occur between and across responders and stakeholders in emergency response incidents is well known (Barr, Burther, & Mahy, 2011; Kovacs & Spens, 2011; Nivolianitou & Synodinou, 2011; Gaynor, Brander, Pearce, & Post, 2008); what to effectively do about it is not. This article reports on conclusions drawn from empirical sources and the literature towards that goal. This article provides recommendations that speak to the gaps noted by the work of others as well as through first hand observations. This research investigated factors associated with fostering rapid and effective communications between various responders to emergency situations. The article presents conclusions by first describing the problem and presenting a review of past and current literature followed by a description of research methodology, then a discussion of findings and observations that were made, and, lastly, a summary of the conclusions and recommendations are presented. The findings from this research should be used to inform the design of policy and system features and functionality for those engaged with emergency response at all levels. As for the academic community, the work should be considered part of a continuing investigation into understanding and improving collective response to crises considering the social, technical and policy factors.

Timely and effective response to crises, disasters, or infrastructure failures requires shared situational awareness on the part of decision makers and real-time information exchange between

[11] This is an expanded version of the article by Treglia, J. V., McKnight, L. W., Kuehn, A., Ramnarine-Rieks, A. U., Venkatesh, M., & Bose, T. (2011). Interoperability by "Edgeware": Wireless Grids for Emergency Response. *2011 44th Hawaii International Conference on System Sciences (HICSS)*.

formal and informal participants (Leavitt, Spelling, & Gonzales, 2007; United States, Executive Office of the President, & United States, Assistant to the President for Homeland Security and Counterterrorism, 2006; Kean & Hamilton, 2004). Enabling policymakers, law enforcement, and citizens to interact in a crisis is a complex challenge, but one which can be met by a focus on the principle issue, which is the barriers to information sharing within and across secure networks and communities of trust (Wasserman, 2010). Technically providing for interoperability and coordination is necessary but not sufficient for overcoming this challenge.

This article introduces a new approach to emergency response – called social emergency response. A social emergency response is analogous to what might occur across general purpose social networks such as Facebook and Twitter, but in a localized context, and augmented by information-sharing methods and devices supporting the user which are not readily available – yet – to all users, whether in a crisis or otherwise. Services such as Facebook, Twitter and Crowdmap.com from Ushahidi may indeed provide valuable input to a social emergency response, but are each only a component of a social emergency response system.

New devices and systems can enable a new paradigm for response to involve what is now described as a social emergency response. Delivery of situational awareness and exchange of vital information to and between disaster managers, response personnel, and citizens in a disaster area, through a new type of networking in difference with established response policy paradigms.

The demonstration and evaluation of systems in use by law enforcement personnel during emergency response training exercises provides essential insight from practitioners dealing with the operational implications of new technologies and policy. Current tools and practices have been evaluated in both urban and rural communities, enabling generalizations to be drawn (NCR Project Team, 2009).

More effective response capability, and changes to established response protocols and governance, will be expected in due course. The anticipated merits and viability of a new social emergency response policy should be sufficiently evident to motivate further policy progress, widespread adoption, and diffusion of these systems and approaches, it is argued here.

Key technical elements for social emergency response approaches are available in some early forms presently and in more sophisticated ways in the near future. There are advanced and more dispersed sharing/communication capabilities available already. These are being developed by various academic and private-sector entities with the ability to capture and share multiple wireless transmission media, including police, fire, EMS, municipal, private, cellular, CB bands, and others. The ability to have file sharing, social and multi-media integration to connect with 911 centers, and first responders is becoming a reality. These are necessary but not sufficient hardware and software components of a social emergency response system, the policy and cultural changes must occur as well.

Social and cultural aspects of coordination and engagement must be taken into account. Emergency situations are both complex and dynamic and it is difficult to account for exigencies in advance (Longstaff, 2003, 2009). Formal, informal, and non-traditional actors and their contribution to, and influence on, law enforcement and emergency response entities during an emergency have gained greater attention of late. The knowledge of how to include these participants in response solutions remains a challenge.

Additionally, there is not yet a broad acceptance of these potentially more inclusive response models. Longstaff, Armstrons, Perrin, Parker, & Hidek, offer a preliminary framework for assessing community resilience as one such tool for policy makers (2010). Consistent with the theme of this article that framework is community-based, holistic, and scalable. Therefore, an important element of a social emergency response policy is a re-conceptualization and focus on citizens and non-traditional stakeholders as central to the new paradigm for all stakeholders at a crisis to coordinate themselves. Research summarized in this article is intended to contribute to both social and technological change in emergency response policy and practice.

Adoption of new collaborative technologies, but even more important, new policy approaches to emergency management – or as it may be called, a social emergency response policy – will be both more effective and lower in cost. Since citizens own resources, and devices are now shared tools and critical components for social emergency response, they will always be off-budget items for public agencies. Once the utility and viability of the novel software, services, and devices for social emergency response have been demonstrated, one may expect calls for parallel research efforts to buttress and support what would be a – socially acceptable, social emergency response policy – will be recognized as being needed, as well. Although researchers here are confident in current and upcoming technical designs, which essentially are a synthesis and integration across various areas of expertise, it is recognized that the larger challenge is devising a social emergency response policy or creating the conditions under which such may emerge.

Results of this research suggest specific elements of such a policy and environment. A wider and continued debate is necessary as observation of and lessons learned from additional exercises and actual incidents further inform and make the benefits apparent. The policy and cultural change to accompany the new devices and services may involve a community policy, a state or national policy, or an industry self-regulatory policy; the crystal ball is too fuzzy to foretell. But one can definitely see telecommunications and network technologies being adopted and used in the near future, and suggest it is time to begin to consider both these systems, and the appropriate policy response to their emergence publicly.

2. Problem

An effective social emergency response policy must reflect the reality that the true first responders to most disasters are neighbors or passersby, many of whom have small handheld computing devices, also known as a smart phone, tablet, or laptop, and includes victims. The old hierarchical model for emergency response, assuming helpless victims in need of rescue, breaks down when the citizens may, in fact, be better informed and coordinated than their supposed "rescuers" or there may be no other help.

In addition to having new technology such as edgeware software (such as is described in the following sections), which can enable the coordination of people-to-people, people-to-resources, and machines-to-machines, new paradigms for response are also necessary (McKnight, Bradner, Howison, 2004; McKnight, Lehr, Howison, 2007). Connecting non-traditional, but common, devices is particularly useful when extreme – emergency – conditions may degrade public networks or render them otherwise inoperable. Further, if an emergency occurs in a rural area, the volume of data traffic generated by emergency response personnel alone may quickly overwhelm even a well-functioning network infrastructure. Technical and social solutions must move toward enabling and leveraging the technology that is at hand and making it available to a broader audience.

There is presently a surprising lack of utilization of existing technologies that can be used to produce and deliver the information products emergency managers need. A startling example is that the majority of 911 centers in the United States to not have capability to accept or send text messages, tweets or images from cell phones. Current 911 center computer-aided-dispatch (CAD) systems have texting capability. As an example, some 911 centers are using this for sending formatted texts to ambulance crews with arrival and dispatch times and other data needed for reporting. For most centers, however, this is only “unofficially” used, as it is not a sanctioned emergency communications channel (the discussion of SMS-to-911 and related matters is important but beyond the scope of this article). A National Research Council report found that “overhead images provide the best early source of information on damage; yet the necessary investments in resources, training, and coordination are rarely given sufficient priority either by the general public or by society’s leaders” (National Research Council, 2007). Often the best source of situational awareness is remotely sensed data from the affected area delivered in real-time or near real-time. This could also be images taken by civilians or responders on the scene using their own devices. Overhead imagery and associated remote sensing based information are also crucial to long term recovery from an incident and for planning mitigation strategies and only valuable when accessible to those involved.

The first priority in a crisis is to contain the situation and rescue those in need, while there is still time to do so. Law enforcement personnel, and local residents – save themselves, through a social emergency response process. The need for real or near real-time situational awareness can improve crisis response. Gaining a wide view including aerial images to identify hardest hit communities – or paths to escape – is just one resource that can help both. Social media are also being investigated for utility in this environment (Viel, Buehner, & Palenchar, 2011). This can involve images that identify and locate those in critical need as well as connecting resources and engaging in voice transmission.

Problems for emergency response given the disparate systems won’t just go away. The objective here is to identify the problems in the emergency response arena and suggest solutions that may be undertaken using existing and emerging technology and policy as well as considering the social and human factors.

A positive vision of the crisis response future includes better support for inclusion of activities and information from the public in disaster response and mass emergency events and relies upon technology as well as changes to existing response policy, structures, processes and expectations (Palen, Anderson, Mark, Martin, Sicker, Palmer, & Grunwald, 2010). This research has created a framework for understanding stakeholders, agents, and entities influencing law enforcement agencies to include technical, social, and policy concerns (Treglia, 2010). There is growing interest in understanding citizen and government partnerships and in finding a successful means for government to engage with the private sector (Pittman, 2011).

An additional focus here is on identification of formal and additional, informal and non-traditional, actors and their influence on law enforcement and emergency response entities and related issues in crisis response. Other researchers have focused on these areas, which are now recognized as having relevance to a coordinated response to crisis incidents. Organizational influences are described in the work of Deverell and Olsson regarding organizational cultures effects on an organizations ability to change in response to crisis, where flexible structures have proven to be more adaptive (Deverell, Edward, & Eva-Karin Olsson, 2010). In regard to information sharing, Mariconi finds that IT must be in line with the professional cultures of the responding agencies in a crisis to be effective and that available technology, context, professional culture, and interaction are key factors impacting response (Marincioni, 2007). Security and trust in the information has been a recognized concern in this arena as well as information quality (Robinson & Disley, 2010). Considerations for building communities of trust is described in Wasserman (2010).

3. Literature

3.1. Emergency Response and Open Issues

There is a growing body of literature regarding information sharing in emergency response contexts. Adam, Atluri, Chun, Ellenberger, Shafiq, Vaidya, and Xiong (2008) investigated secure information sharing in emergency management contexts. Glomseth, Gottschalk, and Solli-Saether looked at occupational culture as a determinant of knowledge sharing by law enforcement agencies in an international study (Glomseth, Gottschalk, & Solli-Saether, 2007). Research on emergency services sponsored by the National Science Foundation (NSF) reports "technical environments such as other agencies' information assurance level and technical standards seem to encourage information sharing systems use" (Lee & Rao, 2007). Pardo, Gil-Garcia, and Burke, looked at the effects of governance structures in state and local criminal justice information sharing (Pardo, Gil-Garcia, & Burke, 2008). Local to state agency information sharing was the subject of the work by Akbulut, Kelle, Pawlowski, Schneider, and Looney (2009). Rational choice, trust and other issues for organizations were studied by Williams, Dias, Fedorowicz, Jacobson, Vilvovsky, Sawyer, and Tyworth (2009), and Gil-Garcia, Guler, Pardo, and Burke (2010).

Recent case studies on knowledge sharing within public sector interorganizational networks confirm information sharing difficulties across agencies (Jing & Pengzhu, 2007; Pardo, Cresswell, Thompson, & Zhang, 2006). Emergency response agencies overlap jurisdictions and responsibility; each with a duty to their own constituencies. Traditionally, there has been a top-down approach to attempts at implementation of information sharing mandates, typically from the Federal level downwards. Success in this has been limited.

Some of the recurring problems that have been identified include:

1) Agencies have not established sufficient trust.
2) Time sensitive information affects the sharing potential.
3) Technical issues such as incompatibility, lack of standards and system reliability exist.
4) Policies are not consistent or in pace with technology or society and may conflict with sharing interests.
5) Personnel issues that involve social and security concerns can interfere with the information sharing processes.

Problems can be classified into three major areas: technical, social, and policy (Treglia & Park, 2009). Technical factors include interoperability issues, availability, and control. Social factors involve social/cultural issues, trust, informal or "shadow" networks and criticality. Policy factors involve concerns over law and policy conflict and under what governance model or structure activities are allowed or restricted. Theoretical and empirical work has been done to identify factors that influence the sharing of information between local and state agencies (Akbulut et al., 2009). Those authors identify similar technical, agency and environmental factors that influence information sharing. A workshop on community resilience and security also investigated “what attributes (human, social, cultural, political, economic, technological) within a community are essential to ensuring resilience, and how are they interrelated (Longstaff, Mergel, & Armstrong, 2009)?”

Issues of security and trust are included in the discussion here as there are particularities attending the emergency response arena deserving special attention.

3.2. Technology Advances

The evolution of communication networks has gone from centralized, hierarchical systems under the management of a single entity toward decentralized, distributed systems under the collective management of many entities. Intelligence has shifted to edge-nodes, which increasingly are capable of acting as autonomous agents making complex decisions to create, deliver, or receive services (McKnight, Sharif, & Wijngaert, 2005; McKnight & Howison, 2003; McKnight, Lehr, & Howison, 2007). Previously, grid computing focused on large-scale sharing of computing resources such as software, hardware, databases, and data sources (Foster & Kesselman, 2004). The growth of wireless increased opportunities for computing to become ubiquitous (always available, always connected). Heterogeneity of networking resources needs to be managed (mobility and wireless/wired interconnection). There are an increasing number of end nodes (connected computers in everything from bodies to clothes, appliances, cars, and walls). This has led to a transition; wireless grids are organized as ad hoc networks and represent an advanced state of evolution in communication networks (McKnight & Howison, 2003; McKnight, Lehr, & Howison, 2007). Wireless grids are defined as the ad-hoc dynamic sharing of physical and virtual resources among heterogeneous devices. Wireless grid applications may be considered in three categories of applications: (1) those that collect or aggregate data; (2) take advantage of their location or where they can move to; and (3) take advantage of cooperation among a mesh of mobile devices.

Related work regarding wireless grids include works on user and socio-technical perspectives and challenges (McKnight, Sharif, & Wijngaert, 2005; McKnight & Howison, 2003), coordination of user and device behaviors (McKnight, Lehr, & Howison, 2007), and future internet applications and bridging communicative channels (McKnight, Howison, & Bradner, 2004; Dutton, Gillett, McKnight, & Peltu, 2004; McKnight, 2007). There has been increasing acknowledgement of the nascent growth of wireless grids as a new engineering field of scientific inquiry and innovation (Fitzek & Katz, 2007; Manvi & Birie, 2009; Li, Sun, Yu, & Cai, 2009; Birie & Manvi, 2010, 2011; Li, Gong, Lai, Han, Qiu, & Yang, 2012; Sun, Mao, Liu, Liu, & Guan, 2012).

The grid, as conceptualized, is an emerging infrastructure that will fundamentally change the way people think about and use computing resources (McKnight, 2007). The concept of this virtual workspace is that of a configurable execution environment created and managed by reflecting client requirements (Foster & Kesselman, 2004; ISOC, 2010). A broader understanding of the nature of the opportunities offered by grid computing, virtual environments, and the technologies or standards needed to realize those opportunities is now required (Foster & Kesselman, 2004; Brooks, Caicedo, & Park, 2012).

“Edgeware” describes software that resides beyond the cloud, across edge network devices, both wired and wireless (Treglia, Ramnarine-Rieks, & McKnight, 2010). Wireless Grids ‘edgeware’ technology sits at the outermost limits of networks, allowing all facets of a user’s environment to be interoperated and shared easily. This new class of software for ad hoc distributed resource collaboration allows for coordination of devices and content on a new scale. There are many kinds of devices that can be shared using this service– for example, mobile phones and Internet devices, printers, displays, remote sensing devices, local weather sensors, wireless sensor networks, etc.

The fundamental difference that this form of interconnection has over traditional networking is that it allows for true resource sharing and not simply access. In the case of wireless grids, you access distant resources and programs similar to using the device directly. In this way, legacy concerns and incompatibility issues are overcome. Security and access controls have been established such that owners determine use and constraints. Ownership, user autonomy, and sovereignty regarding the sharing and process are maintained. The wireless grids technology identified here transforms disparate devices into a shared and interactive grid of accessible resources. Technical standards and open application programming interfaces (API) are needed to enable the adoption and growth of this new technology.

3.3. Standards and Protocols Development

Governments are responding to the need for standards in public warning systems. Examples of these activities include: “Partnership for Public Warning” in the U.S., “Forum for Public Safety Communication Europe”, and also the Internet Society's "Public Warning Network Challenge" (ISOC, 2010). These examples signify recognition of the importance of crisis-ready, multi-channel, regional and international public warning dissemination networks.

Protocols are being established and adopted in the emergency services realm. The Common Alerting Protocol (CAP) is an Extensible Markup Language (XML) based format that allows for messages to be disseminated consistently, maintaining integrity across communications warning applications through the use of compatible alert formats. The goal here was to create a neutral and open format for warning systems interoperability. It was created through an unofficial and non-commercial initiative. The use of the CAP was initially limited but gained wider acceptance following its adoption by the Organization for the Advancement of Structured Information Standards (OASIS) as a standard in 2004, and it has since been implemented in the U.S. and other countries (Botterell & Addams-Moring, 2007). Open source initiatives are proving to be valuable for public warning and commercial ICT-based (Information and Communications

Technology - based) warning services continue to exist as well (Botterell & Addams-Moring, 2007).

Because emergency response situations are emergent and dynamic, it is difficult to account for every exigency in advance. Emergency management as a complex system is being studied in the category of resilient ecological systems (Longstaff, 2009). According to Longstaff (2003) “complex systems often operate under very simple rules but exhibit unpredictable or surprising behavior when several forces interact in the system.” At the crisis scene, it may be that planned technologies may not function or are inadequate under the given circumstances. Emergency response personnel may need to mix and match other disparate and possibly unfamiliar technologies to fit the tasks at hand (Mendonça, Jefferson, & Harrald, 2007).

When it comes to emergency response, additional requirements need to be taken into account. Among others, this includes coordination of resources in ad hoc situations. Interoperability for emergency response is defined as, “The ability of disparate and diverse emergency response units to interact in emergency situations towards common goals, involving the sharing of information and knowledge between involved organizations and units via defined or ad hoc processes to achieve coordinated actions, by means of the exchange of data between their respective information and communication technology (ICT) systems” (IDABC, 2008).

To achieve interoperability among diverse emergency response units and organizations, there are developed and agreed on “Interoperability Principles”. Together with the general objectives of emergency response services, the interoperability principles are policy guidelines that define what should (and what should not) be achieved. For agencies that may have differing techniques for operating, these principles serve as a uniform guide. They can provide additional guidance and compliance checks for implementation on a system, process, and organization level.

These guidelines are necessary to make it clear to all participants what is meant when speaking about interoperability. This goes far beyond technical issues (Kuehn, Spichiger, & Riedl, 2009). A best practice example of how such interoperability principles work is given in the European Interoperability Framework (EIF) in the context of e-government (IDABC, 2008). Similar principles need to be developed for the emergency response sector in a broadly supported multi-stakeholder forum.

Principles are hardly enough to address the complex challenges that interoperability poses. Longstaff identifies the political and environmental complexity as challenges for managing surprises in such complex systems (2009). A conceptual framework is needed to investigate different facets of this challenge as not only technical and semantic factors but also organizational and policy factors and the current political context need to be taken into account. The EIF introduces a framework that considers five levels – political context, legal, organizational, semantic, and technical – that need to be considered to establish interoperability (IDABC, 2008). From an analytical point of view, the five levels offer helpful insights: "where" and “what" interoperability issues may arise and "which" actor may respond to them (i.e. a legally non-compliant transaction on the organizational level that needs to be addressed by a legislative function).

Establishing open, non-proprietary protocols for emergency response communication and information dissemination systems would allow systems to evolve more readily, and incorporate more intelligent and robust capabilities, which would make them more effective.

4. Methodology

A truly mixed-methods approach is being taken. Methods and activities included field observation, case study, policy analysis, interviews and document analysis. The work also included analysis of existing survey data compiled by the Public Safety Networks Study and Police Executive Research Forum and include preliminary findings from a case study of the Central New York Interoperable Communications Consortium (CNYICC). Using an inductive approach and considering aspects of general systems theory, this qualitative research design is suited to the study of complex problems (Schutt, 2006). The case study method and Delphi Technique are effective for gaining insider knowledge from small number of individuals regarding their actual experience. The goal is to obtain the richest data surrounding the research issue and to capture the complexity in context (Benbasat et al., 1987).

Researchers participating here include members of both the law enforcement and academic communities. Researchers included semi-structured interviews with emergency services and law enforcement personnel at the front line and administrative levels, analysis of after-action reports, existing policies, and direct observation (NCR Project Team, 2009). The participants included public officials, service providers, and community leaders. Interviews were conducted in a manner as described by Harrison, Gil-Garcia, Pardo and Fiona (2006). The interviews were semi-structured, open ended, and not exceeding two hours. The interest was in obtaining cooperation and information-related responses from the respondents relative to emergencies with special attention to needs and resources during the response. Social factors, inter-organizational relationships during the response, the effect of pre-existing resources, plans, or programs on the ability to respond, and the effect of rules and laws on the response were factor areas investigated.

The findings in this research are based on field observation and participation in actual crisis incidents. The researcher also participated and observed tabletop and field exercises and reviewed documentation of actual and exercise only after action reports. Common themes and issues were identified through reflection and review of the incidents and commentary.

Researchers reviewed the materials and reflected on key issues, social, policy and technical challenges that emerged from the observations and reports as recurring themes or incidents. Most formal incident reports followed a structured format providing identifiable sections for issues identified, gaps and areas for further analysis, training or restructuring. This made the task of identifying common themes across cases easier and more effective. Having multiple sources for data such as formal reports combined with observation and public records allowed for findings to be validated or questioned. The period involved for these activities includes the years 1999 to 2012. Actual multi-agency crisis event participant observations, and table top and field exercises participated in are shown in the tables below:

Incident	Location	State	Year
CSX freight train derailment with tank car explosion and toxic gas leak	Oneida	NY	2007
Suicidal man with gun at Colgate University	Hamilton	NY	2010
Officer shooting involving a multi-jurisdiction chase and the SUNYIT college campus	Marcy	NY	2010

Table 1: Actual Multi-Agency Crisis Events

Incident	Location	State	Year
Multi-agency emergency disaster response drill at Syracuse University	Syracuse	NY	2011
Large-scale active shooter emergency exercise at Morrisville State College	Morrisville	NY	2011
Winter Fury wide-area multi-jurisdiction severe weather environmental crisis tabletop exercise	Cicero	NY	2012
Multi-jurisdictional mass casualty interstate highway disaster tabletop exercise	Canastota	NY	2012
Railroad accident - explosion and toxic gas multi-agency tabletop exercise	Syracuse	NY	2012

Table 2: Table Top and Field Exercises

After-action reports and documentation from actual crises and exercises were examined and researchers considered the material over several months to come up with patterns and meaning from the data sources. This activity included the following sources shown in the table below:

Report	Year
Report on the Columbine High School Shootings, Jefferson County, CO	1999
Arlington County After-Action Report on the Response to the September 11 Terrorist Attack on the Pentagon - Arlington Virginia Fire Department, Arlington, VA	2001
Response to the Terrorist Attack on the Pentagon: Pentagon Family Assistance Center (PFAC) After-Action Report - Office of the Under Secretary of Defense - Personnel and Readiness, Washington, DC	2003
The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States (9/11 Report), Washington, D.C,	2004
Platte Canyon High School Shooting After-Action Report. Park County (CO) Emergency Management, Park County, CO	2006
Operation Shared Service After-Action Report - Central New York Regional Medical Reserve Corps - State University of New York - Upstate Medical University, Syracuse, NY	2006
The federal response to Hurricane Katrina: Lessons learned - U.S. Executive Office of the President	2006
Report to the President on Issues Raised by the Virginia Tech Tragedy, National Institute of Justice/NCJRS	2007
Empire Express Hurricane Functional Exercise (FE) After-Action Report (AAR), Federal Emergency Management Agency (FEMA)	2009
New York State Department of Health, Office of Health Emergency Preparedness 2008-2009 Interoperable Communications Drills, New York City Department of Health and Mental Hygiene	2009
State of Louisiana After-Action Report and Improvement Plan, Hurricanes Gustav and Ike, Louisiana Governor's Office of Homeland Security and Emergency Preparedness (OHSEP)	2009
2009 Presidential Inauguration Regional After-Action Report, Washington, D.C.: Department of Homeland Security, National Captial Region, NCR Project Team	2009
Independent Assessment Report of the Emergency Alert System and Crisis Communications Capabilities of the University of Alabama in Huntsville, James Lee Witt Associates	2010
Civil Preparedness Communication Drill After-Action Report/Improvement Plan, The Monroe County Department of Public Health (MCDPH)	2010
Shooting on the Woodbridge Campus After-Incident Review, Northern Virginia Community College	2010
Active Shooter/Suicide on the University of Texas at Austin Campus, Police Department, The University of Texas at Austin	2010
Hurricane Irene/Tropical Storm Lee Response, Lancaster County Emergency Management Agency	2011
A Review of the UNCW Police Response to the July 29, 2011 Shooting at 4750 Seahawk Court (Seahawk Square), University of North Carolina Wilmington	2011
University of Texas at Austin Active Shooter/Suicide After-Action Report, University of Texas	2011
After Action Report for Active Shooter Functional Exercise, Chapman University	2012
Tropical Storm Irene: Western Massachusetts After-Action Report/Improvement Plan, August 27-28, 2011, Western Massachusetts Regional Homeland Security Advisory Council	2012

Table 3: After-action Reports and Documentation from Actual Crises and Exercises

The process of observation and cross-checking with consideration of training and actual incident accounts and discussions provided the researchers with the support and evidence for issues and gaps identified . The objective behind the data gathering was to understand the roles of information and technology in response to emergencies as well as the influence of the response on the subsequent work of government agencies, private organizations and citizens with the aim of improving it.

5. Findings and Discussion

5.1 Social Emergency Response

The broader purpose of this research is to contribute to academic and practitioner knowledge regarding information-sharing policy and practice across law enforcement agencies and the emergency response community, to now include non-government entities and others as participants. Of course, the validation of the utility of the novel systems and components for social emergency response described here ultimately has a practical objective: to help people save their own lives, or help save their neighbors, when an emergency occurs. If law enforcement and emergency personnel can assist and channel these instincts and energies through essentially becoming the operators of what may be the only functional network in a town, that is likely to benefit both the public authorities, and of course, the people whose lives may be saved in an emergency, because a more rapid and effective response is now possible. It is not being claimed or anticipated that all problems will be resolved by the new hardware and software systems, far from it; resolution of legitimate policy concerns may inhibit the adoption and diffusion of such a social emergency response approach. All the more reason, therefore, to simultaneously consider the extant social and policy barriers.

Important questions arise for communities in times of crisis. These include concerns about what is going on? where can one find help? how does one contact family and friends? (Longstaff, Mergel, & Armstrong, 2009). Researchers report seeing a positive response and high level of interest showing to date in these exercises by stakeholders who seem to appreciate the opportunity to be part of the –social emergency response - solution.

Multiple commercial partners and possible early adopters have inquired about when these systems will be available, in the U.S., Europe, Africa and Australia. This widespread interest in an alternate approach is not surprising as emergencies can occur – and do – anywhere. The present "single network" approach to achieving interoperability creates the potential for a single point of failure in a disaster. Having just one primary means of communication is a poor engineering approach. This vulnerability allows for potential damage to critical infrastructure by terrorists or others who wish to cause harm. Current communications policy in the U.S. reflects this, as there are now requirements for identification of alternate communications channels for such exigencies.

5.2 Technical factors

Existing approaches to the inter-operability issue are predominantly network-based, such as through deployment of hardware based repeaters or gateways. This is expensive, requires extensive prior coordination and planning, and only addresses part of the problem. The example of entities moving to IPv6 is evidence to the fact that transition issues and deployment challenges bring added security implications (Caicedo, Joshi, & Tuladhar, 2009). Primary and secondary users in distributed networks present security problems and can be a roadblock to system adoption (Zargar, Weiss, Caicedo, & Joshi, 2009). Standards-based approaches are best for connectivity, but time required to develop standards can be high and achieving consensus non-trivial. Configurable radios or software defined radios provide an adaptable infrastructure that can interconnect a variety of frequency bands (Caicedo, 2007). This technology is only now being developed for the emergency response environment.

5.3 Social factors

Having ability to communicate and share in emergency response technically is a necessary first step. There must also be a commonly understood and accepted command structure and willingness to share for the system to work (Treglia, McKnight, Kuehn, Ramnarine-Reiks, Venkatesh, & Bose, 2011). Effective communication protocols involve identifying persons who should be included in the response and the accompanying roles and authority expected. Here, a new paradigm is proposed to include non-government agents and other citizen stakeholders. The victims are important first responders as well.

Crisis response and notification as social practice raises many interesting questions requiring research (Ryan, 2006). Contemporary trends in citizen science and citizen engagement in "participatory" knowledge creation and information dissemination are critical developments in the pro-social use of advanced technology, but the social organization of this space and the social dynamics of the diverse groups involved – which may include law enforcement and designated first responders with their more formal views on notification as "official" practice as well as community leaders and ordinary citizens with their less formal practices in this regard - have not received sustained attention from the public safety, technical and socio-technical research communities.

Notification and participation norms arguably differ across professional and community groups. These are the formal and informal participants. Community leaders, ordinary citizens, and law enforcement professionals at critical sites intend the system for use. Design specifications for the proposed system is based on research into the social organization of notification in two communities in Syracuse, NY – the immigrant groups on the North side and the largely African-American population on the Southside (Treglia, McKnight, Kuehn, Ramnarine-Reiks, Venkatesh, Bose, 2011). Research will be under-taken as part of the lead-up to the two field tests and as part of the debriefing following the field tests. Cultural groups may be fearful of technology and avoid innovation that could improve communication (Kaarst-Brown & Robey, 1999).

Findings from this research will be used in designing policy, system features and functionality and the interface of the refined edgeware software application.

5.4 Policy Factors

At a major crisis, there are multiple layers of governance with overlapping jurisdictions, responsibility, and authority. By way of example, there are 17,876 state and local law enforcement agencies and 26,464 fire departments in the U.S. (BJS, 2007; USFA 2011). Agencies have varied degrees of sovereign leadership, policies, procedures, and resources. Governance, coordination, and information sharing in this multi-interest and dynamic environment are difficult. This shared responsibility and overlapping jurisdiction affects the ability of law enforcement entities to cooperate effectively. At the federal level, there may not be clear sole jurisdiction and even across federal agencies questions of responsibility or control are unclear. To facilitate interagency operations it is necessary to share information, sensitive information and intelligence information across agencies and levels. In regard to information coordination it is noted that “while the U.S. government is generally considered to have the most advanced security classification system, there has been a steady chorus promoting the need for fundamental research on the security classification system” (Thompson & Kaarst-Brown, 2005, p. 246). These ambiguities interfere with collaboration in joint activities or operations. The model shown in Figure 22 below illustrates states having jurisdiction and responsibility that overlaps with lower level units of government. The cities are separate from towns or villages, although they are located within a county and state. The federal arena exists in a separate sense with designated responsibility that still may overlap or co-exist with other entities. Although not depicted here, international agencies add yet another element to be addressed when cross-border incidents are manifest. Non-government entities and other stakeholders also cross these boundaries.

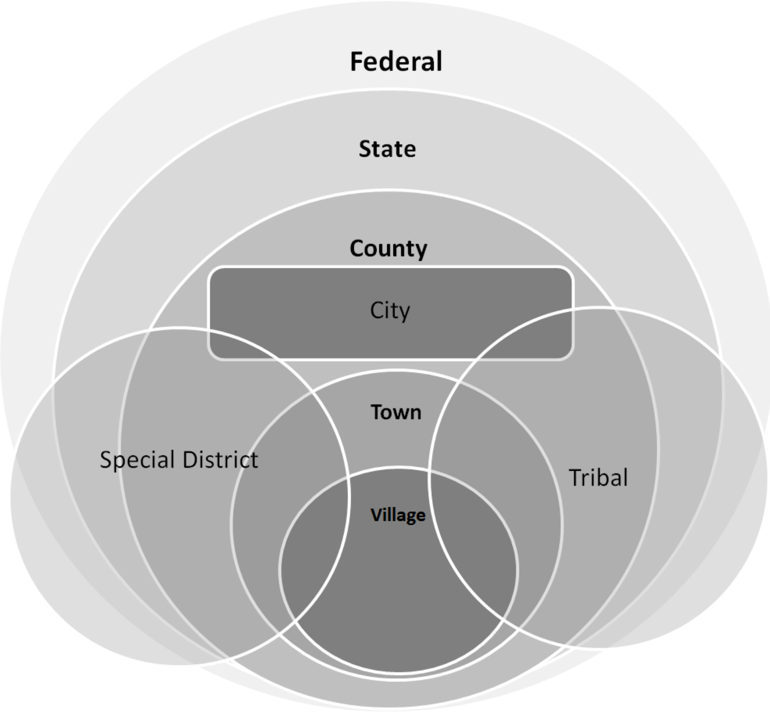


Figure 22: Overlapping Responsibility and Jurisdiction in United States

(Treglia, 2010)

5.5 Two Tier Parallel Circles

In this multi-interest environment, emergency response is best described as a two-tier circle having concurrent parallel operations: 1) the formal recognized law enforcement and emergency responders who are formally and traditionally organized and who operate with a given governance structure having identifiable jurisdiction and responsibility; and 2) the non-government, non-traditional stakeholders and involved persons and entities, who may be victims, and other ancillary or ad-hoc information and service providers or support agencies acting towards goals for the particular incident or crisis event.

In describing the parallel processes, the first circle or level is the formal traditional and officially recognized emergency response system and players, which formally include the police, fire, and EMS. The second layer or level includes other formal and informal stakeholders and non-government support or service entities necessary to the response efforts. This area includes citizen and citizen group participants, which have not previously been considered in this way, and other entities such as the Red Cross, power plant, or water authority where needed. Homeland Security and FEMA may be considered support services providers. This is depicted in Figure 23.

As described above, overlapping jurisdiction, responsibility, and control lead to ambiguity and conflict of interest (Treglia, McKnight, Kuehn, Ramnarine-Reiks, Venkatesh, & Bose, 2011). Necessary resources may be under government control, private or non-government control. In the U.S. there is growing support and adoption of the Federal Emergency Management Administration (FEMA) National Incident Management System (NIMS) model for command and control (FEMA, 2011). This model recognizes sovereignty and provides for joint command and independent control over resources while providing for an ordered and recognizable organizational structure (FEMA, 2011). Much federal funding requires knowledge of and participation in the NIMS model for law enforcement and others. The NIMS model of command and control is suited to the present day multi-stakeholder and participant crisis response environment as depicted in the parallel circle schema described here.

Activity in the two parallel circles is autonomous and, at times, these participants must share information and interact across these boundaries. The traditional formal circle has responsibility and control over human and other resources through formal and socially accepted institutions. The second circle has separate intrinsic authority and purpose based on individual roles, needs, and controls over what can be contributed: information, personnel or other resources. The first circle is more formally organized and the latter can be formal, such as a recognized sectarian group, or more ad-hoc and flexible with few rules or established communications channels to other entities.

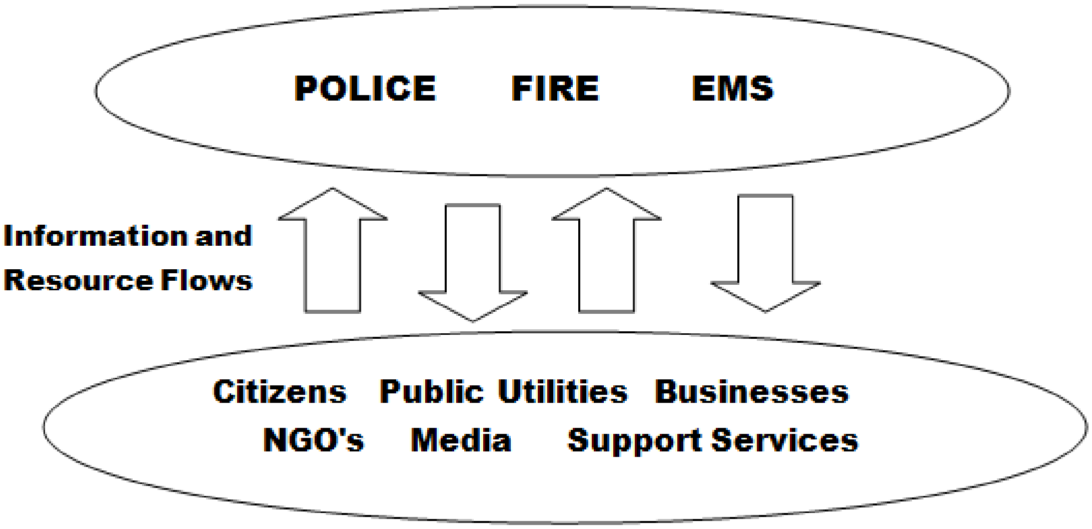


Figure 23: Information and Resource Flows

The two layers operate independently with their own resources and activities. The first layer can dip into the information, contacts and resources of the other layer for knowledge and coordination outside the traditional boundaries. Researchers here propose, as a dramatic shift from the current established relationships and comfort level that greater bi-directional or multi-directional exchange of information and resources will occur than is currently the case. Things of value in the second layer include resources such as camera phone images, twitter information, and cultural knowledge from local groups on interests and needs. This is also where collaboration between agencies and volunteers interact and provide information and inputs to social emergency response policy development, which may be localized and customized to meet the particular social communities and cultures present in particular geographic area.

A mechanism for bridging these two parallel arenas is provided through technology and policy/culture change that must account for the vast overload of information possible and have ability to filter through things like location or identity to identify potentially relevant information from the mix of all available information. Avoiding information overload and its resulting paralysis is as important in an emergency as having information available. There must also be a way to coordinate, manage, retain, and then sift through this captured data and through a process make it available to those who need it (Palen, Anderson, Mark, Sicker, Palmer, & Grunwald, 2010). The technology device, personnel, policy, and social processes described must function in this type of environment to be effective.

Empowering both local authorities and community residents to help each other and save themselves will be proven to be a positive improvement over current practice.

Information sharing in social communities is an example of complex social behavior in that transmitting, withholding, storing, and modifying information is subject to norms and motivated by social obligations (Ryan, 206). There is the opportunity here to further probe into the social organization and dynamics. How do members of immigrant groups on the North side interact with non-immigrant groups around notification? And since the target users include professionals such as law enforcement officers, it would be important to look at the “seams” in this space as well: seams between community members, community leaders, and professionals. How is information shared (or not shared) across such seams? How are information sharing, non-sharing, and social organization related? The objective here is to also examine patterns of social behavior and specify the design accordingly in order to promote trust within and across social groups and within a context of individual discretion. Trust is found to be an important variable for effective communication management in crises (Longstaff & Yang, 2008). Researchers here look to address cross-boundary information sharing issues as identified in Ryan (2006) and Pardo, Gil-Garcia, and Burke (2008). The approach is to take the social aspects of notification as key inputs into system design, which would bring to bear on technical work a rich body of social science research on the diffusion of innovations, theories of social contagion, information disclosure, governance, resilience, and the economics of information, among others (Akerlof, 1970; Quarantelli, 1997; Longstaff et al., 2010).

Four important areas for design work in the system include: first, what would an appropriate configuration of notification roles and responsibilities be in ad hoc, hybrid social support structures? This would be the case when ordinary citizen and professionals must work together at critical event sites. The implications for applications design have been previously identified by the Syracuse University (SU) Partnerships for Innovation (PFI) research undertaken since 2002, namely, that removing complexity from the system for users and facilitating rapid and easy application is crucial; and is facilitated by having open specifications. Second, what would ordinary citizens need to have as a stock of knowledge in order to determine when a gas leak, for example, is potentially disastrous? What features/functionality should be considered in the design in order to facilitate quick access to reliable, actionable, and timely information and knowledge? Third, in a dynamic, ad hoc network with nodes entering and exiting, how should one best support user authentication so as to foster trust? Fourth is the issue of data believability and trust. What additional sources of data, or more frequent sampling by sensors of the environment, could be automatically gathered and provided by the system in ambiguous situations? Can location provide a means for designating priority for communications to the command personnel or responders? Lessons learned from field-testing the system should produce design guidelines and guide development of policies for the distributed cognitive engine/gateway devices envisioned.

5.6 Interpretation Issues

An identified issue that needs to be resolved is how to manage the problem of having access to systems or services but not being able to translate or navigate to the needed data, information or action. Resolving differences in how material and personnel resources are identified and described is a problem separate from gaining physical access or control. Creation and use of ontologies can help improve the understanding of other, possibly unfamiliar, systems. The U.S. Federal Emergency Management Agency (FEMA) is working to address this through its promotion of standardized ontologies of conceptual mappings for resources (Mendonça et al., 2007).

Information overload has been identified as a problem for emergency responders (Turoff, 2002). The capabilities afforded through technologies such as wireless grids will make even more information available in these cases, contributing to that aspect of the problem. Having the ability to filter and create hierarchical or rule-based controls for information access will mitigate the overload and at the same time provide richer and more current information flows to those who need it most.

Soon there are likely to be even more robust communication-based collaborative tools developed that would critically filter out nonessential or duplicate information while placing emphasis on vital information intelligently (Mendonça et al., 2007). In this way, new support systems and a greater amount of information will enhance and not impede the operational processes.

6. Conclusion

That communication and information sharing gaps occur between and across responders and stakeholders in emergency response incidents is well known (Barr, Burther, & Mahy, 2011; Kovacs, & Spens, 2011; Nivolianitou & Synodinou, 2011; Gaynor, Brander, Pearce, & Post, 2008), what to effectively do about it has not been so clear. This article reports on conclusions drawn from empirical sources and the literature towards that goal. Recommendations that speak to gaps noted by observation and the work of others are provided. Factors associated with fostering rapid and effective communications between various responders to emergency situations were investigated. The article presented conclusions by first describing the problem and presenting a review of past and current literature followed by a description of the research methodology used, then a discussion of findings and observations made, and last a summary of the conclusions and recommendations Findings from this research should inform the design of policy and system features and functionality for emergency response at all levels. As for the academic community, the work should be considered as part of a continuing investigation into understanding and improving collective response to crises considering the social, technical and policy factors.

This essay argues that a social emergency response policy must be developed to reflect the reality that the true first responders to most disasters are the victims, neighbors, or passersby with handheld devices or other technology. The traditional hierarchical model for emergency response, assuming helpless victims in need of rescue, breaks down when the citizens may in fact be better informed and coordinated than their supposed rescuers. Social media and crowd sourcing are being explored as a means for emergency coordination. The wisdom of the crowd in a time of panic and rumor may be limited and information distributed across many sources. There remains a need for some level of coordination of data, resources and response.

A new social emergency response policy is needed. This will be best achieved through continued public awareness and debate. Researchers here acknowledge that social aspects of stakeholder coordination and engagement have been neglected at crises. The new recognized emergency response community must include non-government entities and citizens. Technology will provide new supports and opportunities for improving speed and quality of emergency response coordination. It remains true that social, technical and policy approaches must be aligned for effective crisis response.

Smart devices in the hands of on scene users may be insufficient if law enforcement and other personnel cannot tell who is trustworthy, or whether civilians are on the scene by happenstance, or are other first responders such as fire and EMT personnel. Further, public networks in crises often break down from the harsh conditions of for example, an earthquake or hurricane, which caused the emergency, at other times, concerned family and friends from out of the area can overload networks and cause delay in emergency response. In still other cases, the networks are operating fine even in the midst of disaster, but public authorities have essentially seized them claiming most bandwidth for themselves, leaving the public, some of whom may be injured or in need of rescue, unable to communicate.

The results of this research will also lead to new commercial products, services and jobs–in addition to the potential gains in effectively managing emergency and crisis response. Before the market and widespread access to these solutions can fully emerge, however, policymakers and emergency response professional communities face several challenges. Can the emergency response community accept becoming peers on a social network of people, devices, and networks? Without a willingness to work collaboratively with the community to define the specific operating conditions for what some may see as privacy-invading devices, the pace of adoption and diffusion may be slower that is desirable. On the other hand, having strong privacy and security mechanisms built into the core of the technology, such as through wireless grid open specifications, both near the physical (cognitive radio) and virtual (edgeware gridlet) layers, may reassure users and promote trust in these systems (Zargar et al., 2009; Brooks, Caicedo, & Park, 2012). In either case, discussion and debate on social emergency response policy is needed. It is the hope that this work will incite debate and possibly foster change such that there will be new agenda for social emergency response.

Much research still needs to be done on information interoperability especially within the context of emergency response systems.

Emerging technological solutions will allow cooperation and resource sharing to occur in the existing and blended environment. Going forward, systems can grow and even change platforms but will retain their functionality and interoperability by having such intermediary services. Many of the identified barriers to entry and the degree of potential risk that must be taken to implement a new technology are reduced where options may be tried in the present interoperable operating environment. New potential solutions can be implemented with the most successful ones being identified, refined and continued.

Researchers propose to establish by acknowledgement parallel networking communications capabilities, voluntarily, by community residents, emergency responders, and others to serve their own needs. This community grid, once established, can bring significant expansion in the number and variety of devices and networks available to assist in emergency response, is for those residents secondary to their improved ability to look after themselves and each other in the routine emergencies any community can face on a daily basis.

Government officials were involved in the public forums hosted in 2011 by the New York State Office of Homeland Security and Emergency Services. During these “listening sessions” and topic discussions, the notion of stakeholders was identified as including mostly the traditional police, fire, and EMS agencies, some not-for-profit human services providers such as the Red Cross, and utility providers such as the power and water authorities. Engagement with citizen groups, culturally identifiable groups, or other members of the community, private industry– such as a construction company for specialized equipment support or a brewery that could change gears readily to put out and distribute bottled water when necessary– are only now being considered.

The path to this end appears to be to continue to openly discuss the issues, raising awareness, and thereby changing perceptions and expectations. A good example comes from taking a different view of the traditional hierarchical control model. If you view the model as clarifying responsibility and control by having a single responsible party at the top you can see how it may also convey the message that everyone else is then not responsible. The new approach is cooperative and requires a reconceptualization of responsibility and acceptance of shared and dynamic authority and participation by all. All are responsible and all should participate as they can. There is no one magic solution, but a multitude of individual and group solutions occurring simultaneously that interoperates and are adapted as necessary by those able.

The proposed result is human stigmergy in crisis response. Each stakeholder party reacts and contributes individually toward a common goal with the result being a collective social emergency/crisis response led by one and all. The motion and activity of a unified flock of birds reflects this notion of cooperative stigmergy. From a distance the birds appear as one being, moving, changing and reacting to the environment based on basic and shared needs.

The goal of this research is to help people to help themselves in a crisis. This includes formal and informal responders. Emergency services applications, including technology such as wireless grids, can empower citizens through their devices to cooperate and contribute to their own community response. This article asserts that police, fire, EMS, hospitals, municipal services, utilities, gas companies, media, and community residents will benefit from enhanced information sharing in emergencies by embracing a more inclusive understanding and stigmergic approach.

7. Acknowledgements

The development of WiGiT (2010) has been primarily funded by the National Science Foundation (NSF) under (NSF #0227879) 2002-2006 and is continued under (NSF # 0917973) 2009 -2011. Authors are grateful for the continued support by all collaborators and partners. Errors of fact or omission are the author's responsibility. The views expressed are those of the authors and are not necessarily shared by the institutions they are affiliated with.

8. References

Adam, N., Atluri, V., Chun, S., Ellenberger, J., Shafiq, B., Vaidya, J., & Xiong, H. (2008). "Secure information sharing and analysis for effective emergency management. "In Digital Government Society of North America, 407-408. Montreal, Canada.

Akbulut, A., Kelle, P., Pawlowski, S., Schneider, H., & Looney, C. (2009). To share or not to share? Examining the factors influencing local agency electronic information sharing. International Journal of Business Information Systems 4, no. 2: 143 - 172. doi:10.1504/IJBIS.2009.022821.

Akerlof, G. A. (1970). The market for" lemons": Quality uncertainty and the market mechanism. The quarterly journal of economics, 84(3), 488-500.

Barr, J. L., Peddicord, A. M. ., Burtner, E. R., & Mahy, H. A. (2011). Current Domain Challenges in the Emergency Response Community. Proceedings of the 8th International ISCRAM Conference–Lisbon (Vol. 1).

Benbasat, I., Goldstein, D. K., & Mead, M. (1987). “The Case Research Strategy in Studies of Information Systems.” MIS Quarterly 11(3): 369-386. Retrieved November 8, 2009.

Birje, M. N., & Manvi, S. S. (2011). “An Efficient Method of Sharing Device Resource Status in Wireless Grids.” *Multiagent and Grid Systems* 7, no. 4: 127–146.

Birje, M., & Manvi, S. (2010). “Monitoring and Status Representation of Devices in Wireless Grids.” *Advances in Grid and Pervasive Computing*: 341–352.

Botterell, A., & Addams-Moring, R. (2007). “Public warning in the networked age: open standards to the rescue?,” Communications. ACM, 50, no. 3: 59-60.

Brooks, T., Caicedo, C., & Park, J. (2012). Security challenges and countermeasures for trusted virtualized computing environments. *Internet Security (WorldCIS), 2012 World Congress on* (pp. 117–122). IEEE.

Bureau of Justice Statistics (BJS) (2007). BJS Law Enforcement Statistics, August 8, 2007. Retrieved May 9, 2008, from http://www.ojp.usdoj.gov/bjs/lawenf.htm.

BJS. (2011). US Department of Justice, Bureau of Justice Statistics (BJS). *Census of State and Local Law Enforcement Agencies, 2008*. July 26, 2011, NCJ 233982. http://bjs.ojp.usdoj.gov/index.cfm?ty=pbdetail&iid=2216

Caicedo, C. E. (2007). Software Defined Radio and Software Radio Technology: Concepts and Applications. *In proceeding of: International Telecommunications Research and Education Association ITERA*. 01/2007.

Chen, Q. (2009). Cognitive gateway design to promote interoperability, coverage, and throughput in heterogeneous communications systems. PhD dissertation, Department of Electrical and Computer Engineering, Virginia Tech, Blacksburg, Virginia.

Datla, D., Chen, X., Tsou, T., Raghunandan, S., Hasan, H. and Reed, J.H. (2011). “Wireless distributed computing network: a survey of research challenges”, IEEE Communication Magazine, accepted for publication, April 2011.

Deverell, E., & Olsson, E. (2010). “Organizational culture effects on strategy and adaptability in crisis management.” Risk Management 12(2): 116-134. Retrieved August 15, 2011.

Dinesh, D., Volos, H.I., Hasan, S.M., Reed, J.H. and Bose, T. (2011). “Wireless distributed computing in cognitive radio networks.” Ad Hoc Networks in Press, Uncorrected Proof. Retrieved May 4.

Dutton W. H, Gillett S. E, McKnight L. W & Peltu M. (2004). "Bridging broadband internet divides: reconfiguring access to enhance communicative power." Journal of Information Technology.

FEMA. (2011). “FEMA: Emergency Managers and Personnel.” Retrieved June 16, 2011 (http://www.fema.gov/emergency/).

Fitzek, F. H., & Katz, M. D. (2007). Cognitive wireless networks: Concepts, methodologies and visions inspiring the age of enlightenment of wireless communications. Springer.

Foster, I., & Kesselman, C. (2004). The Grid 2: Blueprint for a new computing infrastructure. Morgan Kaufmann, San Francisco, California.

Gaynor, M., Brander, S., Pearce, A., & Post, K. (2008). Open Infrastructure for a Nationwide Emergency Services Network. International Journal of Information Systems for Crisis Response and Management (Vol. 1, pp. 31–46).

Gil-Garcia, J., Guler, A., Pardo, T., & Burke, G. (2010). Trust in government cross-boundary information sharing initiatives: Identifying the determinants. In Hawaii International Conference on System Sciences, 0:1-10. Los Alamitos, CA, USA: IEEE Computer Society.

Glomseth, R., Gottschalk, P., & Solli-Saether, H. (2007). Occupational culture as determinant of knowledge sharing and performance in police investigations. International Journal of the Sociology of Law 35, no. 2 (June): 96-107.

Harrison, T., Gil-Garcia, J.R., Pardo, T.A., & Fiona, T. (2006). "Learning about interoperability for emergency response: Geographic information technologies and the World Trade Center crisis," The Thirty-Ninth Annual Hawaii International Conference on System Sciences, Computer Society Press, Hawaii.

He, A., Amanna, A., Tsou,T., Chen, X., Datla, D., Newman, T., Reed, J., & Bose, T. (2011). “Green Communications: A New Paradigm for Creating Cost Effective Wireless Systems,” Journal of Communications, accepted for publication, March.

Hughey, E.P., & Bell, H.M. (2011). Does comprehensive emergency management work? Risk, Hazards, and Crisis in Public Policy, 2 (1), 1-33.

IDABC. (2008). Interoperable Delivery of European eGovernment services to public Administrations, Businesses and Citizens. European Interoperability Framework, V2.0 (draft). URL: http://ec.europa.eu/idabc/servlets/Doc?id=31597

Jing, F., & Pengzhu, Z. (2007). “A case study of G2G information sharing in the Chinese context,” in (Philadelphia, Pennsylvania: Digital Government Society of North America), 234-235.

Kaarst-Brown, M. L. (1999). Five symbolic roles of the external consultant–integrating change, power and symbolism. *Journal of Organizational Change Management*, 12(6), 540–561.

Kaarst-Brown, M. L., & Robey, D. (1999). More on myth, magic and metaphor: Cultural insights into the management of information technology in organizations. *Information Technology & People*, 12(2), 192–218.

Kean, T. H., & Hamilton, L. (2004). *Nine/eleven Commission report, final report of the National Commission on Terrorist Attacks Upon the United States*. WW Norton & Company.

Kovács, G., & Spens, K. M. (2011). Trends and developments in humanitarian logistics–a gap analysis. *International Journal of Physical Distribution & Logistics Management*, 41(1), 32–45.

Kuehn, A., Spichiger, A., & Riedl, R. (2009). *Interoperabilität und Standards im E-Government, in: E. Schweighofer (ed.) Tagungsband des 12. Int. Rechtsinformatik Symposions*. OCG Books, Vienna.

Leavitt, M. O., Spelling, M., & Gonzales, A. R. (2007*). Report to the President on issues raised by the Virginia Tech tragedy* (No. NCJ 218878) (p. 26). Rockville, MD 20849: National Institute of Justice/NCJRS. Retrieved from http://www.hhs.gov/vtreport.pdf

Lee, J., & Rao, H. (2007). "Exploring the causes and effects of inter-agency information sharing systems adoption in the anti/counter-terrorism and disaster management domains," in Philadelphia, Pennsylvania: *Digital Government Research Center*, pp. 155-163.

Li, G., Sun, H., Gao, H., Yu, H., & Cai, Y. (2009). "A Survey on Wireless Grids and Clouds." In *Grid and Cooperative Computing, 2009. GCC'09. Eighth International Conference On*, 261–267. IEEE.

Li, H., Gong, S., Lai, L., Han, Z., Qiu, R. Q., &Yang, D. (2012). "Efficient and Secure Wireless Communications for Advanced Metering Infrastructure in Smart Grids." *Smart Grid, IEEE Transactions On* 3, no. 3: 1540–1551.

Longstaff, P. H. (2003). Can unpredictable systems be managed? Systems, Man and Cybernetics, 2003. *IEEE International Conference on* (Vol. 2, pp. 2013–2020). IEEE.

Longstaff, P. H., & Yang, S.U. (2008). "Communication management and trust: their role in building resilience to 'surprises' such as natural disasters, pandemic flu, and terrorism." *Ecology and Society* 13(1): 3.

Longstaff, P. H. (2009). Managing surprises in complex systems: multidisciplinary perspectives on resilience. *Ecology and Society*, 14(1), 49.

Longstaff, P., Mergel, I., & Armstrong, N. (2009). Workshop report: resilience in post-conflict reconstruction and natural disasters. *Workshop Report: Resilience in Post-Conflict Reconstruction and Natural Disasters* (March 9, 2009).

Longstaff, P. H., Armstrong, N. J., Perrin, K., Parker, W. M., & Hidek, M. A. (2010). Building resilient communities: A preliminary framework for assessment. *Homeland security affairs*, 6(3), 1–23.

Manvi, S. S., & Birje, M. N. (2009). "Wireless Grid Computing: A Survey." *IETE Journal of Education* 50, no. 3: 119.

Marincioni, F. (2007). “Information technologies and the sharing of disaster knowledge: the critical role of professional culture.” *Disasters* 31(4): 459-476.

McKnight, L. W. (2007). "The future of the internet is not the internet: open communications policy and the future wireless grid(s).” Washington, D.C.: NSF/OECD. http://www.oecd.org/dataoecd/18/42/38057172.pdf.

McKnight, L. W., Anius, D. (2002).Virtual Markets in Wireless Grids: Peering Policy Obstacles,30th Annual TPRC, Alexandria, VA, and Sept. 28-30, 2002

McKnight, L. W., Howison, J., & Bradner, S. (2004). "Wireless grids-distributed resource sharing by mobile, nomadic, and fixed devices,” IEEE Internet Computing, 8(4), 24-31.

McKnight, L., Howison, J., & Bradner, S. (2004). Wireless Grids. Distributed Resource Sharing by Mobile, Nomadic, and Fixed Devices, in IEEE Internet Computing, July/August, and pp. 25-31.

McKnight, L., Lehr, W., & Howison, J. (2007). “Coordinating User and Device Behavior in Wireless Grids.” in F.H.P. Fitzek and M.D. Katz. Eds. Cognitive Wireless Networks: Methodologies and Visions, Springer., Pp. 679-697

McKnight, L., Lehr, W., & Howison, J. (2007). "Coordinating user and device behaviour in wireless grids." In Fitzek, F. H., & Katz, M. D.: Cognitive Wireless Networks:Concepts, Methodologies and Visions Inspiring the Age of Enlightenment of Wireless Communications. Springer.

McKnight, L., Sharif, R., & Wijngaert, V. D. (2005). Wireless grids: assessing a new technology from a user perspective, Designing Ubiquitous Information Environments: Socio-Technical Issues and Challenges. http://dx.doi.org/10.1007/0-387-28918-6_14.

McKnight, L.W., & Howison, J. (2003). "Toward a sharing protocol for wireless grids." Int’l Conference on Computer, Communication & Control Technologies (CCCT '03), Orlando, Fl, July 31-August 2, 2003.

McKnight, L.W., Treglia, J., Kuehn, A. (2010).‘Wireless Grids or Personal Infrastructure: Policy Implications of an Emergent Open Standard,’ TPRC 38th Research Conference on Communication, Information and Internet Policy.

Mendonça, D., Jefferson, T., & Harrald, J. (2007). “Collaborative adhocracies and mix-and-match technologies in emergency management,” Commun. ACM 50, no. 3: 44-49.

National Research Council. (2007). “Successful Response Starts with a Map: Improving Geospatial Support for Disaster Management”, National Academies Press, page 2.

NCR Project Team. (2009). 2009 Presidential Inauguration Regional After-Action Report (AAR) Summary (After-Action Report) (p. 44). Washington, D.C.: Department of Homeland Security, National Captial Region.

Newman, T.R., Hasan, S.M.S., Depoy, D., Bose, T., & Reed, J.H. (2010)."Designing and deploying a building-wide cognitive radio network testbed," Communications Magazine, IEEE, vol.48, no.9, pp.106-112, Sept.

Nivolianitou, Z., & Synodinou, B. (2011). Towards emergency management of natural disasters and critical accidents: The Greek experience. Journal of Environmental Management, 92(10), 2657–2665. doi:10.1016/j.jenvman.2011.06.003

NYS DHSES. (2011). Statewide Communications Interoperability Plan - State of New York. Albany, NY: New York State Department of Homeland Security and Emergency Services. Retrieved from www.dhses.ny.gov/oiec/documents/NewYorkSCIP2010.pdf

Palen, P., Anderson, K., Mark, G., Martin, J., Sicker, D., Palmer, M., & Grunwald, D. (2010). "A vision for technology-mediated support for public participation & assistance in mass emergencies & disasters." P. 8 in Proceedings of the 2010 ACM-BCS Visions of Computer Science Conference. British Computer Society.

Pardo, T., Cresswell, A., Thompson, F., & Zhang, J. (2006). "Knowledge sharing in cross-boundary information system development in the public sector," Information Technology and Management , 7, no. 4 (December 5): 293-313.

Pardo, T., Gil-Garcia, J., & Burke, G. (2008). Governance structures in cross-boundary information sharing: Lessons from state and local criminal justice initiatives. In Proceedings of the Proceedings of the 41st Annual Hawaii Int'l Conference on System Sciences, 211. IEEE Computer Society.

Pardo, T.A., Gil-Garcia, J.R., & Burke, G.B. (2008). "Sustainable Cross-Boundary Information Sharing." Pp. 421-438 in Digital Government, vol. 17, Integrated Series In Information Systems. Springer US.

Pittman, E. (2011). "Government, Industry Converge to Discuss Information Sharing Issues." Emergency Management. Retrieved January 11, 2011 (http://www.emergencymgmt.com/safety/Government-Industry-Converge-to-Discuss-Information-Sharing-Issues.html).

Quarantelli, E.L. (1997). Ten criteria for evaluating the management of community disasters. Disasters 21 (1), 39-56. NYS DHSES. (2011). Statewide Communications Interoperability Plan - State of New York (Brochure) (p. 143). Albany, NY: New York State Department of Homeland Security and Emergency Services. Retrieved from www.dhses.ny.gov/oiec/documents/NewYorkSCIP2010.pdf

Ryan, D. (2006). "Getting the Word Out: Notes on the Social Organization of Notification*," Sociological Theory, vol. 24, pp. 228-254.

SAFECOM. (2011). Multi-band radio project of the Department of Homeland Security. Http://www.safecomprogram.gov/SAFECOM/currentprojects/mbr/

Schutt, R. (2006). Investigating the social world : the process and practice of research. 5th ed. Thousand Oaks Calif.; London: Pine Forge Press; SAGE Publications.

Thompson, E. D., & Kaarst-Brown, M. L. (2005). Sensitive information: A review and research agenda. *Journal of the American Society for Information Science and Technology*, 56(3), 245–257.

Treglia, J. V., McKnight, L.W., Kuehn, A., Ramnarine-Reiks, A.U., Venkatesh, M. and Bose, T. (2011). "Interoperability by 'Edgeware': Wireless Grids for Emergency Response," pp. 1-10 in Proceedings of the 2011 44th Hawaii International Conference on System Sciences. IEEE

Computer Society.

Treglia, J., Ramnarine-Rieks, A. and McKnight, L. (2010). "Collaboration in a wireless grid innovation testbed by virtual consortium," in Networks for Grid Applications: Third International ICST Conference, Gridnets 2009, Athens, Greece, September 8-9, 2009, Revised Selected Papers (Springer), 139.

Treglia, J.V. (2010). "A Classification of Agents and Entities Influencing Law Enforcement Agencies in the United States." in Proceedings of the iConference on iMPACTS, poster. Urbana-Champaign, NC: Ideals.

Turoff, M. (2002). "Past and future emergency response information systems," Communications of the ACM , 45, no. 4: 32.

United States. Executive Office of the President, & United States. Assistant to the President for Homeland Security and Counterterrorism. (2006). *The federal response to Hurricane Katrina : lessons learned.* Washington, D.C.: White House.

USFA. (2011). February 11, 2011. USFA search the national fire department census database. U.S. Fire Administration; National Fire Department Census Database. Government Information, Retrieved February 13, 2011, from http://www.usfa.dhs.gov/applications/census/

Veil, S.R., Buehner, T., & Palenchar, M.J. (2011). "A Work-In-Process Literature Review: Incorporating Social Media in Risk and Crisis Communication." Journal of Contingencies and Crisis Management 19(2): 110-122. Retrieved August 11, 2011.

Volos, H.I., & Bruehrer. (2010). "Cognitive Engine Design for Link Adaptation: An Application to Multi-Antenna Systems", IEEE Transactions on Wireless Communications, vol. 9, no. 9, pp. 2902-2913, 2010.

Wasserman, R. (2010). Guidance for Building Communities of Trust. Washington, DC: U.S. Dept. of Justice.

Williams, C., Dias, M., Fedorowicz, J., Jacobson, D., Vilvovsky, S., Sawyer, S & Tyworth, M. (2009). The formation of inter-organizational information sharing networks in public safety: Cartographic insights on rational choice and institutional explanations. Information Polity 14, no. 1 (January 1): 13-29. doi:10.3233/IP-2009-0170.

Zargar, S. T., Weiss, M. B. H., Caicedo, C. E., & Joshi, J. B. D. (2009, December*). Security in Dynamic Spectrum Access Systems: A Survey,* Working Paper. Retrieved October 9, 2012, from http://d-scholarship.pitt.edu/2823/

ESSAY 3: Identifying Factors that Support Collaboration in a Multi-jurisdiction Environment: A Case Study of the Central New York Interoperable Communications Consortium

1. Introduction

If you ask the janitor at Nlets (National Law Enforcement Telecommunications System) what his job is, he will proudly tell you "saving lives." As part of a larger case study of the organization, researchers interviewed staff at all levels of Nlets and found that they had an embedded culture and sense of higher purpose throughout the entire organization (PSN, 2011). Nlets is a state-owned, not-for-profit organization providing the backbone infrastructure and networking services that interconnect law enforcement agencies across the nation and with many other countries, through such services as interfacing with INTERPOL. Although these staff members are geographically about as far away as you can get from the sites of emergencies, they express a direct connection with the cop on the street facing a dangerous felon and the fireman who scours in the midst of a crumbling structure for signs of life.

The case study of the Central New York Interoperable Communications Consortium (CNYICC) gives a similar and more detailed picture of this process as it relates to county-level inter-agency cooperation and collaborations in public safety that have been successful in multi-jurisdictional environments with competing interests.

This research seeks to identify factors that have an impact upon public safety information sharing collaborations and technology adoption practices in the law enforcement and emergency response communities. The study will contribute to theory on information sharing and collaboration processes in public sector settings, and will make additional contributions by providing practitioners with policy and practice guidance for developing more effective sharing relationships in collaborative information system initiatives to improve operations. It is hoped that these contributions will result in improved law enforcement and emergency response capability to prevent and respond to crime, terrorist activity, and other disasters while providing a foundation for further academic research on information sharing across public and private agencies. Results from this investigation will be relevant to, and assist in informing, the development and implementation of similar emergency response, or public safety, collaborations in the future.

Of any state, New York has the most local police department full time employees (72,380), in their 391 local police department agencies (BJS, 2011, p.16). New York State also has 1,857 fire departments and fire brigades, 1,122 ambulance services, and 785 non-transporting first-response services (NYS DHSES, 2011, p.6). This is a technology - and policy - intensive environment and includes a multitude of cultures and competing interests.

Counties play an important role in the public safety process due to their very position and structure in New York State and in the United States. Research conducted in this area is significant to public safety literature and professional practice locally, nationally and internationally.

Public safety agencies today must collaborate in an unprecedented way to respond to fiscal and technological challenges in providing critical law enforcement and lifesaving services. Improved transportation and the broad reach of the internet have expanded the scope of incidents and investigations. The public no longer accepts legacy arguments regarding incompatible systems and the lack of sharing of vital information and resources; they demand a move forward. Across the country, multijurisdictional collaborations are forming in order to address these needs. Rather than fumbling through trial and error, they should make use of knowledge from others who have gone this way before and gained insights that can help improve the process and outcomes. The mandate was stated most simply by a northeastern 911 administrator, “the obligation to me stays the same . . . I have to deliver status quo, lifesaving results every day without an excuse” (Anonymous, 2011).

A disturbing statistic, the phrase "29/121" refers to the 121 firefighters who lost their lives in the North Tower of the World Trade Center on September 11, 2001 due to a lack of interoperable communications (Peha, 2005). In the 29 minutes after the first evacuation order went out, these firemen who had incompatible communications equipment never received the warning and, thus, did not get out in time (Peha, 2005). This is but one example of communications technology failing to meet the most basic needs of public safety organizations on the scene. These failures are not the results of simple operator error or a design flaw but are rooted in the communications infrastructure and policy for public safety communications in the United States.

To address these problems, innovation in both technology and policy are necessary. The willingness of various public safety agencies and jurisdictions to partner in compatible solutions is more important than the technology to be used (Treglia, 2009; NYS DHSES, 2011).

The purpose of this research is to contribute to scientific and professional knowledge regarding cooperative information sharing across law enforcement agencies and the emergency response community. The basis for this case study is derived from a set of seemingly unsophisticated yet fundamental questions: What are the factors that support collaboration among public safety agencies in information sharing projects involving information technologies? What factors work against successful collaboration among law enforcement, emergency response agencies, and other stakeholders? Answers to these questions are pursued here through case study, policy analysis, interviews, and the use of existing survey data compiled by the Public Safety Networks Study and Police Executive Research Forum.

In this study, researchers focused on a multi-jurisdictional public safety consortium formed and operating in upstate New York – the CNYICC. In the area of public safety, officials in New York State who spearhead communications planning for local systems are primarily from county government and most typically department heads of Emergency Services (NYS DHSES, 2011). Investigation of the CNYICC is significant to public safety study as the core members are heads of county emergency communications departments. Qualitative data from the case study was analyzed using content analysis techniques to identify key issues and factors, as identified by the respondents, which may be relevant to other such formations. Findings addressing the research questions identified previously are reported on.

Law enforcement and emergency response agencies, or public safety agencies, are tasked with responding to crises under any conditions or circumstances. They cannot wait for the eventual change that may take decades to occur as an older generation is replaced by a newer one.

Communications/911 centers comprise a key participant and resource in the intelligence information "gathering and sharing" mission of public safety entities. To be effective, a communications/911 center should be able to connect and share with first responders, intelligence collection, analysis, and dissemination resources, whether they be local law enforcement intelligence units or fusion centers. By leveraging emerging standards in intelligence information sharing, communications centers can assist in the collection and sharing of information with other intelligence centers. This, in turn, allows the communications centers to receive critical intelligence information for dissemination to the field. Cooperation with these other agencies is the critical element that allows this to occur. Understanding how to facilitate such cooperation and sharing in this environment can greatly improve the delivery of public safety services.

This paper is organized as follows: The first section contains a review of prior research on public safety and professional collaboration issues and outcomes. Methodology for the case study and analysis are described next followed by a description of the CNYICC and important macro and micro environmental issues impacting it. This is followed by presentation of key initial findings from the case study, as well as an analysis of significant factors influencing the development and operation of this type of public safety collaboration. This follows a structure similar to that of another case study of a collaborative first responder network, CapWIN (Fedorowicz, Gogan, & Williams, 2007). The study concludes with a discussion of the implications of these findings for practitioners and researchers, and proposes possible directions for further research.

2. Background

This essay reports on the CNYICC. The associated development of interoperable emergency communications in the area through this collaboration was the subject of the case study here. This research has investigated the issue of what elements go into successful collaboration among disparate county government emergency response management agencies. Researchers here consider the social, technical, and policy factors. The motivation for cooperation here consists of multiple dimensions: to better serve the public, to prepare for funding opportunities, to share information, to collectively speak to standards issues, and to collectively pool resources to achieve greater influence over vendors for equipment and services contracts.

The case study of the CNYICC provides an example of an alternative governance solution for public safety collaboration. The CNYICC was created outside, in parallel with, standard formal government structures to address the common interests and needs of multiple counties in providing for emergency communications. The consortium coordinates regional and local communications policy and activities of participating dispatch centers, public safety agencies, and other stakeholders acting through their individual agencies. CNYICC interacts with both the government and private sectors relative to emergency communications and response issues. Formed by written memorandum of understanding (MOU) and espousing a shared interest in improving interoperable communications collectively across the multi-county region, the consortium continues to operate as a loosely controlled cooperative having few formalized policies.

A figure showing the makeup and structure of the CNYICC is provided below. The

Figure **24** shows the CNYICC Core Membership in the center of a concentric circle. Core Membership consists of the directors of the five participating counties and a member representative from the state police. Core members actually vote and direct CNYICC action. It should be noted that the state has not formally signed on to the Memorandum of Understanding as did the counties. The next layer depicted shows the CNYICC Extended Membership, which consists of non-core members from government, profit and not for profit agencies having an interest in the activities of the CNYICC. Types of entities in the extended membership area are listed in the figure; the numbers showing in parentheses at the right of the described types are an approximate number of those observed participating in meetings during the study. At the extended member level the parties have a stake in the work of the consortium. The chairman of the CNYICC said that the public or any interested group or individual may participate in the extended meetings. There is in principal a last layer where the public may participate; however, the researcher did not observe any civilians or members of the public in this category during the course of the study.

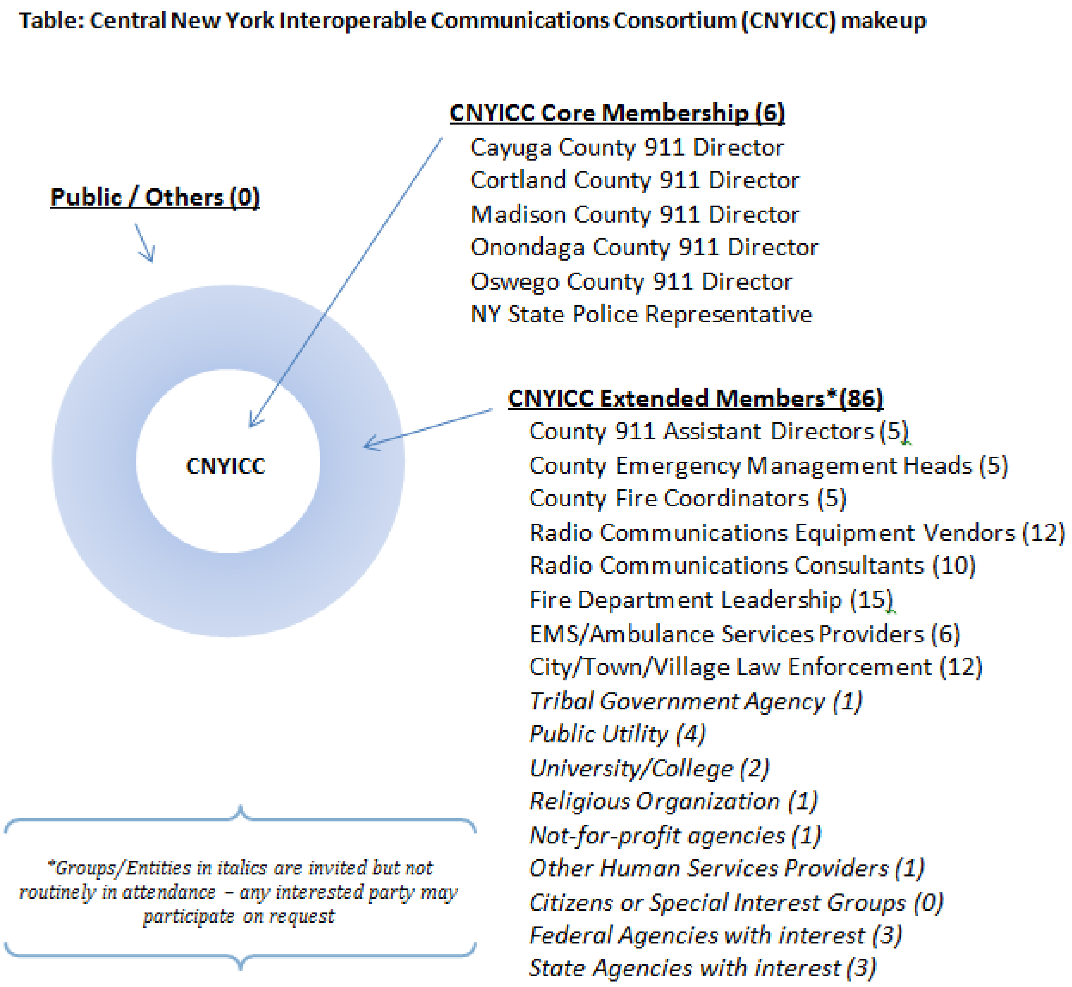


Table: Central New York Interoperable Communications Consortium (CNYICC) makeup
CNYICC Core Membership (6)
Cayuga County 911 Director
Cortland County 911 Director
Madison County 911 Director
Onondaga County 911 Director
Oswego County 911 Director
NY State Police Representative
Public / Others (0)
CNYICC
CNYICC Extended Members*(86)
County 911 Assistant Directors (5)
County Emergency Management Heads (5)
County Fire Coordinators (5)
Radio Communications Equipment Vendors (12)
Radio Communications Consultants (10)
Fire Department Leadership (15)
EMS/Ambulance Services Providers (6)
City/Town/Village Law Enforcement (12)
Tribal Government Agency (1)
Public Utility (4)
University/College (2)
Religious Organization (1)
Not-for-profit agencies (1)
Other Human Services Providers (1)
Citizens or Special Interest Groups (0)
Federal Agencies with interest (3)
State Agencies with interest (3)
*Groups/Entities in italics are invited but not routinely in attendance – any interested party may participate on request

Figure 24: Composition of the CNYICC

3. Literature

Other agencies have come together in response to a crisis, for a targeted funding opportunity or due to formal mandate. Critical incidents can also serve as galvanizing forces that bring about public sector initiatives based on political feedback or pressure. These statements are supported by current research regarding the formation and governance of public safety networks (Kingdon, 1997; Sawyer, Fedorowicz, Tyworth, Markus, & Williams, 2007; Williams, Dias, Fedorowicz, Jacobson, Vilvovsky, Sawyer, & Tyworth, 2009; Sawyer & Fedorowicz, 2012).

According to Weiss (1987), who examined the forces that push public agencies to overcome barriers to cooperation, the question of whether agencies work together may be influenced by economic and financial imperatives, norm satisfaction, reduction of uncertainty, political advantage, and legal mandates. The disparity in classifying information by federal and local agencies is a barrier to effective collaboration (Thompson & Kaarst-Brown, 2005).

Formation of Public Safety Networks (PSNs) as information sharing networks was studied in depth by the Public Safety Networks Study (http://publicsafetynetworksstudy.org), which is a multi-university research collaboration (Sawyer & Fedorowicz, 2012; Sawyer, Schrier, Fedorowicz, Dias, Williams, & Tyworth, 2012). That study focused on Public Safety Networks (PSNs) created for use at the state and local levels in the United States and involved a mix of law enforcement and other emergency response and support agencies. Using factors derived from both rational choice and institutional theories, the authors describe the size and maturity of state-level PSNs and propose a set of factors that may predict public safety collaboration (Williams, Fedorowicz, & Tomasino, 2010). This dissertation argues that in at least one North American case study public safety officials formed a consortium for interoperable communications based not on those reasons but for higher-order interests such as the public good (Treglia, 2012).

A finding from the Public Safety Networks Study project regarding PSN development included that institutional factors provided the most significant coefficient indicating a state's culture of endorsing technological advances, collaboration, transparent sharing of data, or other administrative reforms (Williams, Fedorowicz, & Tomasino, 2010). An organizational culture fearful of information technology may avoid innovation that could facilitate communication (Kaarst-Brown & Robey, 1999). A different culture may seek out new processes.

Agranoff and McGuire (2001) show how a change in state-administered federal programs, increasing regulation at the state and federal levels, reductions in financial assistance programs, and increasing regulations require agencies to form unconventional partnerships in order to share resources. This was not entirely the case here.

To date, no single ''true'' definition of "collaboration" has been widely adopted in the realm of emergency response and public safety. The case study focuses on the collective action of the organizations' players, which involves their disparate and interdependent responses to internal and external environmental influences, rules, and options (Astley & Van de Ven, 1983). Researchers provide insights based on a limited view of public safety collaborations in general, so research here is but one contribution to that larger effort. Thomson anticipates that theory on collaboration will evolve over time through empirical work, including ''models for particular niches'' that collectively support a greater understanding of collaboration and which account for the dynamism and complexity in this environment (Thomson, Perry & Miller, 2009; Ostrom, 1990).

Wood and Gray (1991) proposed, as a preliminary research agenda for collaboration, the investigation of four key issues: 1) the meaning of collaboration; 2) how collaborations are convened; 3) the relationship between collaboration and environmental uncertainty and control; and 4) the relationship between the individual and collective interests of collaborating partners (Wood & Gray, 1991). In this essay, researchers address these issues in the context of CNYICC and thereby contribute to the greater effort of describing and understanding problems and solutions within this niche area of public safety and emergency response.

Collaboration, as conceptualized in this essay, involves a joint organizational entity (i.e., the CNYICC) and its infrastructure, processes, technological resources, and relationships. Various autonomous actors come together for a common purpose, be it a program, service, or product, over time and in infrequent emergency event situations (Agranoff & McGuire, 2001; Moynihan, 2005; Milward & Provan, 2006). Fedorowicz, Gogan, & Williams (2006) write that, “for every successful initiative, there have, unfortunately, been many failed attempts, thanks to a variety of complex political, administrative, and technical challenges.” A similar model is proposed for considering these issues in the law enforcement and emergency response field involving technical, social and policy considerations (Treglia & Park, 2009).

The challenge of finding a means by which to assess effectiveness of these collaborations (networks) is considered by Provan, Milward, and Brinton (2001). Emergency response activity does not always lend itself to traditional hierarchical organization and is therefore difficult to measure. New age management activity is represented by Lipnack and Stamps’ (1994) five "teamnet" principles: 1) Purpose (unifying purpose) – shared commitment to goals is the binding force, not legalisms; 2) Members (independent members) – sovereignty is retained during cooperation; 3) Links (voluntary linkages) – actors participate by choice with crisscrossing relationships and communicate extensively on an ad-hoc basis; 4) Leaders (multiple leaders) – more than one person can assume leadership role; 5) Levels (integrated levels) – people work at different levels within and across the organization, up and down (Lipnack & Stamps, 1994). Here, these principles can be seen as characteristics of management within a federated system, particularly the emergent jurisdiction-based and network models. Today's public safety emergency response agencies would fit with such a model.

Collaborations formed may be governed informally (Bardach, 2001) or in a more explicitly or formally structured way (Milward and Provan, 2006). Interorganizational systems (IOS) provide connecting infrastructure in support of information exchange and communication (Cash & Konsynski, 1985). Research such as this has identified a need for explicit structures for multi-agency collaborations. Social capital and having governance structures especially suited to the context or environment can promote trust and by extension improve collaboration (Ostrom, 2009; Walker & Ostrom, 2007). The case studied here does not align exactly with a more structured organizational model. Experience here reveals a more complex dynamic regarding the need for and types of formalization regarding governance and activity.

Collaboration has been described as a process where "autonomous or semi-autonomous actors interact through formal and informal negotiation, jointly creating rules and structures governing their relationships and ways to act or decide on the issues that brought them together; it is a process involving shared norms and mutually beneficial interactions (Thomson, Perry, & Miller, 2011).

Collaboration success can be difficult to quantify. Several approaches have been taken to measure and describe collaboration outcomes (Westphal, Thoben, & Seifert, 2008). Kothari, MacLean, Edwards and Hobbs (2011) note that traditional mechanisms and indicators for measuring cooperation are not well established. Thomson, Perry and Miller developed a multidimensional assessment model of collaboration using data from a survey of national service program participants (2009). From that study five key dimensions are described that form an overall construct of collaboration. Collaborating with partners is an essential competency for public safety entities. Kuenzel and Welscher report that there are eight factors important to 'Public Safety Collaboration Success' (2009). The eight success factors are explained below and serve as an essential frame-work for analyzing and assessing collaboration processes:

1. Relevance and Sense of Urgency: The need to collaborate can emerge from political strategy; improvement in services; civil society and media exerting pressure on the public sector to change the policies.
2. Incentives and Benefits: The reciprocal benefit from partnership can arise from the interest of each member.
3. People & Roles: The success in collaboration depends directly on establishing a social system wherein the individuals must have interpersonal relationship and a mindset for collaboration.
4. Organizational Structure: It is because of the organizational structure that collaboration from the individuals, having political and social relationships, is mostly sought.
5. Reflection & Learning: It is due to the changing environment which makes the ongoing learning process occur. Collaboration thus demands that all the partners must have a great deal of reflection and knowledge.
6. Skills and Capabilities: A variety of skills are needed for the collaboration to be feasible. These skills pertain to management, strategic aptitude, negotiating and communicating capabilities.

7. Resources: The more the resources the more the collaboration. The scope and duration of collaboration determines the amount of resources required.
8. Outside Support & Supervision: when collaboration has admittance to external support it can easily achieve its targeted goals.

The authors suggest that the eight identified success factors (above) must be made part of the design and operation of a collaboration to have the highest probability of achieving its desired public safety objectives (Kuenzel & Welscher, 2009). This model may be used to describe the success of public safety collaborations. Following the presentation of the study findings the information sharing model and factors from this model are used as a tool to assess the success of the CNYICC discuss other relevant issues from the case study.

Findings from the Public Safety Networks Study project include prescriptive recommendations for government policy makers, and participating agencies as they work towards collaborative information sharing. The five implementation recommendations from Sawyer and Fedorowicz (2012) include:

1. Involve all stakeholders in the design of a collaborative work
2. Create networks that stakeholders will value, participate in, and use .
3. Pursue every opportunity to fund a collaborative network
4. Develop a diverse set of performance goals
5. Leverage technology to advance a collaborative network

Formalization is conceptualized as the extent to which tasks or obligations are structured within an organization or entity, and the degree to which these activities are governed by identifiable rules and procedures. Other, early, definitions of the concept of formalization include "… statements of procedures, rules, roles, and operation of procedures which deal with (a) decision seeking (applications for capital, employment, and so on), (b) conveying of decisions and instructions (plans, minutes, requisitions and so on), and (c) conveying of information, including feedback" (Hall, Johnson, & Haas, 1967; Pugh, Hickson, Hinings, Macdonald, Turner, & Lupton, 1963). The measurement of formalization in organizations is operationalized as "… the proportion of codified jobs and the range of variation that is tolerated within the rules defining the jobs, the higher the proportion of codified jobs and the less the range of variation allowed, the more formalized the organization" (Aiken & Hage, 1966, p. 499; Hage, 1965, p. 295).

Sales (2010) suggest that formalization of policy has positive effects on the organization and can improve information sharing. Others see formal systems as potentially less effective in facilitating information sharing than informal ones (Hall & Tolbert, 2004; Kim & Lee, 2006; Willem & Buelens, 2007). It may be that having informal policy leads to increased openness and greater interaction and communication in an organization (Jarvenpaa & Staples, 2000; Kim & Lee, 2006). The case of the CNYICC demonstrates operation of a collaboration having less formal structures in its development stages. For longer term mature operation of collaborations the need for greater formalization may arise.

Reflecting on the formation and purposes of professional associations may help create a better understanding of the CNYICC development and activities as collaboration. Montgomery (1987) argues that professional associations are movements of workers coming together purposely to protect their collective interests. In describing the proper motivation and sentiment of the members of these organizations, Montgomery notes that members were "fully prepared, if need be, to sacrifice personal interests to the common good" (Montgomery, 1987). Interestingly, this sentiment was reflected by all of the members in CNYICC.

Professional associations in the United States gained recognition as early as the 18th century. They were founded due to the ineffectiveness of other structures to sufficiently address their concerns and interests. Associations, or societies, brought together members of the same profession with common interests. Groups from trade, legal bodies, social scientists, and medical professionals found it worth forming associations based on their professional interests (Douglas, 1987; Powell & Steinberg, 2006), and they sought a common voice to protect and serve these interests. Some believed that government structures alone were inadequate to accommodate public interests due to high costs or the complexity of varied public demands (Douglas, 1987). These associations in the public sector provide outlets for solidarity and pluralism in society (DuFour & Eaker, 1998). The success of these associations stems from their ability to bargain and advocate collectively with a common language, to respond to the specialized needs of their members, and to identify significant political and social concerns (DuFour & Eaker, 1998).

Professional associations are recognized as playing a significant role as regulatory mechanisms (DiMaggio & Powell, 1983; Ruef & Scott, 1998). In an article following their case study, Greenwod, Suddaby and Hinings (2002) suggest that associations can exert great influence especially in times of deinstitutionalization and change. The role of associations in that phase is to host the discourse and endorse the change within the profession and as it is portrayed externally (Greenwood, Suddaby, & Hinings, 2002).

Work by Greenwood, Suddaby, and Hinings (2002) suggests that professional associations are important for three reasons. First, associations provide arenas where organizations interact and collectively represent their interests and needs to each other; these are important venues for candid interaction to occur (Greenwood et al., 2002). Crucial in the associations is the construction and maintenance of consensus over boundaries, priorities, membership, and behavior. Associations are not entirely homogeneous communities, and there remain differences among participants (Powell & DiMaggio, 1991). Decision-making in associations has been characterized as a political process (Dezalay & Garth, 1996), which is to say that it is not a static environment. Secondly, identity and norms develop not just from interaction within a community but from outside interactions and social construction as well (Abbott, 1988; Cant & Sharma, 1995). Third, associations monitor compliance with normatively or coercively sanctioned expectations or rules (Greenwood et al., 2002). Associations therefore are active in these processes as they "define or enforce" collective values, acting as guardians and stewards of institutionalized practices.

Theorization is a process of abstracting from prevailing conventions, which may be hard to apply practically to more field-sensitive conventions – a form more suited to broader adoption (Abbott, 1988). Tolbert and Zucker suggest that theorization is comprised of “two major tasks”: the first involves specification of a general “organizational failing”, where local innovation is a “solution or treatment,” and justifies the innovation (Tolbert & Zucker, 1996). They also claim that diffusion also occurs where new ideas are proven more suitable than current practices, that there is a better way of doing something. Empirical work here is limited (Halliday, 1987; Van Hoy, 1993), but includes older studies, such as those of Collins (1979) and Freidson (1988).

Regulatory agencies, such as governmental and professional associations – and, as argued here, consortiums – are important to the theorization process because they foster the formation of shared meanings and understandings in a field (Ruef & Scott, 1998; Scott & Backman, 1990).

Associations have different roles in different stages of the process of change, where they react to events or consider routine activities. As described by Greenwood, Suddaby and Hinings (2002), there are six stages of institutional change: precipitating jolts, de-institutionalization, pre-institutionalization, theorization, diffusion and re-institutionalization, shown in the figure below. These factors are portrayed as being sequential in action. The factors identified here align with those of another conceptual model for considering issues and impacts in the law enforcement and emergency response community – Social, Technical, and Policy (or Regulatory as used here), and Lewin's change model (1951), from Treglia and Park (2009). That theoretical framework was initially applied to information sharing generally in the law enforcement and emergency response communities. Each of the identified factors is considered in assessing a situation or environment; however, they will have varying degrees of applicability depending on the particular circumstances being examined.

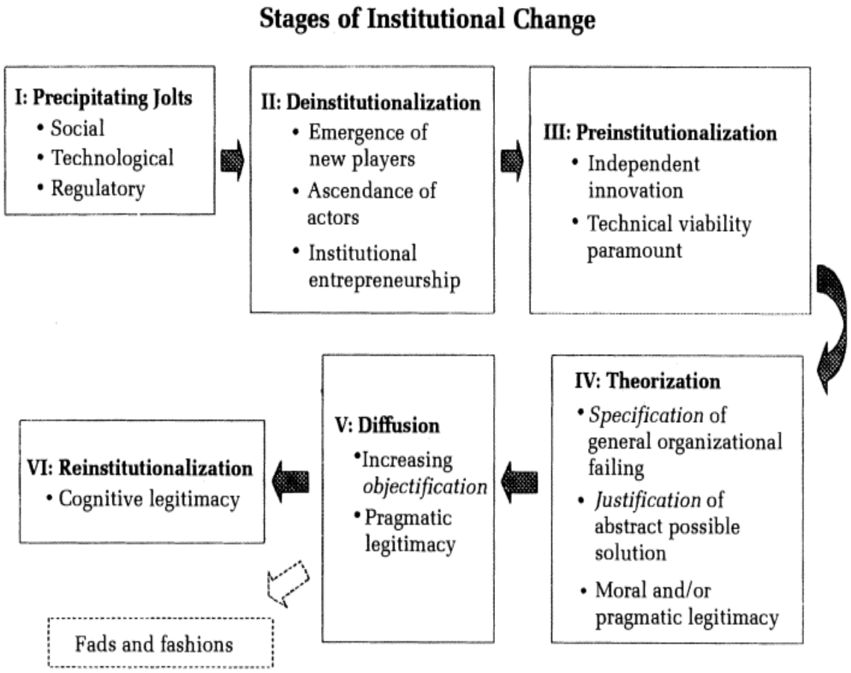

Stages of Institutional Change
I: Precipitating Jolts
• Social
• Technological
• Regulatory
II: Deinstitutionalization
• Emergence of new players
• Ascendance of actors
• Institutional entrepreneurship
III: Preinstitutionalization
• Independent innovation
• Technical viability paramount
IV: Theorization
• Specification of general organizational failing
• Justification of abstract possible solution
• Moral and/or pragmatic legitimacy
V: Diffusion
•Increasing objectification
•Pragmatic legitimacy
VI: Reinstitutionalization
• Cognitive legitimacy
Fads and fashions

Figure 25: Stages of Institutional Change

(Greenwood, Suddaby and Hinings, 2002)

4. Methodology

This essay reports on the CNYICC as well as its emergence and operation as a collaborative entity in the area of public safety. The CNYICC formed and developed to address the needs of various counties in facing technological, financial, and political challenges to providing interoperable communications to emergency responders and services to the citizens in Central New York State. The CNYICC is one of the first and most successful multi-jurisdictional public safety consortiums of its kind.

The case study reported on here examines various aspects of the external environment, agency context, and the consortium's organizational structure, goals, and governance processes. The purpose in this endeavor was to examine factors related to the emergence and sustained operation of the consortium in its context and to capture viewpoints of the participants from the different organizations and jurisdictions that have different roles that impact the consortium and its operation. The investigation was done in order to learn about consortium member views on constraints and barriers to interagency resource sharing and collaboration processes as the consortium evolved over time and to make their own observations.

This article reports the findings regarding the first years of this ongoing collaboration. The intent is to contribute to scientific and professional knowledge about cooperative information sharing in the law enforcement agencies and emergency response communities (referred to as public safety agencies). This research looks to respond to questions of: What factors support collaboration among public safety agencies in information sharing projects involving information technologies, and what factors work against having a successful ongoing collaboration among these participants?

This was an exploratory study that involved grounded theory and an inductive approach in parts to explore and investigate collaboration and information sharing in a specific public safety context, the CNYICC. A multi-method approach was selected using a research design including literature review, field observation, participant observation, document analysis, empirical investigation, case study, interviews and the Delphi technique. The interview protocol was adapted from the protocol used in the study of Public Safety Networks (Sawyer, Fedorowicz, Tyworth, Markus, & Williams. 2007; PSN, 2011). That research involved looking at various aspects of Public Safety Network (PSN) formation and continuation as collaborations that share information (Williams, Fedorowicz, & Tomasino, 2010). The PSN interview guide was used as the starting point for creation of the outline and structure of the CNYICC interview guide. The introduction, content areas and order of questions from the PSN interview protocol were considered by this researcher for applicability to the case study purposes and intended interviewees. Sections were deleted and parts added by the researcher. The final interview protocol used was reviewed with fellow researchers, the Syracuse University Institutional Review Board (IRB), the police, and 911 administrators and adjusted based on that feedback to the final form (see Appendix 3 Interview Guide).

To date the state has not formally signed on to the Memorandum of Understanding for the CNYICC, as have the counties. At the extended member level, there is, in principle, a last layer where the public may participate; however, the researcher did not observe any civilians or members of the public in this category during the course of the study.

Several consortium meetings of the core membership and the extended group were observed directly by the investigator from 2010 to 2012. Notes as to the content of the meeting and participants involved were taken by hand. These contacts were not recorded as researchers thought it may cause participants to be more guarded with their remarks. Notes and reflections of the researcher were taken both during and following the activities. Informal and ad-hoc contacts from 2007 forward involved conversations and discussion on the phone or at meetings of the consortium, department and committee, related to training and operational events, such as area multi-jurisdictional tabletop and field exercises related to emergency response. Note that one investigator was also a staff member within one of the consortium agencies and, thus, privy to a certain amount of insider communications.

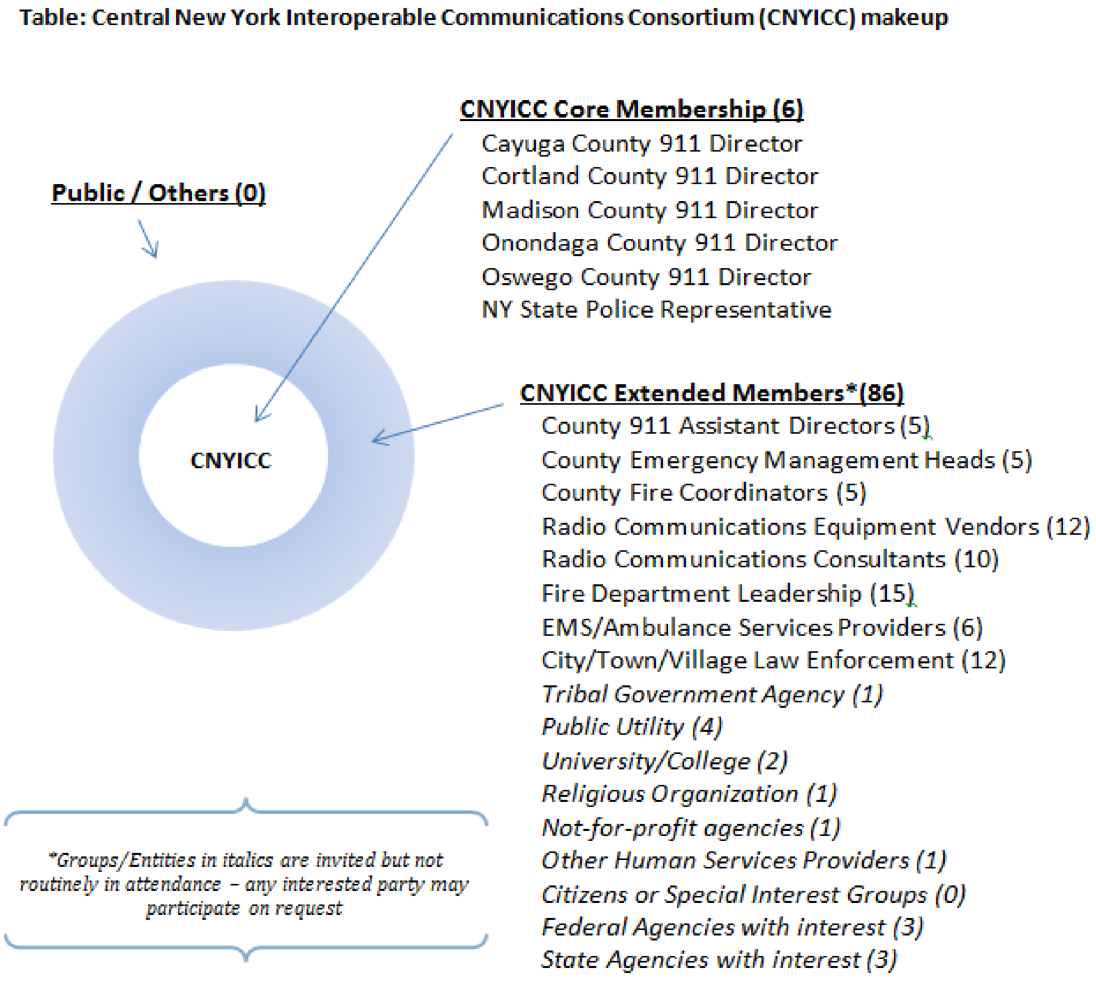


Table: Central New York Interoperable Communications Consortium (CNYICC) makeup

Public / Others (0)

CNYICC

CNYICC Core Membership (6)

Cayuga County 911 Director
Cortland County 911 Director
Madison County 911 Director
Onondaga County 911 Director
Oswego County 911 Director
NY State Police Representative

CNYICC Extended Members*(86)

County 911 Assistant Directors (5)
County Emergency Management Heads (5)
County Fire Coordinators (5)
Radio Communications Equipment Vendors (12)
Radio Communications Consultants (10)
Fire Department Leadership (15)
EMS/Ambulance Services Providers (6)
City/Town/Village Law Enforcement (12)
Tribal Government Agency (1)
Public Utility (4)
University/College (2)
Religious Organization (1)
Not-for-profit agencies (1)
Other Human Services Providers (1)
Citizens or Special Interest Groups (0)
Federal Agencies with interest (3)
State Agencies with interest (3)

**Groups/Entities in italics are invited but not routinely in attendance – any interested party may participate on request*

Figure 26: Composition of the CNYICC

Archival documents, both public and internal, were analyzed covering the time period from 2007, in which year the consortium was officially formed, through 2011. Documents were obtained through direct contact with agencies at their offices, at meetings, as well as through internet web sites. Searches of public records and organizational archives were also conducted. This information includes resources and material such as annual reports, website material, PowerPoint presentations, media coverage, MOUs, legislative reports, grant proposals, memos, meeting minutes, and other materials. These resources are summarized in Table 4 below.

~#	Resource	~#	Resource
30	Archival documents (public and internal)	12	Meeting agenda and minutes – Legislature
10	Agency Annual Reports	1	MOU
5	Agency Web Site Material	40	News Media Accounts (print & web based)
14	Formal interviews	12	PowerPoint Presentations by agencies
16	Grant Proposals	2	Prior documented interviews
90	Informal Agency Contacts/Interviews	24	Staff Meetings
84	Internal memos and email correspondence	16	Training exercises and meetings
4	CNYICC Core Group Meetings	3	CNYICC extended members meetings

Table 4: Summary of Data Collected

Semi-structured face-to-face interviews (ranging from less than a half hour to over two hours in length) were conducted with past and present members of the consortium as well as with key commercial sector consultants and vendors, related staff persons and other outside agencies to include state entities. Topics discussed included: background (agency and individual), contacts, stakeholders, technology, cultural environment, policy, governance, influence over change, competition, and the consortium (formation and what works and does not work well).

The full interview protocol is included in Appendix C.

The study involved a census of all five core 911 Director members of the consortium and additionally included one past founding 911 Director member and the state police representative. As previously described, core consortium membership consisted of the five 911 directors, or members of equivalent positions, from each of the five original consortium counties with a state police representative. Additionally, formal interviews were conducted with four other staff members from consortium county agencies and three vendors/consultants who had interest in public safety communications and related events in Central New York in this area. These persons were selected from the extended membership as they were in county management or supervisory positions or upper managers of the vendor/consultant agencies and would be familiar with CNYICC issues. Informants discussed the environment and their individual motivations for creating and participating in the consortium. They reflected on key issues, social, policy and technical challenges that they had encountered, based on the interview protocol previously described.

The formal interviews were conducted by one interviewer over a two-month period in the fall of 2011. All formal interviews were recorded and professionally transcribed for verification and analysis. During the period of the study, fourteen such formal interviews were conducted in addition to about 90 informal contacts/informal interviews that occurred in the workplace, at meetings, trainings and other events.

During the course of the formal interviews, the interviewer summarized the noted responses and solicited verification and additional feedback from the informants as a means of verification of understanding. Transcripts for the core members were provided to each individually to review for accuracy and verify allowable content for use in the study, formally referred to as “member checking.” The business here involved sensitive material and activity, so information required vetting for dissemination or use.

The researcher spent a considerable amount of time reviewing the tapes, transcripts and other supporting materials to look for patterns, common themes and conflicting elements. One such information conflict came in the area of the stated rationale for consortium members working together. The members, in the interviews, state that they did not meet for financial reasons or in response to regulation but for broader more higher order interest goals. In the public material, such as media accounts and legislative transcripts their participation is described as necessary to address financial and regulatory needs as well as for technical reasons. This could be reconciled by considering that the purpose of the public and legislative rhetoric was to persuade and provide a clear statement and reason for the need to participate that could be embraced and understood by those audiences. There was no such need for this in the private interviews. What is said publicly does not always match that said behind closed doors.

A table summarizing the timeline for this research is provided below (Table 5).

Date	<<< Related Meetings & Activity	Case Study Milestones >>>	Date
		Interviews with Nlets personnel, Phoenix, AZ (PSN Study)	12/16/2009
		Met with Onondaga County Commissioner, preliminary	06/08/2010
		Formal request for access to CNYICC for study	06/10/2010
		Access to CNYICC for study granted	07/28/2010
08/25/2010	CNYICC Meeting, Extended Membership, Oswego, NY		
09/01/2010	CNYICC Meeting, Extended Membership, Oswego, NY		
01/26/2011	Winning Grants and Meeting CJIS Requirements, Teleconference		
03/16/2011	NYS Univ. Police Morrisville College Tactical Exercise, Morrisville		
03/30/2011	CNYICC Meeting, Core Members, Syracuse, NY		
04/06/2011	Cyber Terrorism Speaker, Douglas Smith, Asst Dir for Private Sector US DHS, Albany, NY.		
04/11/2011	ICGP (Interoperable Communications Grant Program) Grant Summit, Wampsville, NY		
04/19/2011	911 Center CAD Product DEMO, Wampsville, NY		
		SU IRB (Institutional Review Board) Case Study Submission	04/24/2011
05/05/2011	SCNYUA (Syracuse Central New York Urban Area) Working Group, Syracuse, NY (Meet first Thursday each month 10:30 am)		
05/24/2011	DHSES Office of Counter Terrorism Conference Call - RE: FY2011 HSGP Grants		

06/28/2011	Nlets Conference & Business meeting, Burlington, VT	
	Informal interviews with Nlets members	06/29/2011
	SU IRB (Institutional Review Board) Case Study Meeting	07/11/2011
07/22/2011	SCNYUA & CNYICC, Tabletop Exercise Planning Conference, Teleconference	
	SU IRB (Institutional Review Board) Case Study Approval	07/22/2011
08/01/2011	SCNYUA Crisis Response Syr. Univ. Field Exercise, Syracuse	
08/08/2011	SCNYUA & CNYICC, Tabletop Crisis Response Exercise, Auburn	
	Formal Interviews with participants begin	09/15/2011
09/21/2011	NYS Division of Homeland Security and Emergency Services Office of Counter Terrorism Regional Workshop, Auburn, NY	
10/12/2011	Syracuse UASI TTX After Action Conference, Teleconference	
10/14/2011	CNYICC Meeting, Core Members, Oswego, NY	
	Formal Interviews with participants complete	10/14/2011
	Data collection from interviews and transcription complete	10/21/2011
11/01/2011	Critical Infrastructure Grant Program (CIGP) Conference Call	
	Initial factors identified, list & interview transcripts sent to CNYICC core members for ranking, input, data verification and edits (Delphi technique begin)	11/27/2011
11/28/2011	CNYICC Meeting, Core Members, Oswego, NY	
	Explain factor ranking request to CNYICC core participants	11/28/2011
	Factor rankings received & combined then resent to group for comment (one member unavailable)	11/29/2011
	Final factor rankings and edits received & compiled; result verified by CNYICC core participants	12/09/2011
	Case study draft of results completed	12/26/2011
01/07/2012	Syracuse Police/Burmese Community Meeting, Syracuse	
01/19/2012	Madison County Area Emergency Response Tabletop Exercise, Wampsville, NY	

Table 5: Timeline of Research, December 2009 – January 2012

Using a modification of a normative (or consensus) Delphi Technique, the six core 911 Director members (five from the counties and one retired founding member) were asked in their review to rank the key factors that had been identified by investigators in the review and coding of the responses and to add or remove factors as they deemed appropriate (Turoff, 1970; Charlton, 2004; Yousuf, 2007). Delbecq, Van de Ven, and Gustafson (1975) indicate the Delphi technique can be used “To correlate informed judgments on a topic spanning a wide range of disciplines.” Core members are considered subject matter experts in public safety communications.

A preliminary list of sixteen factors believed to impact public safety collaborations in positive and negative ways was provided to them for consideration. The initial list was derived by the researcher from analysis of all interview responses as well as responses to specific questions about the consortium including: “what about it is working well, what is not so well, why do you stay in this,” and “what could be done to improve the effectiveness”? The related responses were aggregated based on similarity to reduce the number of factors as much as possible. Researchers reviewed the data looking for these themes both manually and through the use of Atlas.ti (data analysis) software. The researcher studied the audible and transcribed interviews over several weeks to identify themes and issues. Other researchers, doctoral students and public safety personnel were consulted regarding the various themes and categorizations proposed. This process was repeated in part several times. The participants were asked first to review the factors provided, then to add or remove factors as they saw fit and finally to rank order them, ties for the factors were allowed (one member was unavailable for this stage of the process and after the final ranking was completed they indicated their support for the findings). Following the receipt of all refined and rank-ordered responses, investigators created an aggregated rank-ordered list based on that ranking, and sent it out to the group for final comments and appraisal. Feedback from this stage was then used to create the final factors – considered important to establishment and maintenance of successful public safety – identified in this case study.

Threats to validity were acknowledged and addressed in a number of ways. Bias in the participant selection process was reduced, as there was 100% participation of the core consortium membership. Another threat to validity in the interview and data analysis process involved the potential for investigator bias (Weiss, 2004). The researcher here had prior experience in public safety and the potential for observing things in a pre-conceived way had to be accounted for (Diesing, 1992). Awareness of this, engaging with other researchers, and having input and direct feedback from the participants (member checking) reduced this effect. This was a source for potential subjective validation, expectancy, and bias in the data interpretation and observation process. The established interview protocol was used with all participants.

A concern is that some respondents may not complete the process. In the CNYICC case study, one of the core members was unavailable during a portion of the Delphi technique survey where responses were reviewed and ranked. This member reviewed and accepted the responses and rankings after the others had already completed this. No additional changes were made.

The threat that there may be contamination with others participating in the study would not necessarily have adverse impacts. Networking by the participants was allowed. In real life the respondents discuss their activities with anyone they choose and therefore if they wish to discuss the study with each other while it is going on that is fine and reflective of their actual way of operating.

This material and process as described formed the basis of the case presentation in the sections that follow.

5. CNYICC Overview

The CNYICC was formally created in 2007 by a Memorandum of Understanding (MOU) between five central New York counties – Cayuga, Cortland, Madison, Onondaga, and Oswego (shown in the Appendix) – and signed by the various legislative bodies. Consortium membership has been evolving since its inception with the New York State Police participating since 2009, and there are several other counties now considering joining as well. The active working team for the consortium consists of the participating 911 County Administrators and representation from the New York State Police, with technical support being provided individually and by various private sector consultants under contract with some consortium counties and acting without contract for others. The mission of the consortium is “[t]o provide wireless UHF narrow ban, simulcast communications network for all first responders in the CNYICC area, to encourage participation in the CNYICC thereby reducing member agency cost, and to continue to seek alternative funding methods to reduce local governmental costs” (Allen, Balloni, Hartnett, & Stayton, 2007). Consortium members promote creating interoperable communications systems for all emergency responders. The consortium is not funded, nor does it have dedicated staff or formal corporate entity status. The mission statement provides direction for the consortium members collectively and as individual entities.

The CNYICC meets on a monthly basis and as needed. As of this date, the consortium has developed only a draft plan of governance and policy that can be expanded upon further. The governance plan is not signed, nor has it been formally adopted; the version at the time of this writing is shown in the Appendix E (the current plan was given to an upstate college for review and possible update by CNYICC). Activities, strategic planning, and governance (to include membership, agency rights and responsibilities, and regional authority for coordination and assignment of interoperability assets) remain as informally negotiated items without formal written policies. The consortium has a Chairman who is appointed by the working members. The core members, who are the 911 directors for the participating counties, meet to decide policy and approve actions to be taken in the name of the consortium, such as the consortium approval of a policy position or grant proposal to jointly pursue. The consortium also has an extended membership group that meets several times a year. The extended membership meetings include the core members as well as their staff and may include other county emergency managers, heads of fire departments, EMS, law enforcement, hospitals, and public utility providers; colleges, universities, communications services, equipment vendors, and others are also allowed to attend.

In 2010, there was a significant change to the core membership of the CNYICC. A strong founding member accepted another government position, and so the new incoming county 911 commissioner was going to assume a role in the consortium as a core member. Potentially, this could have been a negative turning point as this member had been a critical part of the initial formation and possessed great leadership, vision, and interpersonal skills. Since it was a relatively small group, this also meant that each participant had a strong impact on the consortium as a whole. The core members had no prior personal relationships when the consortium formed. They had known of each other through participation in professional association meetings and through participation in training and conferences. In this case, the incoming commissioner possessed interpersonal and technical skills, as described in the following sections of this article, which allowed for a fluid transition and continuation of synergy among the group that continues to date. When asked about the potential of changing the consortium dynamics due to such a transition, some of the core members said that they (as a group), and the positive momentum that was there, simply would not have allowed a person to come in who did not fit; the new arrival would have had to conform.

The CNYICC is an example of a challenging new model for collaboration among previously independently oriented public safety entities. Police, fire, and EMS agencies as well as their respective jurisdictions have traditionally been autonomous in their operations and governance. In this paper, researchers identify several factors that, it is argued, led to this newly created union and additional factors that promote sustainability and success of such partnerships in the public safety arena. In the next section, researchers briefly identify some external factors and issues that were active at the time of the consortium's formation and progress, and which impact consortium decisions and activity. Figure 27 below depicts CNYICC's influence and relationships, both inward and outward. Arrows are used to show direction of influence and a general weighting for degree of influence, contact, or frequency. As shown in the figure, the individual 911 directors have increased and more direct access and influence with vendors and government agencies than if there had been no such consortium.

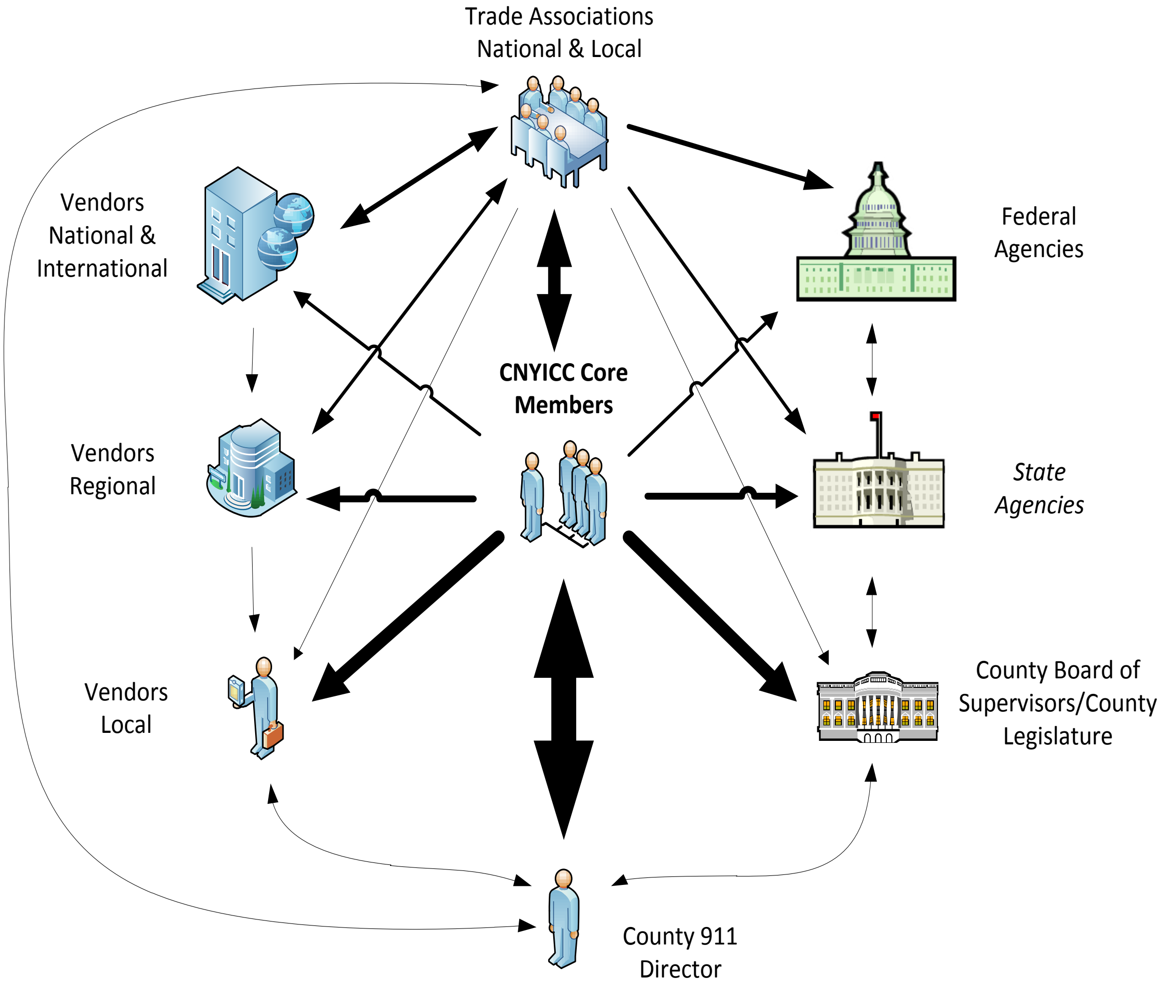


Figure 27: CNYICC Influence and Relationships

6. External Factors

A number of external factors were identified as having influence in the formation and ongoing operation of the CNYICC. This section begins with a timeline (table 5 below) highlighting these factors/events at the federal, state, and local levels, followed by a listing of the identified external factors. An expanded timeline (table 9) with event description and implications included is provided in Appendix H.

Date	*Federal Level Event*	*State Level Event*	*Local Level Event*
1982	National Emergency Number Association (NENA)		(CNYICC members all participate here currently)
1989	Project 25 (P25 or APCO-25) initiated		
1991		911 Wireless Surcharge imposed	Counties not getting proposed revenues as anticipated
1995	Project 25 - Phase I Completed		
2001	9/11 Terrorist Attack in US	Statewide Wireless Network (SWN) RFP initiated 9/11 Terrorist Attack in US	9/11 Terrorist Attack in US
2003	Next Generation 911 (NG9-1-1 or NG911)	Next Generation 911 (NG9-1-1 or NG911)	Next Generation 911 (NG9-1-1 or NG911)
2004	Narrowbanding Land Mobile Radio (LMR) ordered by FCC		
2005	National Incident Management System (NIMS) use mandated by Presidential Directive Incident Command System (ICS) use mandated by Presidential Directive SAFECOM – Interoperability Continuum Hurricane Katrina	States adopt same States adopt same Hurricane Katrina Statewide Wireless Network (SWN) initiated	
2006			***CNYICC Discussions Initiated***
2007	Project 25 compliance verification from vendor required	Statewide Wireless Network (SWN) reporting required	***CNYICC Formally Created (MOU)***
2008	The National Emergency Communications Plan (NECP)		
2009		Statewide Wireless Network (SWN) Cancelled Project 25 (P25) standards included at state level	
2010			CNYICC Core Membership Change

		911 Landline Surcharge and Mortgage recording tax blocked by State	
2011		911 landline Surcharges and Mortgage recording tax still not allowed by State	911 landline Surcharge and Mortgage recording tax adopted by counties

Source: (Treglia, 2012) See also table 5 in appendix.

Table 6: Events and Activities Impacting CNYICC

External factors that impacted the CNYICC include the following: Statewide Wireless Network (SWN), Project 25 (P-25), Next Generation 911 (NG911), National Emergency Number Association (NENA), SAFECOM, The National Emergency Communications Plan (NECP), National Incident Management System (NIMS), Incident Command System (ICS), and Narrowbanding. These factors are each described in Appendix I.

6.1 Funding Environment

The funding climate in the United States for public safety communications centers was not affluent. Policy measures for raising funds for infrastructure was being curtailed by limitations on such things as counties ability to create revenue through things such as mortgage filing fees or surcharges. In the state of New York, there has been ongoing conflict regarding the appropriation and distribution of allowed surcharges and allocations for interoperable communications and infrastructure improvement. During the time of this study, there were emerging from the federal and state levels, a number of competitive and formula funding opportunities through a variety of agencies. The state of the nation regarding the scope of need for systems overhaul and improvement was far greater than the proposed allocations would provide. Local entities took issue with having to compete for these financial resources that they felt were due each by reason of their individual contributions. Having fewer opportunities for funding makes it more likely that public safety entities will see each other as competitors and this could lead to lack of cooperation. In the case of the CNYICC it brought them together more. The conflicts over funding made for a common cause or issue that public safety entities could identify with and work together to address as a group.

7. Findings

This section presents the initial findings and identifies factors considered important to establishment and maintenance of successful public safety collaboration– in this case the CNYICC– involving multiple county level government agencies in New York State, which is one of the central research questions. The final factors presented were derived from the data collected in the case study and are the result of the combined responses from all primary consortium members to include one past founding member, as described previously in the methods section.

The responses were inductively derived from the interviews and data through a grounded theory approach. The terms used are taken and presented, where possible, verbatim from the respondents. The interpretation and use of the factors are from the perspective of the interviewees. Use of the terminology by the interviewees may not correspond directly or accurately to the conceptualization of these same terms in other contexts or the academic literature of a particular field. The findings *do* accurately represent the opinions of the consortium members and related stakeholders from an insider perspective.

Although these factors are presented individually, they are interrelated and should be considered collectively. Researchers argue that in concert the factors represent important elements of what in this case is considered a successful collaboration. At this point in the research, researchers are not able to quantify or separate out individual factors to assess individual impacts. A summary of the important factors to consider in establishing and maintaining a consortium in public safety (derived from the consideration of study data and feedback from consortium members) includes the factors identified in Table 7 below and further described in the section following.

What helps foster Collaboration:

1. In it for right reasons - greater good
2. Trust
3. Personal characteristics of key managers people oriented focus
4. Face to face, and regular contact with partners and stakeholders
5. Autonomy and flexibility for participants
6. Basic written agreement/understanding (flexible, not complex or detailed)
7. Measurable Objectives
8. Technical Standards
9. Share control, all are important, i.e. don't have biggest partner in charge
10. Use consultants for knowledge and insights

What does not help Collaboration:

1. Lack of standards
2. Dictate from the top, top-down bureaucracy in County Governments
3. Assumption that everything will work everywhere, Insist participants follow same course
4. Manage by memo or indirect communication
6. Look out just your own interests
7. Strict and detailed governance plans

Table 7: Factors Important to Successful Collaboration in Public Safety

7.1. What helps collaboration

7.1.1 In it for right reasons - greater good

All core participants identified being in it for the right reasons and working for the greater good as the top most important factors. This is the highest rated factor among the consortium members. “The enemy of my enemy is my friend” is translated in public safety to signify the common foe of protecting lives of the citizens, officers, and responders that put themselves out to help and protect others. The difference in the public safety realm, that sets it apart from the business world and to a degree the not for profits, is the motivation;, in public safety, that it is about saving lives. Those engaged know it and feel it. In a corporation when the third quarter returns are below the projections, there is a problem. When the 911 center has a failing in the system or their communications to an officer on the scene or between fire units needing information and resources to battle a blaze or catastrophe people’s lives are lost and that has no comparison on a balance sheet. Higher-order interests as a motivating factor in business literature regarding collaborative behavior is not on the list. Where collaborators can satisfy each other's different interests without hurting themselves, collaboration can occur (Wood and Gray, 1991). Similarity in mission, and commitment to similar populations, have been identified as important factors for collaboration success (Lax and Sebenius, 1986; Thomson, 1999). The effects of these factors are most visible in the public safety realm where it is this higher-order interest and mission that drives behavior. Those who have competing fiscal and political interests are galvanized and unified against the foe or notion of saving lives and protecting the public in a way that overcomes such barriers.

In the interviews, informants provided several emotional examples of their shared interest in higher order interests. One administrator said:

> “One of the reasons that so many lives were lost on September 11th is the inability to communicate between emergency services. We want to build a system where we can communicate between emergency services. People die when communication, it’s critical on the battlefield and it doesn’t matter whether you’re fighting a fire, fighting a, doing a major police action or dealing with any other emergency, or doing a battlefield.”

Another administrator expressed his thoughts regarding another consortium member in a leadership position:

> “… he’s also in it for the right reasons. He’s doing it for the right reasons.”

When asked about formation of the consortium as being done “because it was just the right thing to do,” one administrator replied:

> “That’s, I don’t think you could have hit it more on the head. The people that were in the business and knew what we were facing got together ‘cause, and we all agreed this is the right thing to do, now how do we get others on board and so that was agreed before any government was involved in it other than at that 911 director level. We agreed that this was the right thing to do.”

Lessons learned in this arena are applicable to other areas. In government, there is a higher order interest of helping people and in the not for profit sector the entities are typically in it for a higher purpose, in school districts this is also true. In those cases, one should expect that managers and policy and practice should press on the higher moral ground for doing the job to increase collaboration and worker performance and cooperation and sticking to the mission. This works for collaboration and also in insuring cyber security, which is an ongoing challenge that requires constant vigilance and reminders from management to keep it fresh as it is easy to get complacent when things go well.

This is a highly regulated and technologically infused area and environment. In this way, the public safety consortia and operation is differentiated from a great many typical businesses. Still, much of what is learned here is relevant to other places, business or otherwise, that share the policy and technology complexity and engagement.

There is further work to be done to see if the higher-order interest has as strong a corollary in the business world. Existing models for collaboration should now rate trust, personal contact and shared vision highly in the formation formulas for cooperation. Other business strategic texts address formal strategic alliances as existing beyond a narrow joint project or action to a longer term relationship that acknowledges that at times one may be getting more from the relationship than the other but aware that over the long term it is better for both, sticking together in lean times as well as when all is good - or not jumping ship just for a short term gain.

7.1.2 Trust

Trust and establishment of trusted relationships was rated as essential to success in collaborative efforts. This is reflected in the comment from a 911 administrator:

> “Right from the very beginning we were very candid and honest and we have a very good relationship among ourselves that we’re in it to work together and help each other out and I think that that’s really been the most important part is the fact that there’s no, you know, we don’t, there’s no hidden agendas, you know, we just seek to do the right thing for the ..."

Another administrator spoke highly of their peers in the consortium:

> “They were all straight shooters. I mean, really, they all pretty much give you things at face value. I know when XXX tells me something, or when YYY tells me something, I’m getting it at face value.”

Those interviewed also reflected a sense of trust in others generally:

> Respondent Why did I, I trust people until you give me a reason not to.
>
> Interviewer Okay. And then these people gave you plenty of reason to trust them.
>
> Respondent Yes.

There were examples of how consortium members worked to establish trust with stakeholders:

> “I’m not going to tell you what you want to hear;, I’m going to tell you what the truth is,

> …that’s about building faith and confidence that what you’re saying is correct, and there were times that what we were saying was not correct because we misunderstood something and then you go back to them and say you know what I said at the last meeting, that was not correct and again you build credibility, you build faith, you build that relationship …”

Another administrator described the trust building process as ongoing and requiring direct personal involvement:

> “We’re going down to the firehouse, we’re going, I cannot tell you the amount of night meetings and face-to-face, it’s all about building relationships and trust.”

Trust is essential to unified action. Law enforcement and emergency response agencies are tasked with responding to crises under any conditions or circumstances. The movie "Gladiator," DreamWorks Home Entertainment, 2000, includes a telling scene where the hero (Maximus) unites his comrades, who are expected to be defeated in a mock battle against more powerful forces. As they stand facing the large closed doors in the Roman Coliseum, Maximus urges them saying "whatever comes out of these gates, we've got a better chance of survival if we work together. Do you understand? If we stay together we survive" (Wick, Franzoni, Lustig, & Scott, 2000). By their coordinated, selfless, and collective action, against the terrible and unknown, they triumph. You can picture this today as the Chairman and CNYICC face the ominous doors to the legislative chamber (for example) urging consortium members "work together," "whatever comes out" of the legislature, committee, technology, or other source, and they will have a better chance for survival. The members have stayed together and have better prepared and positioned themselves for success and opportunity because of this.

Levels of trust are identified in the literature as playing a strong role in people's or groups choices to share information, and it is argued here collaborate. Razavi and Iverson portray the sense of trust as varying by degree (2006). They describe trust as not simply being a trust or not trust decision but rather that users' sense of trust may move from greater to lesser levels. This is applied to human groups as well in virtual and face-to-face environments. Level of trust, according to this same study, can be raised over time through participation with the group or community. Also consistent with the findings of Razavi and Iverson, members of the consortium were able to meet virtually and continue to grow their trust where face-to-face meeting was not possible. The significance of developing trust was noted by all core members of the CNYICC interviewed.

7.1.3 Personal characteristics of key manager's people oriented focus

Management style and personal characteristics of key leadership personnel was identified as an important factor to success of getting people to work together.

When asked about the skills necessary for success in the consortium, one administrator said that the most important would be "vision and it's that ability to go out there and talk to people and get them on the same page."

Each of the director's involved showed evidence of people-focused orientations. A cultivational culture was evident in each of the agencies visited. Investigators observed that open door policies were the norm. Most had candy or food in their offices to invite casual meetings. All members have pursued higher education. Each of the consortium members made a point of recognizing and encouraging quality performance in their staff formally and informally. One administrator routinely uses items accumulated from participation in conferences and workshops (such as coffee mugs, water bottles, pouches and pens) as prizes to acknowledge and recognize those doing good work:

> "There's very little you can do as a government agency to recognize your people. So anything that you can do, I think, is a good thing. You know, I can't give them a bonus if they do a good job, but I can give them a pat on the back; I can say pick something out of the prize bin 'cause that's what that box is over there, the prize bin, and I fill it with all the things I get from all the conferences that I go to, you know."

Individually, each of the consortium members is committed to working together constructively and selflessly, as one administrator describes:

> "Yeah, I think so. I think because of our very nature that we've been so far been able to be successful, and I mean when I said each of us are very capable of checking our egos at the door when we sit down."

There was observed a clear management style that engaged with others, managing by committee and making use of multiple means and channels for input. This is well described by one of the 911 Administrators:

> "Well, there's a ton of different, I mean we, not a ton, but one thing that I think makes this center very successful is that it doesn't do things in a vacuum. We have always been

open to input by committee and things that we do. For example, when the radio system was started up from the very beginning there was a team leads set up, and that team leads [sic] was consisting of representatives from all the major users, police, fire, government, county government, and they made global recommendations, but they also made service related recommendations of the radio systems. So, for example, you know, we talked when planning this system we talked overall on what we all felt we would want to do in writing the RFP and then, when it came to the things like programming radios and templates and talk groups and things like that, each service, you know, we would meet as a combined group to talk about the interoperability of it, but when it came time to how does county fire work, you know, fire people would meet and make those recommendations, police people would make those recommendations. So, a lot of things that we do here are done by committee, which I think ultimately is responsible for a big portion of the success of what we do. "

"You know, computer-aided dispatch, when we did computer-aided dispatch, it wasn't just us making a recommendation we involved all the users and what CAD system are we going to go to and, consequently, I think we got a much better CAD system ultimately. So we do do a lot of things by committee."

"I don't think that fire has this, but there's a police users group that has representatives from the police service, and they will sit there and meet and talk about things that, if it can be resolved on that level, it gets resolved, if not it comes forward to the representative

> to PROC (Policy Review and Oversight Committee), PROC will bring it to the table kind of thing."

There was clear evidence that the consortium sought out participation of the stakeholders and others throughout the process. These meetings are ongoing. One administrator describes a "roundtable" discussion conducted with extended members:

> "Yeah, our roundtable discussion includes members of each piece in the consortium and it's open to everyone; we've been very open with who can be a member or take a part in this. You know, early on, we invited you to come and see and we were very happy to have you here and now we have the state police playing a part in this consortium idea. So we bring them to the table. Anyone who we think can advance our cause to be very honest."

Most all administrators reported adjusting their schedules to be able to interface with those working afternoon and evening schedules. The positive characteristics of the members of the consortium, as reflected in the way they work within their agencies, are believed to be an important contribution to its success.

7.1.4 Face to face, and regular contact with partners and stakeholders

Engaging personally, face to face, with partners and stakeholders was identified by all of the consortium members and vendors that were interviewed as significant to developing and maintaining working relationships. This was originally described as face to face contact with partners and separately with stakeholders but combined them for discussion here as they are related and share justifications. This is explained by one of the 911 administrators in the following:

> “The stakeholders, well, you have your own government is one of the stakeholders, certainly all of the fire and EMS first responders is another major stakeholder, citizens are your stakeholders. Ultimately, they’re footing the bill and in addition to reaping the greatest benefit because they know that if we have the right tools, we can help them when they need our help. Those are the critical stakeholders.”

When asked directly if they felt that if they did not meet face-to-face would they have accomplished what they did or be as organized, the respondent administrator answered, “No, no I would say definitely not.” This position is further reflected in statements from other administrators interviewed:

> “I like that face-to-face contact, it builds relationships as well and the rapport. It’s you need to have face-to-face stuff.”

> “…we’re going, I cannot tell you the amount of night meetings and face-to-face, it’s all about building relationships and trust.”

Those interviewed also spoke of limitations and problems with impersonal communication such as emails or memos:

“Well, first of all, sometimes things in e-mails can be misinterpreted: you don’t have inflection in your voice, it’s easier to explain it than it is to– explain it in words– than it is to explain it in a typed message. I find myself doing that often, you know, e-mail back and forth, let’s just talk to each other, so I get on the phone and say look at, ‘this will work much easier.’ You can’t have a conversation through e-mail as far as I’m concerned, so I mean, you know, e-mail is good for ‘we have a SNIC meeting next Tuesday at 10:00, see you then,’ but it’s not good for, as far as I’m concerned, ‘XXX this is YYY how you doing, …, you know, I’m thinking about having a SNIC meeting next week what days do you have available. You know, I talked to ZZZ he’s got Tuesday, how does Wednesday look for you?’ You can’t do that kind of, I can’t do that on e-mail.”

“Yes. I do the County Police Chief’s meeting every month. I do the Central New York Fire Districts meeting every two months it is, but face-to-face wherever we can.”

“I think the best form of communication, and this is me personally, is face-to-face. A lot of people can interpret e-mails incorrectly– the tone of them, or the wording– some people aren’t good writers and have trouble expressing themselves, electronic or on paper, if you will, and I think it’s best sometimes done face-to-face.”

“…but we also have conference calls now ‘cause we’re getting down to the nitty gritty. Some of those conference calls can be intense because people take what was said the wrong way by other members; well, you’re not seeing the person and it can get, it has

> gotten, confrontational at times where the same team met yesterday things were said that could cause confrontation, but they weren't because you're in the same room, you see how it was delivered, the tone it was delivered, the mannerism, the body language."

The practice of engaging with as much personal contact as possible under the circumstances was consistently observed and reflected in the interviews. Building or establishing trust is described as a key linkage in the connection between communication and cooperation (Ostrom & Walker, 2005, p.34). Consistent with the observations in the case study here researchers such as Ostrom and Walker (2003) demonstrated that trust and positive reciprocity is promoted through face to face interactions in both small and larger groups. Trust is further characterized in the literature as "a lubricant of social interaction" (Ostrom, 2003). Good faith builds these positive perceptions and relationships for all parties involved.

7.1.5 Autonomy and flexibility for participants

Recognition of sovereignty and maintaining individual identity and control are important to the members of the consortium, and any formation to organize must account for this. The counties, agencies, and departments that all must work together are diverse. There are strong interests and personalities involved; however, each are brought together under the common interest of protecting the public. The current organization and governance structure of the consortium reflects this and seems to be effective. The current MOU is the guiding document for the operation of the consortium but to date the policies and procedures that would further formalize and codify the operation of the consortium and supporting committees or groups remain on the drafting table. In this case, less formalization seems to be valuable to sustaining the effective relationships. Several remarks from those interviewed provide evidence of this:

> “We started doing this because we needed to and we wanted to, not because somebody told us to.”

> “Alright, it wasn’t like ‘well you got to do this, no you don’t, you don’t have to do anything.’ That’s what makes the consortium work: there’s no pressure to do anything okay. That’s probably the only success story I can really tell you, but it was also, I have to tell you, that it was also a component of that was the personalities involved, the people involved. They were all willing to work together; there was no, ‘it’s mine, I’m better than you are, I’m smarter than you are,’ I call it the brat mentality, there was none of that. They were all very straight forward, very easy to work with, you know, we’re willing to share, there was none of that, I got to be in charge or I’m not playing or I’m going to take my toys and go home, I didn’t see any of that the whole time and that’s four years now, five years now it’s been going on.“

Other remarks included statements such as:

> “The fire service in general has got major issues, issues that I can’t fix. One, because we don’t have any control to fix them. They’re all kings in their castles and there’s major issues ...”

> “It’s not a policy thing, it’s the law. The law says they’re the kings in their castles, it’s the home-rule state and you can’t change it unless you change state law. Change state law

> we can fix some of these problems, but people in my position to work for the county we have no authority to step into a fire department and say hey you're doing this wrong"

> "That's the key is, you know, taking the politics aside, the finances of folks that they can afford to fund the solutions. So they need to be flexible and have a work around and you'll still maintain that connectivity and the coordination between these users that, you know, I think that's happening."

Other interviewees said:

> "But, at one point, we went to Albany, went to Washington and we lobbied for this, you know, and SWN (Statewide Wireless Network plan) and said look, 'we don't have any problem with SWN, we'll let SWN on the network, we don't have any issues with them, we're not in competition with them, we want to maintain and own our own radio system just for the safety of our first responders, I don't want to be dealing with somebody in Albany and the bureaucracy that goes around with it, okay. So if you want to come on the system you're more than welcome to do that,' and that's the premise we went on."

> "I'll have a regional system here; we'll have a regional system here, you can go anywhere in five counties, you'll have to go a long ways to get out of reach of our radio system, which is really cool. Farther than probably you ever will, you know, you can't expect to go to New York City and talk on your radio system."

Still others said of flexibility that:

> "You can be a member of more than one consortia. You can work with the other counties. You know, we have Onondaga as well as they have their own little consortium. Broome County is developing their own; we're going to be a part of both of them."

Interviewees provided statements regarding their sentiments on sovereignty as:

> "…when they (State) came here and did their presentation, we went after them on that, 'who's going to run this, who's going to operate it, who's going to own it, how do we make changes? Well you have to call the state, and we'll give you a rep from the state, call Albany they can put you on, make changes and we're all looking at each other going thank you very much we're out of here, okay, have a nice day. '"

> "We weren't giving up, we've had our own system for years, and we're not giving up our own system here and it should be managed and funded locally for how you operate and every county is different, some are more rural than others and that needs to stay in place. You lose sight of that; you're going to have a New York City mentality running everything up here and the next thing you know it's not going to work for anybody, and it will fail miserably."

Another member continued on about local interests and flexibility as:

> "… you have to design it until it functions on a local situation locally for what you do, your county is different that my county. My county is different than your county; we all have our different problems and our different issues. You can't take one shoe does not fit everybody, even during the consortium, we recognized early on some of the stuff we got working here they will never have, never want, that's okay, you know? That's okay because if it's there and you ever want to get into it you're welcome to join us that's fine too and that's how we left it."

7.1.6 Basic written agreement/understanding

The common understanding in business is that partnerships should be codified in detailed written contracts that clearly specify goals, expectations and responsibilities for all parties involved. Contrary to this notion, the CNYICC operates through a loose written memorandum of understanding (MOU). The consortium is successfully operating in this way still. A finding here is that agreements should be basically written, flexible, and not complex or overly detailed. Several of the interviewees provided some insights and support to this form of operation:

> "No, it's a very, I think, it's a loose fit organization. Like I said, it's really the consortium is the five of us and I think that we all have the same common goal, you know, we're very concerned about the service that we provide our people and we all look into the ghost of Christmas future and know that our business is going to get more and more expensive and we know that working together we can do better than working independently in terms of saving money, putting together better interoperable systems.

> So it’s a win/win situation: there’s nothing to lose here. So, I think that helps and they’re good people, you know… they’re very good to work with.”

Adjustments to initial plans are required at times and the present consortium structure allows for flexibility. Working from an overall agreement that the county has originally approved, adjustments are made case-by-case as needs, priorities, and opportunities arise. A 911 administrator gave the following account of making changes in course:

> “Exactly, they’re just made operationally and I don’t think there’s anything– there’s nothing illegal about that– you make operational adjustments, but mostly you know, the contract is your guiding document and it’s good to spend a lot of time, my recommendation, spend a lot of time in that contract clarification period making sure ...”

In one instance, linking two sites across counties through a microwave link was discussed. This was not part of the original plans, it bore a significant cost, and there was no funding for it. During a consortium member meeting, the State Police informally offered to provide the hardware and install the link. This was a several hundred thousand dollar general verbal commitment made during the course of a meeting of the core membership. The state *did* follow up and formalize the offer and working with the consortium and counties involved the link was established. The initial discussion and offer to assist by the state occurred through the course of consortium meetings. The formal follow up required written agreements and financial commitment as well as discussion and agreement over future stewardship and maintenance. The process slowed and the offer nearly was withdrawn at the point where the verbal commitments were to be put to paper and the formal agreement drafted. General consensus towards the goals and mission was found to be relatively easy to achieve. When the details of the contract and commitment had to be formalized, it was more scrutinized and the informal way of working gave way to the more business style formal contract negotiation process. Still, it is possibly because of the relationships that are part of the consortium that this volatile stage was able to be effectively worked through. In this case if it were not for the positive relationships established in and through the consortium the solution would have not come about in the first place or likely been dropped in the negotiation phase.

There was discussion across the consortium members that, in the future, as more complex agreements and activities are undertaken, there may be a need for a more formal structure. This was reflected in the statement below regarding potential benefits to greater formalization:

> “I think we have to. In order for us to be successful in that area, you know, up to this point what we have now has worked and will probably continue to work for what we’re doing right now, but if we want to do better, if we want to explore new areas like a regional communication system, or you know, a regional telephony system, or regional maintenance, or regional repair shop, or you know, think way outside of the box we’re going to need more structure than that. “

7.1.7 Measurable Objectives

Identifying measurable objectives and clarifying the purpose for the consortium was added to the list of factors after review by the members of the consortium. There is a need to have a means for identifying milestones or objectives that are observable and reportable to maintain the course and to provide support and justification to stakeholders and members. A consortium member said of this, "… you have to show where you're going to benefit yourself and the other party…." Another member said of the person initiating the idea of the consortium that he "had vision." The literature on collaboration in business and government supports this. Clear objectives and other things such as an identifiable vision for what is to be accomplished and having standards or models to compare against also seem to be valuable to supporting ongoing collaborative activity:

> "Each of us spend the majority of our day taking care of ourselves, but we get together from time to time to make sure that we can learn a lesson from the other and to make sure that the vision of all this is going to work and the end remains intact."

In the case of public safety and emergency response, there are models for improving interoperability, such as SAFECOM that can be followed (SAFECOM, 2011). A large technology vendor was asked if using the SAFECOM model in development of governance and communication policies and practices would lead to long term relationships amongst the counties and the respondent administrator said that:

> "In a limited way, yes. I believe it (SAFECOM) is one of many tools to maintain long-term relationships. However, I think having common financial interests and common technology may do more for building long term consortium relationships."

Other objectives come about through mandates such as P25 or Narrowbanding, as discussed in the earlier sections. Some examples from this investigation are included below.

> “There were three things, September 11th, and the need to be interoperable, that was huge, you know, the basic is that you need to be able to talk to whoever you need to talk to when you need to talk to. So interoperability, narrow banding was a factor, and the fact that our legacy systems were obsolete or impractical. Impractical being low band VHF that fire service was using. You know, the amount of equipment being manufactured for low band is disappearing, the noise, the appearance, the size of the antennas, there’s a lot of things that render that an impractical alternative.”

> “The narrow banding is going to happen, it’s going to happen on January 1st, 2013.”

Regulation and existing policy allowed for clarity or purpose and provided guidance for implementing new ways of operating. This is shown in a statement from a 911 administrator:

> “We basically took existing radio policies and rather than reinvent the wheel we said lets adapt our existing policy which people are used to, cause we had a 911 system, we had policies and procedures, let’s adapt those to meet our new system, you know; so we’re going to have to change some things to meet the new system but basically people already know how to operate in terms of policies and procedures, who talks when and that kind of thing, and we included them in writing the policies. Okay, you know, the fire chief’s radio committee have several members sit on the, actually chair, the committee deciding

on the policies for fire communications. Police chief, same thing, on the police talk groups."

7.1.8 Technical Standards

Clearly, having identified technical standards allows for greater interoperability and it also provides, in some cases, a more stable base for cooperative ventures such as consortium's for public safety. It was found that the emergence of standards for technology allowed for collective activity and consensus. Members of the consortium described and identified many instances of technology standards for hardware and policy in emergency response communication that helped them to work together to provide services and prepare for upcoming changes. Some of the relevant comments are provided below:

Q	It seemed like everybody is floundering until someone stepped up and put some standards out there.

Resp	Yeah.

Q	So that I think that even that raw set, you know, that very rough outline of standards gave people a way to come together, otherwise you know, it's just every man for themselves.

Resp	Right, right. And that's something where we're really starting to get a hold of now, you know, I'd like to see that statement you just made in writing.

Resp	There's standards, you don't get that little part of the pie if you don't comply.

Regarding commercial purchasing or choice in technology solutions standards allowed, the consortium to consider greater interoperable technology options as a group. According to those interviewed, technical standards forced a degree of interoperability on the market and allowed cooperative planning by groups such as the consortium:

Q So that’s better for the end users because now there’s more choice.

Resp Sure, now they have a choice.

Q So some of that before was based on lock in, if XXX had you buying XXX stuff you were likely to be stuck buying XXX stuff forever.

Resp You’re right, if you had a YYY trunk system, you only bought YYY ... if you bought a YYY trunk system, you could only buy YYY subscribers to talk on that system. If you had a XXX deck system, you only could by a XXX deck radio to talk on the system. You couldn’t go buy a YYY and have it talk on that system. So that locked you in. Now, as systems are being built, you could build a YYY infrastructure and have ZZZ radios talking on it or ...

Things such as technical standards are good candidates for higher-level government or organizational control and guidance. Sovereignty and control are recurrent concerns among those observed in this study. They expressed fears over federal mandates or state direction and control without consideration of local interests. They do, however, express acceptance of a role for State or Federal levels of government in the area of broad technology policy and standards adoption and enforcement. This would include standards setting bodies such as IEEE (Institute of Electrical and Electronics Engineers) or APCO (Association of Public-Safety Communications

Officials – International) as well. In the words of one local member, “be the standard bearer” and provide the overall guidance and standards so that the commercial vendors and local providers can progress. There is an acknowledgement that standard setting is a good thing and that it is best done at the higher levels.

> “Yeah, we’ll probably be saying LTE and broadband spectrum and, you know, if the federal government gets its way with the development and build out of 700, 800 spectrum for LTE network this will be a public safety, there will be a public safety grade device that looks very similar to this that does everything.”

> “there’s standards that need to be in place so that all of that is serviceable and manageable and you don’t have a lot of proprietary technology that’s in the middle of it that becomes costly and difficult to service and maintain. So the standards need to be built to talk, to merge the two very distinct to spare technologies between public safety, P-25 infrastructure and LTE 4 GE, 3 GE, whatever that happens to be.”

> “I think P-25 is critical, in order to bring this to the masses affordably and, again, I use my voice over IP. When voice over IP was first adopted, you had an awful lot of companies, the big guys, the XXX’s the YYY and ZZZ’s that had their own proprietary communication between their core server and the actual telephone instrument.”

> “Once the industry drove that technology to what’s called SIP, which is an industry standard you can now purchase a telephone that will work that’s agnostic, doesn’t care

> whether that XXX, YYY, ZZZ, if P-25 if it's truly going to work and drive the cost of that subscriber radio down and commoditize it which from where I sit is good and bad because there's an awful lot of revenue that's generated by the XXX's of the world selling radios and the YYY's and if you commoditize that then, obviously, there's, you know, it would hurt a company like XXX, but as a consumer, as a taxpayer it's important that P-25 is a standard that that radio becomes agnostic whether that's ZZZ infrastructure like it is in X County A, County B went ZZZ or whether it's YYY infrastructure it really should be interoperable."

There are also problems with current technology standards and regulations that limit interfere with how agencies may interoperate. Outdated regulatory structures do not reflect the multi-jurisdictional complexity of current public safety emergency response operating environments. An example described here involves limitations on flexibility for spectrum licensing and use:

> "Yeah, so we decided that hey, you know, the door is open if you want to come and play you can come and play, we'll get interoperability with you somehow. But they all agree to go with a 450 system whether they're trunked or conventional, okay. Most of them have a trunk system; some are using the conventional mode for a number of different reasons in their own county. That's their business, but right now we can, the hardest part right now is trying to find interop because you cannot license, we were unable to license frequencies on multiple counties because the FCC won't let you do that as of yet. So you can't get a licensed frequency to cover three different areas, three different systems."

> "You cannot license; right now we have been unable to license a frequency to go to multiple counties because they're licensed to agencies. So I have a frequency licensed to me, I can't license it to them, okay, that type of thing."

In other ways new technologies are enabling cooperation in ways that was not before possible amongst partner agencies. This is evidenced in the standards for fiber connectivity and microwave transmission used to link partners. A 911 administrator put it this way:

> "Well, I mean, part of the things that we can do in communications we couldn't do until we had fiber op, you know, fiber in the microwave that's out here and the linking that we're doing between the counties is really the key to this, you know, because we didn't have that kind of data with them and the pipe wasn't big enough to carry what we needed to carry."

Standards and technology capability play a critical role in the ability of agencies to come together as cooperatives or through organization such as the CNYICC.

7.1.9 Share control, all are important

Members of the consortium unanimously voiced their opinion that control issues were significant in this environment. They explain that creating and maintaining a sense that each entity has a degree of control in the process, which they can accept, and especially over their own resources and area of responsibility was paramount to their acceptance of the consortium and its direction. A finding in this study includes that participants must share control, governance, and that each one is considered important. The structure and operation of the consortium must reflect this in structure and operation. A firm recommendation coming from the respondents is to not have the largest, or most apparently influential, party being in charge. Players in this arena are especially committed to their roles and responsibilities and have a sense that if something will negatively impact safety or their ability to do their job, be it personnel, policy, or technology, they will quickly dismiss it. One administrator put it as:

> “We want them to control their own system; we’re just sharing resources. They have a say in how the system operates and that was the safety really.

The participants and stakeholders have a strong sense of sovereignty and are sensitive to mandates or external party’s demands. In this environment, it was important to acknowledge this and constantly and consistently reiterate the message that each would maintain individual control while participating in the larger group. Along these lines, the consortium purposefully saw that the largest county was not the one to chair the committee because of the inherent appearance that they would take charge and be controlling. This is reflected through one of the administrators:

> Resp … we had said “you know what, for the greater good of this fledgling organization that we have here let’s pick one of the lesser counties to be the head of this so it doesn’t look like it’s an XXX County initiative.”
>
> Q Very purposely.
>
> Resp Yes, very purposely we decided…

> "Yeah, … without the government stakeholder buying into it, you don't have the backing to go forward here, you really don't, you need that backing. So that's a huge stakeholder and unless you get all the emergency services to some degree or another singing from the same sheet of music you can't build 30 or 50 or 100 different systems for 100 different kingdoms, you got to build one system that's going to be that everybody in all their kingdoms can live with and feel like they have a say-so in it, you know; it can't be just we're going to dictate these things. So governance was an important thing. Again, that governance thing, you're going to have a seat at the table when we decide who gets what talk group, something the state couldn't promise us, we could promise our stakeholders, you'll have a seat, you'll have input."

One of the benefits of the consortium was to allow for a combined collective voice in contract negotiations and purchases with vendors for services. Even here, the need to maintain individual identity and control were considered. Collective purchasing while maintaining individual interests and needs is shown in the following statements from a staff member:

> Resp … now if we pool our resources, if one fire department, now we have twelve, XXX has 54, last I heard. If one fire department wants to go out and buy a thousand feet of hose, they're going to get one price for it. If twelve fire departments each want to buy a thousand feet of hose, they can get a better price

for it. They buy it jointly as a co-op. We do the same thing with your radio resources.

Q But does that, do you get constrained by that or does this leave you guys with freedom?

Resp Just because you buy it at co-op, nothing else is controlling you.

The authority and power of the consortium here is derived from the consent of the participants and stakeholders. They take measures to actively convey this message in an ongoing way. The understanding was well described by one of the staff members:

> "XXX doesn't sit there and say 'okay the consortium has decided,' what he'll say is 'we were talking with some of the other counties and an idea hit the table and this is what it is and what do you guys think about it.' So you always make sure it goes back down to a county level as YYY did, as ZZZ does today. It really comes back down to the independent counties are still making the decisions; some of the ideas are the consortium."

7.1.10 Use consultants for knowledge and insights

The use of independent sources of research and information by the members of the consortium was said to be important to effective decision making and data collection. Use of external consultants can provide a sense of empowerment to organizations (Kaarst-Brown, 1999). Members of the consortium report that they conducted their own research in addition to including insights and knowledge from paid consultants, vendors and consultants working in an unpaid capacity, and through university researchers. They sought out information and insight from a variety of sources.

> "… they (Independent Consultants) were vendor agnostic so they didn't care, they didn't care if it was XXX, YYY, or whatever the system was, they went into it without bias. That's what the … (independent consultants) … that's what they brought to the table was that the county department heads could go back to them and say listen, if I tell them I want this, it's not going to carry as much weight. You do the research, take look at what our best options are, and bring all of our options to the table, that's where a consultant is always good."

> "… there's a certain role here that it's always easier for us a servicer to sit down with our end user and discuss ideas, discuss system designs."

There is also a recognition that consultants are gaining more than the financial remuneration, for those that are paid, through their participation in the process. This information came from one of the administrators in the consortium:

> "When it came to consultants, you know, there's also another side of this to where the consultant wants to come in and sit down with the servicer so that they can educate themselves on the system so that they can appear educated out in front of their customers. And again, I don't mean that in a derogatory sense, but we at that point start looking out for our own livelihood and saying alright what's the return on this, making sure that the

consultants understand the advantage of doing business with us over doing business with someone else."

Among the commercial vendors it was found that they network and share information even though they are in competition with each other in some areas. This is revealed in interviews with some of the vendors:

Resp Yeah, I guess that was a, they trust me a little bit more. And the nice thing is, even though it's competition amongst the shops, we do quite often talk amongst ourselves to solve the problems for the ... (Communications Project)

Q Common problems

Resp Common problems. You know, XXX at Company A, we are in constant contact with and YYY at Company B, whenever I have an issue that I need to talk to him about he would be my contact….

It was found that the degree of use of paid and unpaid consultants as well as the timing of their involvement with the process varied amongst the counties. There did not emerge a clear right or wrong way to do this. There does appear to be a change in the relationship at the point where a written contract is to be executed. Vendors participate as unpaid consultants through affiliation with the counties in related projects and at the point where the vendor may be engaged more directly in work that is part of a formal project that will be under contract it becomes more of a professional and formalized relationship.

In other cases, counties have informal relationships with University researchers who provide research support as well. Technical and policy expertise can be accessed in this way through formal and informal means. At least one of the CNYICC counties was engaging informally with a local university (Syracuse University) for such support and included assistance with grant opportunities; they credit having this support for their being awarded nearly $3 million dollars through recent competitive funding requests.

The themes identified above have significance based on the rank order that was created by the core member participants. It is important, however, to note that they are not to be considered independently but work in combination. The researchers have not quantitatively assessed the frequency of the remarks by category. Researchers did find evidence of the identified factors present in all of the core member interviews, the common themes being mentioned by everyone.

7.2 What does not work to facilitate collaboration

This article first considered ten factors identified by the participants as being important to the initiation, formation and ongoing operation of the CNYICC. Information from 911 administrators, staff, and related government and private stakeholders was included. This section briefly describes factors that were identified as working against collaboration in this environment. This is related to the 2nd research question and results stem from analysis of the interviews and data collected.

The factors were rank ordered by the participants for their significance as follows: 1) lack of shared standards; 2) decisions being dictated from the top as in the top-down bureaucracy of county governments; 3) the assumption that everything will work everywhere, insisting that participants follow the same course even when structural and political frames of each county differ; 4) management by memo or indirect communication; 5) looking out just one’s own interests; and 6) overly strict and detailed governance plans.

Many of these factors were addressed in the context of the earlier discussion of positive factors, so that information will not be repeated here. This section provides further discussion on some of the findings regarding those factors that were identified as working against collaboration and connect them with other research and literature.

The lack of explicit standards and the existence of conflicting or ambiguous standards have been identified as a cause of early and persistent incompatibility problems in public safety. This was echoed by the interviewees in the preceding sections. Organizations in public safety still use hardware and software of varying types. Integration of heterogeneous platforms, non-standard data, and proprietary schemas impede collaborative use and sharing (Atabakhsh, Larson, Petersen, Violette, & Chen, 2004; Fedorowicz, Gogan, & Williams, 2007). Having standards can make it possible for companies to make universally compatible systems. This would lead to greater availability for these products and cheaper pricing due to increased demand. According to some of those interviewed, companies still create proprietary features in communications products that hinder full compatibility. The instance was described where certain radio brands met the P25 standard but included additional features such as greater encryption capability. In that case– to be able to use a feature that was beyond the standard or communication with others who have that capability– you must purchase that particular type of radio and the feature. It is a similar case with upgrades for software. Agencies with interoperable software systems may lose compatibility if they do not all pursue the same upgrade paths over time. Technological standards promote collaboration but the benefits can be limited as has been shown in this case and other studies of public safety agencies (Lee & Rao, 2007).

Among public safety agencies, there is a great sense of personal identity and sovereignty; their staff members express a direct sense of responsibility to their constituents and stakeholders. It was evident in this study that a strategy of top-down bureaucracy, or dictating from the top in working with county and local governments, was not well accepted where local-level participants were not made to feel part of the process, that their interests were being considered, or that they had adequate power in the process. This is also reflected in the literature on leadership. Leadership that is innovative and having leaders exercise the proper amount of authority lead to greater sustainability in collaborations in studies that included state level justice agencies (Dawes, Cresswell, & Pardo, 2009). Other work found that organizational autonomy influence by managers within the particular agency mattered to a greater degree than management or political leadership from outside the agency (Vann, 2005). The respondents in the case study here reflected these sentiments and added that each agency also has their preferred way of operating.

Agencies may have similar objectives but operate differently. One cannot assume in regards to technology, governance, and control that everything (or solution) will work the same everywhere. The CNYICC study confirmed this point. Different persons perceive situations from their own, or their agency, perspective and each interprets it differently (Alter, 1999). Even successful solutions do not work in the same way in all environments. Multiple paths can lead to a similarly successful end, and not all agencies will choose the same means. Brafman and Beckstrom describe successful governance systems that have distributed leadership and leaderless entities that account well for regional nuances (2008). One agency may require a higher standard for security than another or have different priorities for protection (Ivkovic & Shelley, 2005). There are great similarities across operations in the public safety arena, but there remain political, technical, social, and other factors that are so dissimilar that they must be accounted for individually.

Good interpersonal communication skills were identified as key to successful collaboration engagements in this case study and the literature (Yang & Maxwell, 2011). A sure-fire way for a joint activity to fail can be to manage it impersonally through memos or indirect communication. Collaboration is a contact sport and requires relationship building and personal attention. A respondent 911 administrator remarked "…people can interpret e-mails incorrectly, the tone of them, or the wording, some people aren't good writers and have trouble expressing themselves, electronic or on paper…" Evidence from the literature and this case study support the notion that impersonal and one-way communication should be used sparingly in this area.

Another way to diminish the enthusiasm and support of partners and stakeholders in a collaborative venture is to look out for just one's own interests. In the case of the CNYICC, numerous positive remarks were made regarding the selflessness of those involved and their efforts in looking out for the greater interests of all. The agency problem or principal-agency problem is a concern among even public safety personnel and entities. This involves conflicts that arise where those responsible for looking to the interests of others use their power or positions for their own interests ahead of those they are to serve (Gailmard, 2010; Miller, 2005). For these reasons, oversight or control mechanisms may be necessary to mitigate such self-interest (Eisenhardt, 1989). Such principal-agent role conflicts can impair fair and effective management of public safety resources. In public safety especially command personnel depend on agents who may not directly report to them and the interests of those agents may conflict with those of the command personnel (Rauchhaus, 2009). Agencies can use measures such as monitoring, incentives, punishment, and the like to foster compliance. Providing for effective accountability and control mechanisms that allow autonomy for participating agencies remain difficult issues to be addressed in the law enforcement and emergency response context. The appearance of self-interest, beyond looking out for one's agency, citizens, and stakeholders interests was seen as having a negative for collaboration according to all members of the consortium.

Having strict and detailed governance plans was found not to be necessary for building trustworthy working relationships in this study. Bardach (2001) found that collaboration may be effectively governed informally. In the case of the CNYICC, members have yet to complete their written policy and procedures for governance and operation. The wording of the original MOU was broad and continues to be controlling. Consortium participants state that the CNYICC operates better by depending on the personal commitment of the members over a detailed written contract; they depend upon each other and their personal commitment and trust to bind them together. Individual personal commitment is largely responsible for the success of this collaboration and not the paper. One cannot, however, draw the inference that formalization of policy and procedure in collaborations is not needed. Cash and Konsynski (1985) showed that established infrastructure in support of information exchange and communication was good for collaboration. The experience of the CNYICC is still young by other organizational standards. The case study points to the need to allow for flexibility and some informality in the development and early stages of formation and growth. Participants stated that for longer term mature operation the need for greater formalization does arise. Research by Sales (2010) suggests that formalization of policy will have a positive effect on the organization and improve information sharing. This important related finding will be examined further in the discussion section.

8. Discussion

This section discussed the assessment of success factors relative to the CNYICC and other issues that this case study may address or contribute to understanding collaboration and information sharing in the public safety sector. This research sought to identify factors that foster and hinder public safety collaboration. An inductive approach was taken and recommendations derived from practitioners in the field were gathered and empirically assessed, analyzed and presented. The participants believe that this collaboration has been successful. A public sector collaboration success assessment model is used to consider the CNYICC and the recommendations that are derived from the case study. Further discussion on social, technical and policy related matters, as those factors have been identified in the information sharing framework (Treglia & Park, 2009) that were developed from this case study is provided as well.

8.1 Success Model and Assessment

Alternate models for collaboration success were sought out as a means to test the recommendations from respondents in the case study of the CNYICC, to consider the success of the CNYICC, and to triangulate results. The previous section presented the findings and discussed each of the ten specific factors that were identified by the study participants as helping to achieve or improve collaboration as well as the seven factors that work against success in collaborations and by extension information sharing and cooperation. The factors that support collaboration, in the words of the respondents are: In it for right reasons or the greater good, Trust, Personal characteristics of key managers and people oriented focus, Face to face and regular contact with partners and stakeholders, Autonomy and flexibility for participants, Basic written agreement/understanding (flexible, not complex or detailed), Measurable Objectives, Technical Standards, Share control (all are important, i.e. don't have biggest partner in charge), and Use consultants for knowledge and insights. The factors they identified as working against collaboration were: Lack of standards, Dictate from the top or top-down bureaucracy in County Governments, Assume that everything will work everywhere or insist participants follow the same course, Manage by memo or indirect communication, Look out just your own interests, and Strict and detailed governance plans. It is but a single case study, however, it is one that is representative of many other public safety communications collaborations occurring across the United States

Kuenzel and Welscher propose an alternate model positing that there are eight factors important to ‘Public Safety Collaboration Success’ (2009). The success factors serve as an essential frame-work for assessing public safety collaboration processes. These factors are: 1. Relevance and Sense of Urgency; 2. Incentives and Benefits; 3. People & Roles; 4. Organizational Structure; 5. Reflection & Learning: 6. Skills and Capabilities; 7. Resources; and 8. Outside Support & Supervision. They suggest that the eight identified success factors must be present or made part of the design and operation of a collaboration to have the highest probability of achieving its desired public safety objectives (Kuenzel & Welscher, 2009). This section takes the eight factors and groups them for analysis into the categories of social, technical and policy using the information sharing factor framework (Treglia & Park, 2009). The success of the CNYICC is assessed in this way. By using this process the CNYICC case study data may also be more readily compared to extant literature on other collaborations in public safety that may use this same tool. The table below shows the grouping of the factor correlations, see Table 8 below.

Information Sharing Framework (Treglia & Park, 2009)	**Public Sector Success Factors (Kuenzel & Welscher, 2009)**
Social	
Criticality	Relevance and Sense of Urgency
Trust	Incentives and Benefits
Culture	People & Roles
Informal Network	Reflection and Learning
Quality	Skills and Capabilities
Technical	
Interoperability	Resources
Availability	
Control	
Policy	
Regulation and Legislation	Organizational Structure
Governance	Outside Support and Supervision
Levels	
Jurisdiction	
Financial	
Organizational Capability	

Table 8: Information Sharing Framework and Assessment Factors

The social category from the information sharing framework contains issues of criticality, informal networks and culture. Using this schema the Relevance and sense of urgency, incentives and benefits, people & roles, reflection and learning, skills and capabilities, from the public sector success factors of Kuenzel and Welscher (2009) fit in the heading of Social in the framework. The technical category of the information sharing framework maps to resources in the Kuenzel and Welscher (2009) success factors list. The final information sharing category of policy is most related to public sector success factors of organizational structure, and outside support and supervision. In this way one may assess the success or lack thereof of the CNYICC according to that instrument.

The CNYICC is successful in the social aspects with respect to the public sector factors identified in Kuenzel and Welscher (2009). Socially the CNYICC formed and operates out of a sense of higher order interest and public purpose. The need for public safety and the urgency associated with the task of creating interoperable communications for emergency responders is a clear, important and galvanizing purpose. Activities of the consortium are directly relevant to this purpose and supported by local government officials and the public. Benefits to participation in this consortium are many as described in the findings section. The discussion on the objectives of professional associations is relevant to this view of the operation and motivation of the CNYICC and assessing it in terms of criticality or sense of urgency. Members of the CNYICC act collectively to benefit each other and their society based on the sense of urgency in preparing for opportunities and positioning themselves to create fiscal advantage, to avoid problems and to work for the greater good. Seeking funding opportunities and securing more advantageous arrangements with vendors for services is a stated purpose of the CNYICC and they have successfully secured funds and unified to influence vendor relationships and contracts.

The CNYICC is also successful in relation to skills and capabilities as well as reflection and learning. CNYICC members are observed to have high levels of interpersonal communication skill and leadership skill. They showed this in their actions by operating their meetings and agencies as learning organizations. They spoke of and were observed to lead and communicate in a “hands on” way and “face to face” where possible. Members of the CNYICC display fine leadership qualities. Members of the CMYICC put a great deal of time into their development of interpersonal relationships and trust within and across organisations.

The CNYICC is successful in procuring adequate resources for ongoing operation and growth as these are described by Kuenzel and Welscher (2009). CNYICC members have adequate fiscal and personnel resources to meet routinely, participate in conferences, meetings, lobbying and education outreach activities with the support provided through their agencies in support of their stated goals and objectives. This support resource that the participating agencies have provided includes things such as time, manpower, equipment, facilities, other supplies and communications support as needed. All of this has allowed for adequate participation and communication as a consortium.

Outside support and supervision, and organizational structure are success factors from Kuenzel and Welscher (2009) that are considered policy related. From this conceptual view the CNYICC was observed to react to perceived external policy and regulatory changes coming from state and federal levels (see Tables 6, p. 229 & 9, p. 331). In interviews with respondents there were mixed remarks, as identified in the previous sections, that evidence keen awareness of pending mandates such as narrowbanding yet they also explicitly state that pending regulation did not cause them to collaborate. CNYICC members report being supported by outside consultants, university researchers, and vendors in addition to their own agency personnel, see the previous findings section for specific examples and discussion on this topic. The 911 administrators reported that they have adequate authority and control within their agencies to effect necessary change. Governance structures are according to the members adequate for the time being. They report as well that they are all high enough in the hierarchy to effect policy, procedure and even cultural changes in their organizations. It is also valuable that the legislatures have chosen to give weight and influence to the CNYICC as there are no formal processes for enforcing mandates or recommendations from the CNYICC. This is not so say that dealing with local legislatures or other municipal management personnel is without conflict. The respondents report that it is manageable for them.

Organizations participating in the CNYICC participate and follow the guidance because they trust the CNYICC and choose to do so. This is so because it serves their higher and legitimate interests in the short and long term for service to the community and communications services. The primary controlling document is the broadly worded MOU for the establishment of the consortium. The draft documents outline operation and policy and procedures for the consortium are under development and have not been formalized. The consortium operates successfully in its governance as they have sought appropriations and funding and created policy and infrastructures within each respective jurisdiction that works for them and works in aggregate across the region.

Using the information sharing framework (Treglia & Park, 2009) of social, technical and policy factors researchers described and summarized the Kuenzel and Welscher (2009) success factors as they pertain to the CNYICC. The CNYICC is a successful collaboration as assessed by the eight public sector success factors described by Kuenzel and Welscher (2009).

8.2 Social Factors

Effective leadership is consistently recognized as an essential element to collaboration. Brafman and Beckstrom confirm that flexibility in leadership guided by a shared vision and goal are important aspects of successful governance and collaboration models (2008). Individual leadership characteristics were identified important to collaboration success in the

CNYICC study. The contribution of individual leadership characteristics in organizations have been studied by many (Zhang, Dawes, & Pardo, 2009; Parry, 2009). Internal leadership, that being from managers considered to be within the agency, matters more than external or outside political leadership (Vann, 2005). In line with this proposition members of the consortium seemed to extend their allegiance outward to the membership agencies. Those parties considered to be outsiders may move closer to the trusted circle by participating in a consortium or other recognized public safety affiliation.

Trust is considered in many ways in the CNYICC study and is a significant component for consideration in collaboration and information sharing transactions. Trust in face to face to face interaction can readily develop over time (McEvily & Tortoriello, 2011; Jeffries, 2002). In the case of the CNYICC respondents proclaimed the importance of face to face contact whenever possible with staff and stakeholders. Group identity, affiliation and norms develop from interactions within a community and from outside interactions and social contacts as well (Abbott, 1988; Cant & Sharma, 1995). It appears that in moving to virtual communication it was important to at least initially develop rapport and trust through face to face interaction. This is conclusion is supported by the work of (Zheng, Veinott, Nos, Olson, & Olson, 2002; Koufaris & Hampton-Sosa, 2004). Face to face, and regular contact with partners and stakeholders, which can be considered socialization, was a top factor for collaboration success as identified by CNYICC respondents. Socialization has been shown to support establishment of group identity and improve trust (Rocco, 1998).

An interesting aspect of trust relationship emergence based on prior relationships was observed in the CNYICC study. Participants in collaborative work need to develop a degree of trust in each other and their institutions to be successful in interacting and sharing information.

Respondents in the CNYICC study report that most did not have prior social contacts or relationships with the other members. They report having met each other and developed their trusted relationships through common association meetings and through participation the CNYICC itself. Respondents acknowledged that over time meetings and contacts had to be conducted virtually, by phone, due to logistical constraints.

An argument could be made that participants have a propensity to trust others and that this was a determining effect for their establishing trust relationships in the workplace. Self-reports from CNYICC respondents show that they considered themselves trusting of others generally. Research has been done that looked at aspects of establishing, maintaining and re-creating trust in working relationships (Zheng et al., 2002; Koufaris & Hampton-Sosa, 2004). These studies included a focus on the effects of pre-disposition to trust or propensity to trust on cooperation and engagement and have resulted in mixed results. There is evidence that found no support for a hypothesis that individual trust propensity leads to increased trust in collaborative encounters (Koufaris & Hampton-Sosa, 2004) and other evidence and findings to the contrary (Ridings, Gefen, & Arinze, 2002). Having a general disposition to trust others increased the degree of trust that persons in the study afforded to others in the study (Gefen, 2000). The studies described here involved virtual transactions as well. This is significant as the interaction of the CNYICC involves both face to face and virtual meetings and engagement.

8.3 Technical Factors

Technology impacted the actions of the members of the CNYICC and their agencies in many ways.

Technologically, respondents in the case study projected that use of multi-media such as video teleconferencing would likely support distributed collaboration in a positive way. They only accept voice communication for meetings as they have established prior personal contact and relationships. Research supports the proposition that image and video use to accompany communication virtually improves the communication experience almost to that of face-to-face (Ben-Ner & Puterman, 2002). The study by Zheng, Veinott, Bos, Olson and Olson (2002) conclude that "having a static photograph of the partner is as effective in establishing trust, whereas a text-based, static information sheet of personal information is not." This same study also confirms a finding that face-to-face meeting is the most effective form of interaction.

Technological implications on talk groups were an issue. Determining who can talk with whom and under what conditions was discussed as constrained by the technology. One example is in the case of talk groups and channels. The radio technology that is being used only allows for a certain number of channel positions. Based on brand and model radios may have 16 or 24 readily selectable positions, for example. The structure of the radio controls the range of decisions that can be made as to channel position, numbers and access (such as the number of channels or channel groups that can be selected by a particular style of radio). In this way the technology is dictating the way he that channels can be picked and limiting the number that there could be at any one time and also because of physical dial it means that you have deterred him from one position to the next. The most important channels need to be at the top or most readily accessible. As a responder you want to scroll up or down from the most used channel. If using a physical dial considerations such as size come in to play and one should turn left and right from the most used positions. It should also be noted that constraints such as having to do this while wearing heavy gloves or in conditions of black smoke impact what choices can be made.

Technological considerations such as these influence policy and practice decisions acutely in the public safety environment.

Although there are technical standards that help support collaboration there are other things that vendors do that work around this. It was identified in the study that having standards would help collaboration can help companies to make compatible systems that would make them cheaper in competition. An observed problem was that although P25 and other such requirements provide standards the company's still work around them to differentiate their products. A certain company can meet the basic standard but offer additional non-standard proprietary services or features that may not be supportable by competitors. One example of this is in encryption for talk groups. Radio companies can meet the standard for required channels and frequencies and then offer additional services such as a proprietary encryption capability. The problem that this creates is that now if the one agency needs to talk to another agency which has a radio from another manufacturer that agency cannot do so. Although having established and enforced standards in place promotes interoperability companies are still able to create exclusivity with add-ons or special features that go beyond the standards and ultimately impede interoperability. Participation by informed stakeholders in the legislative and regulatory processes can work to address issues such as these.

Investigation of the CNYICC brought to light additional technological concerns related to communication and information sharing. Things such as the number of characters possible or display size influence how radios are set up and what information may be available to users. Identifying channels for use can be problematic when there are limitations to the number and types of characters that can be used to identify a channel. Further problems using the technology can involve ontology or choices in naming or otherwise identifying channels used by various agencies. A recommendation that plain language be used is helpful but does not account for variations in terminology for those from different regions or professions. Universal terminology or graphic images may help. Having additional capacity to show more characters or to add graphic images may mitigate some of these issues.

8.4 Policy Factors

Policy associated with technology affects operational decisions for agencies as well. As an example ownership and use of licensed channels and frequencies creates legal conflicts over frequency channel use by emergency response agencies. Multiple jurisdictions may wish to use or operate on the same channels to share information and collaborate yet regulation can preclude such an arrangement. Respondents echoed concerns over communications regulation. The current structure in the United States for the licensing is FCC channels require a particular owner be identified and does not generally allow multiple-jurisdictions to share a frequency. This type of policy makes it hard to have shared ownership or use of radios across multiple jurisdictions, and includes issues crossing and overlapping state and international territory.

The case study for the CNYICC identified that flexible and informal governance structures facilitate collaboration in public safety during early developmental stages. Other researchers acknowledge that alternative governance and collaboration arrangements may improve success, participation and the sharing of information (Brafman & Beckstrom, 2008). This insight must be paired with the statements from CNYICC participants acknowledging that it is important to appreciate that "one size does not fit all" and that solutions must be suited to the particular context. In some cases early formal processes, such as a memorandum of understanding (MOU) or memorandum of agreement (MOA), may be necessary to secure commitment or provide assurance to partners that their interests will be met and that what is agreed upon is clearly understood and documented. Other collaborations, such as those involving less trusted partners, may need to allow more initial space and less pressure in the early and formative stages (Cook, Hardin, & Levi, 2007; Benamati, Serva, & Fuller, 2006). The comfort that comes with having explicit documented contracts may be achieved by having such flexibility built into the policies provisions and understandings that things can change as necessary. There is no universal recipe for the perfect degree of formalization other than to suggest that the process itself remain malleable and must not be rendered static.

The public safety network study identified maturity as an element for successful public safety networks (Williams, Fedorowicz, & Tomasino, 2010). Successful public safety networks in that study were identified as having characteristics of having been around for some years, showing a certain level of critical mass for participation, and having established funding sources resources to sustain themselves. The public safety network study included formalization of governance structures and standard operating procedures (SOPs) as elements relating to success.

The respondents (CNYICC) report that they see a need to be more formalized at some point in the future to meet possible government requirements related to funding or to have greater impact with vendor relationships and contracts. This is consistent with their correlation to professional associations as discussed previously. Professional associations formed to address these similar needs and interests. To speak with a greater voice to leverage, contract or service is shared by both.

Researchers do not at this point know what the one perfect combination of formal structure and flexible and informal structures is that produces the most effective collaboration arrangement over the long term. The CNYICC and cases in the public safety network study (Sawyer et al., 2007) show that both formalization and flexibility are important factors to collaboration. A limitation in the CNYICC study is that it has not yet been around long enough to be considered an example of mature or long term collaboration. Researchers here do not know exactly when the need changes from one focus to another in the evolution of the organization. Future research will focus on further investigating public safety collaborations over time to see which ones are surviving and under what conditions. Circumstances to be considered include observed changes in formal and informal structures, flexibility, and other issues. An important question to be pursued involves understanding what the optimal degree of formalization and flexibility is for an organization to be successful under various scenarios.

The case study of the CNYICC is ongoing and researchers will continue to observe activity over the long term.

9. Conclusions

The case study of the CNYICC provides important insights into human, technical, policy and other factors that influence or impact the formation of collaborations, their governance and the ways of dealing with technology implementation in the public safety communications arena.

This article provides a descriptive account of the CNYICC, its formation, development, and operation. This research has brought out, through interviews and observations, numerous factors that are believed to have helped this collaboration and factors believed to be a hindrance to such collaboration. This research examined the question of what elements comprise successful collaboration among disparate county government agencies in emergency response preparedness and activity. The researchers here found that this collaboration was pursued to provide better safety and services to the public, to save lives, to prepare for funding opportunities, to share information, to collectively speak to standards issues, and to collectively pool resources for leveraging influence on vendors for equipment and services contracts. This was found to be similar to the motivation and benefits sought out by professional associations generally. Higher-order interests were found to be a significant driving influence as reflected through the respondents in this study and as observed by researchers. This motivating factor is relatively specific to the public safety arena and differentiates the findings from collaborative activity in non-public safety oriented contexts.

An important contribution in this area comes in the form of describing and framing the broader factors surrounding information sharing and collaboration in the public safety area and in describing the environment and influences that operate across this community. The case is significant in that it is representative of the activities, needs, and concerns of other multi-jurisdictional law enforcement and emergency services providers across the nation.

There are unique features of New York State public safety entities and their environment that should be taken in to account when considering broader application of findings. It is a strength that the CNYICC faces challenges that make it representative of situations faced by other public safety collaborations across the country. New York State, however, is one of the most targeted states for terrorist activity. It has major metropolitan areas, international borders, and multiple layers of public safety entities. There are many parts of the country where public safety agencies face much less complexity and criticality. These aspects in New York State add to the comprehensiveness of the issues raised and understood through the study. As a case for comparison with other areas of the country and other less complex collaborations the lessons learned are argued to be still valid. The success factors identified still apply.

The importance of interoperable communications is well acknowledged today. There are federal and local mandates affecting law enforcement and emergency response agencies, driving them to change and implement interoperable technology and policies. Financially, economic drivers are pushing agencies towards standards-based interoperable equipment and software. Agencies across the nation and world are finding that they must work together to effectively protect the public and respond to ever-occurring local and large-scale crises. The lessons learned here regarding successful collaborations are useful and timely. Lessons learned from this case, although it is acknowledged that it is a single limited case in a given environment, have applications in other similar public safety environments.

This "generalizable knowledge" contributes to the theoretical framework for understanding information sharing, described previously, and adds to the established body of knowledge relative to factors influencing information sharing and collaboration. Some of the primary beneficiaries of this research are other researchers, scholars, government officials and legislators, and practitioners in the field of law enforcement and emergency response.

Publication, presentation, or other distribution of the results from this work will inform the field. Results are expected to be generalizable to a larger population beyond the site of data collection. The case study itself is relevant to understanding other similar coordination efforts in this community. Research results are intended to be applicable in other settings, obviating the need to constantly reinvestigate or start from the beginning each time something is done. Much of what law enforcement and emergency response personnel face is common across the field; thus, insight from this study will be relevant to other similar circumstances.

Future work in this area should focus on governance issues such as identifying the CNYICC, its formation, proper balance between formal and informal operation in public safety and other contexts. It will be important to create models that identify contexts or other events that may inform agency heads when more or less governance and what type and form of formalization may be needed to improve the success of collaborative endeavors.

Governance of collaborative action is an important area of concern that is addressed to a limited degree in this study. In regards to information sharing, governance is perhaps an undervalued aspect of the larger picture involving collaboration in public safety. The observations and recommendations identified in this dissertation arguable are applicable to environments such as the business, not-for profit sectors and even collaborative activities such as product development teams and in education. The findings regarding the need for promoting the appropriate degree of control, proper motivation and making use of interpersonal skills and practices is valuable guidance for virtual or face to face collaboration efforts by involved leaders.

Much work remains to be done to fully understand public safety collaboration and information sharing generally and as it applies to other geographic areas and types of organizing.

10. References

Abbott, A. (1988). *The system of professions: An essay on the division of expert labor.* University of Chicago Press.

Agranoff, R., & McGuire, M. (2001). American federalism and the search for models of management. *Public Administration Review*, 61(6), 671−682.

Allen, M., Balloni, J., Hartnett, P., & Stayton, D. (2007). Memorandum of Understanding (MOU) for the creation of the Central New York Interoperable Communications Consortium (CNYICC).

Alter, S. (1999). A general, yet useful theory of information systems. *Communications of the AIS*, 1(3es), 3.

Astley, W. G., & Van de Ven, A. H. (1983). Central perspectives and debates in organizational theory. *Administrative Science Quarterly* 28: 245–73.

Atabakhsh, H., Larson, C., Petersen, T., Violette, C., & Chen, H. (2004). Information sharing and collaboration policies within government agencies. *Lecture notes in computer science*, Vol. 3073/2004. (pp. 467-475)Springer: Berlin and Heidelberg.

Bardach, E. (2001). Developmental dynamics: Interagency collaboration as an emergent phenomenon. *Journal of Public Administration Research and Theory*, 11(2), 149−164.

Benamati, J., Serva, M. A., & Fuller, M. A. (2006). Are Trust and Distrust Distinct Constructs? An Empirical Study of the Effects of Trust and Distrust among Online Banking Users. *System Sciences, 2006. HICSS '06. Proceedings of the 39th Annual Hawaii International Conference on* (Vol. 6, p. 121b). Presented at the System Sciences, 2006. HICSS '06. Proceedings of the 39th Annual Hawaii International Conference on.

Ben-Ner, A., & Putterman, L. (2002). *Trust in the New Economy1 (HRRI Working Paper)* (p. 36). Minnesota, US: Industrial Relations Center, University of Minnesota.

Brafman, R., & Beckstrom, O. (2006). *The starfish and the spider: The unstoppable power of leaderless organizations*. Portfolio.

Cant, S., & Sharma, U. (1995). "The reluctant profession-homoeopathy and the search for legitimacy." *Work, employment & society* 9(4):743.

Cash, J. I., Jr., & Konsynski, B. R. (1985). IS redraws competitive boundaries. *Harvard Business Review*, 134−142.March–April.

Charlton, J. R. H. (2004). "Delphi Technique." *In The Sage encyclopedia of social science research methods*, edited by Michael S. Lewis, Alan Bryman, and Tim Futing Liao. Thousand Oaks Calif.: SAGE.

Collins, R. (1979). *The Credential society: An historical sociology of education and stratification.* Academic Press (New York).

Cook, K. S., Hardin, R., & Levi, M. (2007). *Cooperation Without Trust?* Russell Sage Foundation Publications.

Dawes, S. S., Cresswell, A. M., & Pardo, Theresa A. (2009). From "need to know" to "need to share”: Tangled problems, information boundaries, and the building of public sector knowledge networks. *Public Administration Review*, 69(3), 392-402. doi:10.1111/j.1540-6210.2009.01987_2.x

Delbecq, A. L., Van de Ven, A. H., & Gustafson, D. H. (1975). *Group techniques for program planning*. Glenview, IL: Scott, Foresman, and Co.

Diesing, P. (1992). *How Does Social Science Work?: Reflections on Practice* (p. 432). University of Pittsburgh Press.

Dezalay, Y., & Garth, B. (1996). “Fussing about the forum: Categories and definitions as stakes in a professional competition.” *Law & Social Inquiry* 21(2):285-312.

DHS NECP. (2011). U.S. Department of Homeland Security, National Emergency Communications Plan. Website (retrieved 12/26/2011) http://www.dhs.gov/xnews/releases/pr_1217529182375.shtm

DiMaggio, P. J., & Powell, W. W. (1983). “The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields.” *American Sociological Review* 48(2):147-160.

Douglas, James (1987), " Political Theories of Nonprofit Organizations." In The Nonprofit Sector, edited by Walter W. Powell. New Haven and London: Yale University Press.

DuFour, R., & Eaker, R. (1998). *Professional learning communities at work: Best practices for enhancing student achievement*. Bloomington.

Eisenhardt, K. M. (1989). Agency theory: An assessment and review. *Academy of management review*, 57–74.

FCC. (2011). “Narrowbanding.” Federal Communications Commission - Public Safety and Homeland Security Bureau. Retrieved November 28, 2011 (http://transition.fcc.gov/pshs/public-safety-spectrum/narrowbanding.html).

Fedorowicz, J., Gogan, J. L., & Williams, C. B. (2006). The challenge of interagency integration: Lessons learned in five eGovernment cases. Washington, DC: *IBM Center for the Business of Government Monograph*.

Fedorowicz, J., Gogan, J. L., & Williams, C. B. (2007). A collaborative network for first responders: Lessons from the CapWIN case. *Government Information Quarterly*, 24 (4), 785-807.

FEMA NIMS. (2011). U.S. Federal Emergency Management Agency, National Incident Management System (NIMS). Website (Retrieved 12/26/2011) http://www.fema.gov/emergency/nims/AboutNIMS.shtm

FEMA. (2011). U.S. Federal Emergency Management Agency (FEMA). Website (Retrieved 12/26/2011) http://www.fema.gov

Freidson, E. (1988). *Professional powers: A study of the institutionalization of formal knowledge.* University of Chicago Press.

Gailmard, S. (2010). Politics, Principal–Agent Problems, and Public Service Motivation. *International Public Management Journal*, 13(1), 35–45.

Gefen, D. (2000). E-commerce: the role of familiarity and trust. Omega 28 (6), 725–737

Greenwood, R., Suddaby R., & Hinings, C. R. (2002). "Theorizing change: The role of professional associations in the transformation of institutionalized fields." *Academy of management journal* 58-80.

Halliday, T. C. (1987). Beyond monopoly: lawyers, state crises, and professional empowerment. University of Chicago Press.

Ivkovic, S. K., & Shelley, T. O. (2005). The Bosnian police and police integrity: A continuing story. European Journal of Criminology, 2(4), 428-464. doi:10.1177/1477370805056057.

Jeffries, F. L. (2002). Subjective Norms, Dispositional Trust, and Initial Trust Development. *Journal of Behavioral and Applied Management*, *3*(2), 129 – 139.

Kaarst-Brown, M. L. (1999). Five symbolic roles of the external consultant–integrating change, power and symbolism. *Journal of Organizational Change Management*, 12(6), 540–561.

Kaarst-Brown, M. L., & Robey, D. (1999). More on myth, magic and metaphor: Cultural insights into the management of information technology in organizations. *Information Technology & People*, 12(2), 192–218.

Kingdon, J. W. (1997). *Agendas, Alternatives, and Public Policies*. 2nd ed. Pearson Education.

Kothari, A., MacLean, L., Edwards, N., & Hobbs, A. (2011). Indicators at the interface: managing policymaker-researcher collaboration. *Knowledge Management Research & Practice*, *9*, 203–214. doi:10.1057/kmrp.2011.16

Koufaris, M., & Hampton-Sosa, W. (2004). The development of initial trust in an online company by new customers. *Inf. Manage*., 41(3), 377–397.

Kuenzel, E., & Welscher, H. (2009). "Management Model for Successful Collaboration in the Public Sector." [Managing Collaboration] *Federal Ministry for Economic Cooperation and Development.*

Lax, D. A., & Sebenius, J. K. (1986). *The manager as negotiator: Bargaining for cooperation and competitive gain*. New York: Free Press.

Lee, J., & Rao, H. R. (2007). Exploring the causes and effects of inter-agency information sharing systems adoption in the anti/counter-terrorism and disaster management domains. *In Proceedings of the 8th annual international conference on Digital government research: bridging disciplines & domains* (pp. 155-163). Philadelphia, Pennsylvania: Digital Government Research Center.

Lewin, K. (1951), *Field Theory in Social Science*, Harper and Row, New York, NY.

Lipnack, J., & Stamps, J. (1994). The age of the network: organizing principles for the 21st century. John Wiley & Sons Inc.

Mayberry-Stewart, D. (2008). 2008 *New York State Statewide Wireless Network Annual Report*. Retrieved from http://www.cio.ny.gov/assets/documents/RevisedSWNAnnulaReport3.pdf

McEvily, B., & Tortoriello, M. (2011). Measuring trust in organisational research: Review and recommendations. *Journal of Trust Research*, *1*(1), 23–63. doi:10.1080/21515581.2011.552424

McKenna, C. (2009). *NY Statewide Wireless Interoperable Communication Network Refocused on Regional Systems*. Retrieved from http://www.govtech.com/public-safety/99355764.html

Miller, G. J. (2005). The political Evolution of Principal-Agent Models. *Annual Review of Political Science*, 8(1): 203-225.

Milward, H. B., & Provan, K. G. (2006). A manager's guide to choosing and using collaborative networks. *Report published by the IBM Center for the Business of Government*, Washington, DC.

Montgomery, D. (1987). *The Fall of the House of Labor: The Workplace, the State, and American Labor Activism,* 1865-1920. Cambridge: Cambridge University Press.

Moynihan. (2005). Leveraging collaborative networks in infrequent emergency situations. *Report published by the IBM Center for the Business of Government*. Washington, DC.

NENA. (2009). *"What is NG911?"* Retrieved November 28, 2011 (http://www.ems1.com/ems-products/communications/articles/588619-What-is-NG911/).

NYS DHSES. (2011). SCIP 2010 - *Statewide Communications Interoperability Plan Update Year 2010. Albany, NY: New York State Department of Homeland Security and Emergency Services* Retrieved November 28, 2011 (www.dhses.ny.gov/oiec/documents/NewYorkSCIP2010.pdf).

OSC. (2006). *Office of the State Comptroller. Statewide Wireless Network - Briefing Document for State Officials. Albany, NY: Office of State Comptroller* Retrieved (http://www.osc.state.ny.us).

Ostrom, E. (1990). Governing the commons: The evolution of institutions for collective action. Cambridge, England: Cambridge Univ. Press.

Ostrom, E. (2003). Toward a behavioral theory linking, trust, reciprocity, and reputation. In E. Ostrom & J. Walker (Eds.), *Trust and reciprocity: Interdisciplinary lessons from experimental research* (pp. 19-79). NY: Russell Sage Foundation.

Ostrom, E. (2009). What is social capital? *Social capital: Reaching out, reaching in* (pp. 17–38). Northampton, MA, US: Edward Elgar Publishing.

Ostrom, E., & Walker, J. (2003). In E. Ostrom and J. Walker (Eds.), Introduction. *Trust and reciprocity: Interdisciplinary lessons from experimental research* (pp. 3-18). New York: Russell Sage Foundation.

Ostrom, E., & Walker, J. (2005). *Trust and Reciprocity: Interdisciplinary Lessons from Experimental Research*. Russell Sage Foundation.

Parry, K. W. (1999). Enhancing adaptability: leadership strategies to accommodate change in local government settings. *Journal of Organizational Change Management*, *12*(2), 134–157. doi:10.1108/09534819910263677

Peha, J. M. (2005). "Protecting Public Safety With Better Communications Systems," *IEEE*

Communications, March.

Powell, W. W., & DiMaggio, P. J. (1991). *The new institutionalism in organizational analysis.* University of Chicago Press.

Powell, W.W., & Steinberg, R. (2006). *The nonprofit sector: a research handbook*. Yale University Press.

Provan, K. G., & Milward, H. B. (2001). Do networks really work? A framework for evaluating public-sector organizational networks. *Public Administration Review*, 61(4), 414−424.

PSCR. (2011). “The Public Safety Communications Research Program.” Retrieved December 23, 2011 (http://www.pscr.gov/projects/lmr/p25_stds_dev/p25_stds_dev.php).

RadioReference.com. (2011). “Narrowbanding - The RadioReference Wiki.” Radio Reference - Narrowbanding. Retrieved November 28, 2011 (http://wiki.radioreference.com/index.php/Refarming).

Rauchhaus, R. W. (2009). Principal-Agent Problems in Humanitarian Intervention: Moral Hazards, Adverse Selection, and the Commitment Dilemma. *International Studies Quarterly*, 53(4), 871–884. doi:10.1111/j.1468-2478.2009.00560.x

Razavi, M. N., & Iverson, L. (2006). A grounded theory of information sharing behavior in a personal learning space. *In Proceedings of the 2006 20th anniversary conference on Computer supported cooperative work* (pp. 459-468). Banff, Alberta, Canada: ACM. doi: 10.1145/1180875.1180946.

Ridings, C. M., Gefen, D., & Arinze, B. (2002). Some antecedents and effects of trust in virtual communities. *The Journal of Strategic Information Systems*, 11(3-4), 271–295.

Rocco, E. (1998). Trust breaks down in electronic contexts but can be repaired by some initial face-to-face contact (pp. 496–502). Los Angeles, California, United States: *ACM* Press/Addison-Wesley Publishing Co.

Ruef, M., & Scott, W. R. (1998). “A multidimensional model of organizational legitimacy: Hospital survival in changing institutional environments.” *Administrative Science Quarterly,* pp. 877-904.

SAFECOM. (2011). U.S. Federal Emergency Management Agency, *SAFECOM Program,* www.safecomprogram.gov/default.aspx

Sawyer, S., & Fedorowicz, J. (2012). Designing Collaborative Networks: Lessons Learned from Public Safety. *IBM Center for The Business of Government - Collaborating Across Boundaries Series*.

Sawyer, S., Fedorowicz, J., Tyworth, M., Markus, M. L., & Williams, C. B. (2007). A taxonomy for public safety networks. *Proceedings of the 8th annual international conference on Digital government research: bridging disciplines & domains* (pp. 240–241). Digital Government Society of North America.

Sawyer, S., & Rosenbaum, H. (2000). Social informatics in the information sciences: Current activities and emerging directions. *Informing Science, 3*(2), 89–89.

Sawyer, S., Schrier, R., Fedorowicz, J., Dias, M., Williams, C., & Tyworth, M. (2012).

Architectural patterns of US public safety networks: a fuzzy set qualitative comparison analysis. *Proceedings of the 13th Annual International Conference on Digital Government Research* (pp. 49–57). ACM.

Scott, W. R, & Backman, E. V. (1990). "Institutional theory and the medical care sector." *Innovations in health care delivery: Insights for organization theory* 20:52.

Thomson, A. M. (1999). AmeriCorps organizational networks: Six case studies of Indiana AmeriCorps programs. National Service Fellows Program. *Report for the Corporation for National Service*, Washington, DC: Corporation for National and Community Service.

Thomson, A. M, Perry, J. L., & Miller, T. K. (2009). "Conceptualizing and measuring collaboration." Journal of Public Administration Research and Theory 19(1):23-56.

Thompson, E. D., & Kaarst-Brown, M. L. (2005). Sensitive information: A review and research agenda. *Journal of the American Society for Information Science and Technology*, 56(3), 245–257.

Thompson, A. M., Perry, J. L., & Miller, T. K. (2008). Linking Collaboration Processes and Outcomes; Foundation for Advancing Empirical Theory. *In: Big Ideas in Collaborative Public Management.* Edited by Lisa Blomgren Bingham and Rosemary O' Leary. Armonk, N.Y: M.E. Sharpe Inc.

Tolbert, P. S, & Zucker, L. G. (1999). "The institutionalization of institutional theory." *Studying Organization: Theory & Method* 169-184.

Treglia, J. (2008). "Two Cans on a String: Technical Social & Legal Barriers to Effective Information Sharing Among Federal, Tribal, State & Local Law Enforcement Agencies in the United States." *Poster in proceedings of iConference 2009 - iSociety: Research, Education, Engagement*. University of North Carolina at Chapel Hill, NC, February 8-11, 2009.

Treglia, J. V., & Park, J. S. (2009). "Towards trusted intelligence information sharing." Pp. 45-52 *in Proceedings of the ACM SIGKDD Workshop on CyberSecurity and Intelligence Informatics*. Paris, France: ACM.

Turoff, M.(1970). "The design of a policy Delphi." *Technological Forecasting and Social Change* 2(2):149-171).

USDOT. (2011). "Research and Innovative Technology Administration (RITA) - United States Department of Transportation (USDOT, US DOT or DOT*)." U.S. Department of Transportation - Research and Innovative Technology Administration*. Retrieved November 28, 2011 (http://www.its.dot.gov/ng911/).

Van Hoy, J. (1993). "Intraprofessional politics and professional regulation." *Work and occupations* 20(1):90.

Vann, I. (2005). *Testing the Rocheleau data sharing model on North Carolina law enforcement agencies. North Carolina State University*. Retrieved from http://search.proquest.com/docview/305425615?accountid=14214

Walker, J., & Ostrom, E. (2007). Trust and reciprocity as foundations for cooperation: Individuals, institutions, and context. *Capstone Meeting of the RSF Trust Initiative at the*

Russell Sage Foundation.

Weiss, J. A. (1987). “Pathways to cooperation among public agencies.” *Journal of Policy Analysis and Management* 7(1):94-117.

Weiss, R. S. (2004). In their own words: making the most of qualitative interviews. *Contexts*, 3(4), 44.

Westphal, I., Thoben, K.-D., & Seifert, M. (2008). Managing collaboration performance to govern virtual organizations. *Journal of Intelligent Manufacturing*, *21*, 311–320. doi:10.1007/s10845-008-0182-5

Wick, D., Franzoni, D., & Lustig, B. (Producers) & Scott, R. (Director). (2000). "Gladiator" [Motion picture]. United States: DreamWorks Home Entertainment.

Williams, C., Dias, M., Fedorowicz, J., Jacobson, D., Vilvovsky, S., Sawyer, S., & Tyworth, M. (2009). The formation of inter-organizational information sharing networks in public safety: Cartographic insights on rational choice and institutional explanations. *Information Polity*, 14(1), 13-29. doi:10.3233/IP-2009-0170

Williams, C. B., Fedorowicz, J., & Tomasino, A. P. (2010). Governmental factors associated with state-wide interagency collaboration initiatives. *Proceedings of the 11th Annual International Digital Government Research Conference on Public Administration Online: Challenges and Opportunities* (pp. 14-22). Puebla, Mexico: Digital Government Society of North America.

Wood, D., & Gray, B. (1991). Towards a comprehensive theory of collaboration. *Journal of Applied Behavioral Science* 27: 139–62.

Wood, D. and Gray, B. (1991). Towards a comprehensive theory of collaboration. Journal of Applied Behavioral Science 1991;27:139-62.

Yang, T. M., & Maxwell, T. A. (2011). Information-sharing in public organizations: A literature review of interpersonal, intra-organizational and inter-organizational success factors. *Government Information Quarterly*, 28(2), 164–175.

Yousuf, M. I. (2007). “The Delphi technique.” *Essays in Education* 20:80-9.

Zheng, J., Veinott, E., Bos, N., Olson, J. S., & Olson, G. M. (2002). Trust without touch: jumpstarting long-distance trust with initial social activities. *Proceedings of the SIGCHI conference on Human factors in computing systems: Changing our world, changing ourselves* (pp. 141–146). ACM.

Zheng, L., Dawes, S., & Pardo, T. A. (2009). Leadership behaviors in cross-boundary information sharing and integration: comparing the US and China. *Proceedings of the 3rd International Conference on Theory and Practice of Electronic Governance* (pp. 43–50). ACM.

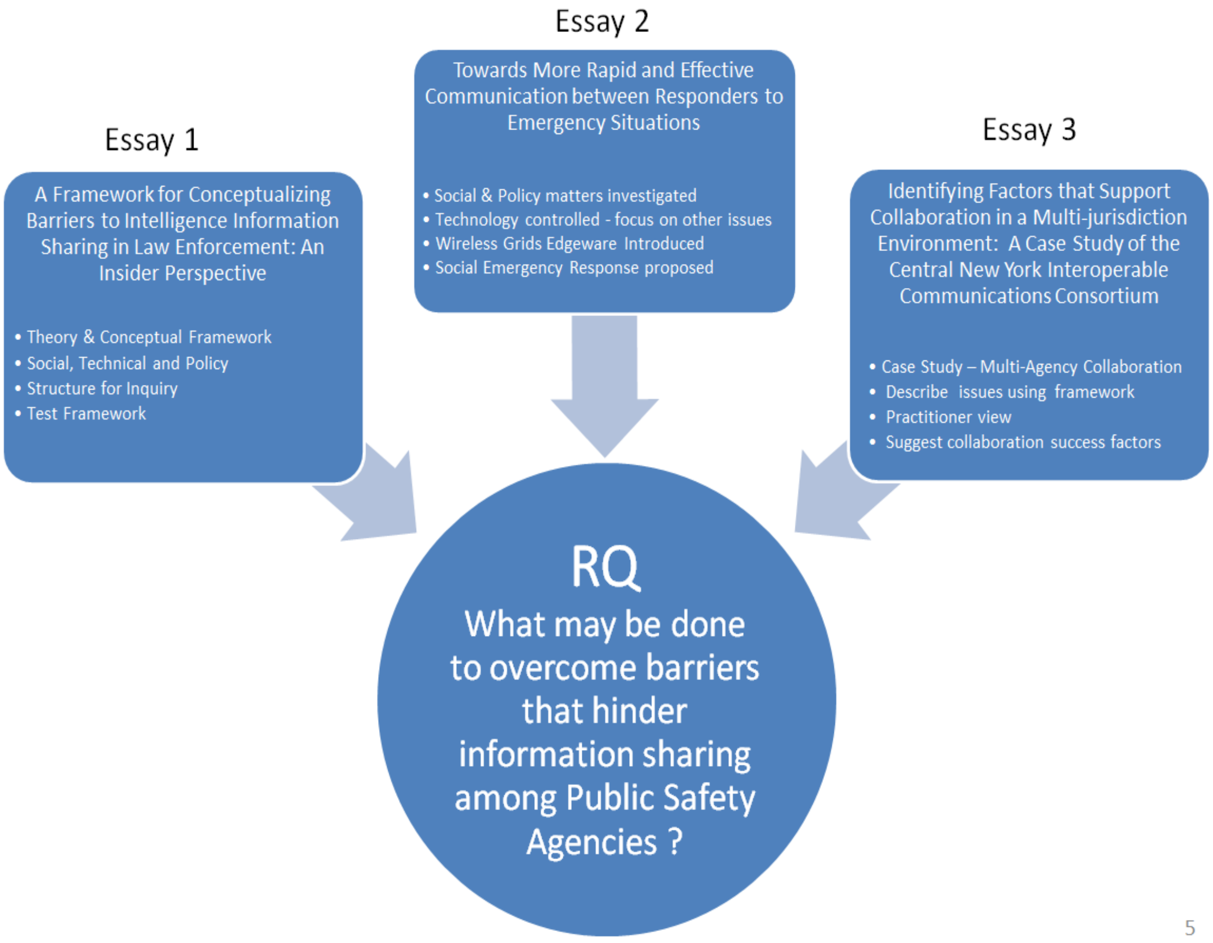
V. CHAPTER - CONCLUSION

This chapter provides an overview of the dissertation, highlights the major findings and factors, and describes proposed future work. A summary of the three essays is presented first. This is followed by a brief summary of the responses to the research questions and propositions. Contributions to the field are identified followed by challenges and finally a discussion of proposed future work.

These three essays explore the common theme of information sharing and collaboration in organizations with a focus on the law enforcement and emergency response community from an insider perspective. The essays include a theoretical piece, research regarding a social emergency response paradigm, and technology, with the last essay focusing on elements of successful collaboration. The findings contribute to a greater understanding of the forces that impact the agencies under consideration in regard to information sharing and thereby leading to identifying and implementing solutions to this problem from a new perspective.

1. Broader Context and Summary

This dissertation of three essays examined factors related to information sharing in the law enforcement and emergency response community. There is ample evidence of the loss and damage caused by failures in communication and information sharing in this area as well as the obvious value to society of finding solutions to this problem. Sparrow, Moore and Kennedy (1992, p. ii) wrote optimistically that, in this area, society has “a chance to forge new attitudes of mind and structures of relationships that will help it produce high-quality solutions to society’s problems – not just one problem but many problems; not just now but in the future – whatever the issues and constraints.” This dissertation contributes to understanding of the current and future factors, framing them in a way that they may be more constructively discussed and debated publicly, considering new technological possibilities and transforming existing social and policy paradigms. The role and contribution of the three papers is provided in the table below and described in detail in the following.



Essay 1

A Framework for Conceptualizing Barriers to Intelligence Information Sharing in Law Enforcement: An Insider Perspective

- Theory & Conceptual Framework
- Social, Technical and Policy
- Structure for Inquiry
- Test Framework

Essay 2

Towards More Rapid and Effective Communication between Responders to Emergency Situations

- Social & Policy matters investigated
- Technology controlled - focus on other issues
- Wireless Grids Edgeware Introduced
- Social Emergency Response proposed

Essay 3

Identifying Factors that Support Collaboration in a Multi-jurisdiction Environment: A Case Study of the Central New York Interoperable Communications Consortium

- Case Study – Multi-Agency Collaboration
- Describe issues using framework
- Practitioner view
- Suggest collaboration success factors

RQ

What may be done to overcome barriers that hinder information sharing among Public Safety Agencies ?

5

Figure 28 Summary of Three Essays

Essay #1

The creation of a framework to understand information sharing was the focus of the first essay, which is a theoretical piece identifying the framework and justifying its structure and use.

A number of theories were identified and considered throughout this work: General Systems Theory (GST), Socio-technical Systems Theory, Stakeholder Theory, and Public Choice Theory. Researchers considered the interplay of technology and policy with human systems in the law enforcement and emergency response environment. This dissertation proposes that information sharing in this environment is affected by social, technical and policy factors as influencers.

This research contributes to application of GST as well as contributing to the field of intelligence informatics, which concerns itself with the study and development of information systems and technology for international, national and societal security-related applications and for the academic researchers, law enforcement, intelligence experts, and IT professionals (Chen, Dacier, Moens, Paass, & Yang, 2009). Topics of interest for intelligence informatics include information sharing, infrastructure protection, crisis and emergency response. The model described is useful to frame the discussion and research in this area and further proposes additional steps towards identifying specific measures and contributions of model elements as well as their individual and collective impacts on information sharing behavior.

Essay #2

The second essay proposed and described a new social emergency response paradigm for whole community engagement in crisis response together with a new form of wireless grid networking technology. The social emergency response paradigm includes stigmergic involvement of both traditional and other non-traditional stakeholders, and entities, not previously considered as essential participants in this area. This whole community engagement plan is enabled through the promise of new networking technology to connect devices and people. Wireless grids "edgeware" technology is identified as one such emerging middleware solution in this space. Social and policy factors that currently impact information sharing in public safety emergency response were examined. This work further extends the understanding of technical, social, and policy factors in information sharing in the law enforcement and emergency response arenas.

Essay #3

The third essay presented in this trilogy is a case study of the Central New York Interoperable Communications Consortium (CNYICC), a five-county collaboration involving law enforcement, public safety, government and non-government participants. Human, technical, policy, and other factors were examined. Insights and recommendations regarding the formation, ongoing governance and strategies for dealing with technology implementation were identified and described. This work identified and described important elements of successful collaboration. The conceptual framework for information sharing derived in the first essay was used to organize the investigation and to verify the utility of the theoretical framework itself for describing information sharing factors.

2. Response to Research Questions

In this dissertation, it is proposed that information sharing is affected by factors involving social, technical and policy influencers. Steps are suggested that may be taken to overcome the internal and external barriers that hinder information sharing among federal, tribal, state and local law enforcement agencies and emergency responders. Social, technology and policy factors were identified and investigated in the second essay, which considered use of a transformative edgeware technology that allows for an unprecedented degree of connectivity among devices. Wireless grids edgeware was introduced and, with it, a focus on associated emergent social and policy factors that impact information sharing in an environment where all technology resources can be readily shared. Use of the framework in considering the factors and conducting the investigation proved useful for providing structure to the research and further in having the data follow a consistent format. The final essay addressed information sharing through collaborative behavior in public safety communications. Important elements to forming and maintaining collaborative relationships were identified by members of the law enforcement and emergency response community.

Research Proposition - P1

The first proposition is related to creation of the larger framework: (P1) Information sharing is affected by social, technical, and policy factors, and this conceptualization frames the problem of information sharing in such a way that it can be commonly understood by government and non-government stakeholders. The created model proved to be useful in explaining the literature and real-world issues and problems, and served as a means for framing the discussion and investigation. The framework was statistically validated through use of a national survey of law enforcement agencies. All three essays involved the use of this model, which was shown to be an effective model and tool for conceptualization of the problem factors.

Research Proposition – P2

The next research proposition involved the role of technology, policy, and social systems in information sharing: (P2) Social and policy factors influence information-sharing more than technical factors (assuming that it is physically possible to connect and/or share). The second and third essays addressed this proposition. In the second essay, technology is held constant by considering the use of edgeware, which allows disparate devices to communicate securely where this capability may not have been previously possible. With the enabling of communication between devices and parties, it became apparent that other factors continued to affect the sharing relationship beyond the limitations or constraints of technology. Social and policy factors still had to be considered even where seamless communication was made possible. In the third essay, the CNYICC case study, there is ample evidence provided by informants and through observations that the social factors are the major problem in information sharing so long as information can be shared technologically. The case study provides support for the claim that having the ability to share information technologically does not necessarily cause parties to share information with each other. The conclusion drawn is that social and policy factors pose more stubborn obstacles to information sharing, though technological factors are by no means of minor impact.

Proposition – P3

The third proposition addressed was as follows: (P3) Social factors play the greatest role in the creation and sustaining of information sharing relationships. This is proposed from the model and literature of the first essay. Evidence supporting this proposition is available from the second and third essays. The second essay considered the elements of the sharing relationships in the absence of limitations that may come from technology, and it was it was corroborated that there are stubborn social and policy barriers to be dealt with which interfere with the goal of effective information sharing. The final essay, the CNYICC case study, provides the most direct evidence supporting the third proposition. Statements and actions of the informants directly indicated that social factors played the most important role in driving and maintaining sharing relationships. The generalizability and applicability of the findings here are limited due to the fact that they involved an individual case study. The study involved actual county-level emergency responder agencies in central New York with some state level participation, and included non-government stakeholders. An argument can be made that this instance is unique or that the experience of the participants is not common. Nonetheless, researchers experience and observations in this area support the argument that it is representative of other public safety collaborations.

3. Contributions and Lessons Learned

Model and Theory Development

The first essay, "A Framework for Conceptualizing Barriers to Intelligence Information Sharing in Law Enforcement: An Insider Perspective," developed a model and theory of intelligence information sharing through literature review, interviews with practitioners and field observations. The contribution in this area comes in the form of describing and framing the broader issues and describing the environment and influences that operate across the law enforcement community. A conceptual framework for the examination and study of information sharing was developed and utilized to frame the problem and as a means for identifying solutions to the problems identified. This framework was more concise, focusing on three factors, yet consistent with elements from other scholars models and frameworks.

Information systems in business and organizational studies identify information systems as comprised of people, procedures, data, software, telecommunications, databases, and hardware used in concert to support a business purpose (Stair & Reynolds, 2011; O'Brien & Marakas, 2008). Operations management and information systems similarly identify system components such as plants, equipment, control procedures and policies (Lewis & Slack, 2003; Gupta, 2000).

Information sharing research by Dawes (1996) and Zhang et al. (2005) identify three primary influential factors as technology, management and policy. These are similar to the framework created in this dissertation; technical, social, and policy. Yang and Maxwell (2011) created a model consisting of three identified perspectives (Technological, Organizational and Managerial, and Political and Policy) that influence public sector information sharing, see Figure 8 for additional perspectives and factors.

Various schemas were considered in consultation with fellow researchers and practitioners and ultimately the three factors of Social, Technical, and Policy were determined to be inclusive of all system components and descriptive enough to provide for understanding and examination of information sharing systems and processes in public safety.

Challenges and New Solutions

In the second essay, "Towards More Rapid and Effective Communication between Responders to Emergency Situations," challenges in emergency response are identified and include both technical interoperability and social factors. Wireless grids edgeware is used as an example of a technology solution with the potential capacity to solve technical problems of interoperability and control over resources. There has been increasing acknowledgement of the nascent growth of wireless grids as a new engineering field of scientific inquiry and innovation (Fitzek & Katz, 2007; Manvi & Birie, 2009; Li, Sun, Yu, & Cai, 2009; Birie & Manvi, 2010, 2011; Li, Gong, Lai, Han, Qiu, & Yang, 2012; Sun, Mao, Liu, Liu, & Guan, 2012). Wireless grids research include works on user and socio-technical perspectives and challenges (McKnight, Sharif, & Wijngaert, 2005; McKnight & Howison, 2003), coordination of user and device behaviors (McKnight, Lehr, & Howison, 2007), and future internet applications and bridging communicative channels (McKnight, Howison, & Bradner, 2004; Dutton, Gillett, McKnight, & Peltu, 2004; McKnight, 2007). This technology allows users, in this case those formally and informally involved in emergency response, to access programs and data on disparate devices, across available wired and wireless networks more readily, allowing greater access to resources; however, technology does not resolve all issues as is evident from the research in the second and third essays.

Social Emergency Response

A goal of the project described in the second essay was to "help people help themselves." A social emergency response, together with the use of technology applications, such as wireless grids, can empower citizens to contribute to their own whole community response. The traditional response agency model, this dissertation argues, is outdated. Furthermore, widely disparate groups, including police, fire, EMS, hospitals, municipal services, utilities, gas companies, media, and community residents benefit from improved information sharing capability in emergencies, and this can be enabled by new social response paradigms and technologies, such as wireless grids edgeware. "Edgeware" describes software that resides beyond the cloud, across edge network devices, both wired and wireless (Treglia, Ramnarine-Rieks, & McKnight, 2010). A broader understanding of the nature of the opportunities offered by grid computing, virtual environments, and the technologies or standards needed to realize those opportunities is now required (Foster & Kesselman, 2004; Brooks, Caicedo, & Park, 2012). The fundamental difference between this form of interconnection over traditional networking is that it allows for true resource sharing.

Open source initiatives are proving to be valuable for public warning and commercial ICT-based (Information and Communications Technology - based) warning services continue to exist as well (Botterell & Addams-Moring, 2007). Emergency management as a complex system is studied in the category of resilient ecological systems (Longstaff, 2009). Emergency response personnel may need to mix and match other disparate and possibly unfamiliar technologies to fit the tasks at hand (Mendonça, Jefferson, & Harrald, 2007).

The research her provides further evidence that when it comes to emergency response, additional requirements need to be taken into account. Social and policy factors remain significant and will continue to constrain effective response unless solutions such as those suggested here are implemented.

Collaboration and Interoperability

A case study, “Identifying Factors that Support Collaboration in a Multi-jurisdiction Environment: A case Study of the Central New York Interoperable Communications Consortium,” was conducted focusing on interagency collaboration and cooperation in the emergency services area involving the emergence and activities of a multi-jurisdictional radio consortium. The study is significant in that it is representative of the communication dynamics, and other issues, of other multi-jurisdictional law enforcement and emergency services providers across the nation. The importance of interoperable communications is well acknowledged today. There are federal and local mandates affecting law enforcement and emergency response agencies, which are driving them to change and implement interoperable technology and policies. Financially, there are economic drivers pushing agencies towards standards-based interoperable equipment and software. Agencies across the nation and world are finding that they must work together to effectively protect the public and respond to ever-occurring local and large-scale crises. Specific recommendations regarding collaboration in this environment are provided. The findings from this study are consistent with other case studies and work in this area. Kuenzel and Welscher propose model factors important to ‘Public Safety Collaboration Success’ (2009) as: 1. Relevance and Sense of Urgency; 2. Incentives and Benefits; 3. People & Roles; 4. Organizational Structure; 5. Reflection & Learning: 6. Skills and Capabilities; 7. Resources; and 8. Outside Support & Supervision. They assert that the eight factors must be incorporated in a collaboration for it to achieve its desired public safety objectives (Kuenzel & Welscher, 2009). Success factors identified in the case study have some common elements. Consistent with the CNYICC case study, Brafman and Beckstrom assert that flexibility in leadership guided by a shared vision and goal are important aspects of successful governance and collaboration models (2008). The contribution of individual leadership characteristics have been studied by many (Zhang, Dawes, & Pardo, 2009; Parry, 2009). Also consistent with statements from the CNYICC case study, it is internal agency leadership that matters more than external or outside political leadership (Vann, 2005). Resources were not identified in the CNYICC case study as being an essential element to collaboration. Members report working with what they have for the overall good.

A best practice example of interoperability principles at work is the European Interoperability Framework (EIF) of e-government (IDABC, 2008). There are “Interoperability Principles” that can form policy guidelines to make it clear to all participants what is meant by interoperability (Kuehn, Spichiger, & Riedl, 2009). Similar principles could be developed for the emergency response sector in the United States.

The aim of theory is to help explain and understand the underlying conditions and causality of an activity or event in order to thereby understand what works well so that it can be repeated. The case study provides important insider insights from members of the emergency response community themselves. Going forward, the need for collaboration and integration of investigative and response resources across the law enforcement and emergency response community will be paramount to successfully achieving public safety goals. Lessons learned from the case study of the Central New York Interoperable Communications Consortium contribute to this effort and evolution. This is much like the story of the self-made millionaire who went to college only after achieving personal success, returning to school with the understanding that if she could not explain her success, she could not effectively repeat it (Handy, 1976). From the CNYICC case studied, researchers are able to report on multiple factors that help and hinder cooperation. This research has produced some valuable tools for the re-creation of success in emergency response interagency cooperation, and information sharing.

There is practical benefit in understanding and applying the lessons learned in this study regarding successful collaborations between such agencies. The case study itself is relevant to understanding other similar coordination efforts in this community. Research results are intended to be applicable in other settings as “best practices,” obviating the need to constantly engage in trial and error. Many of the situations and challenges that law enforcement and emergency response personnel face are common across the field, so insight from this study will likely be applicable in other, similar interagency collaborations.

This "generalizable knowledge" contributes to the theoretical framework and adds to the established body of knowledge concerning the factors that influence information sharing and collaboration in public safety, law enforcement, emergency response and the field of information science.

3. Reflection

This research involved three stages of model development and included empirical investigation, through case study, survey data, and document content analysis over the course of several years. This extended and separated research design process changed the focus and contribution of the study and findings. Initially, activities were focused on the law enforcement community. Through participation in the Public Safety Networks Study and involvement with the community and public safety focused problems investigated in the Wireless Grids Innovation Testbed (WiGiT) a broader and more comprehensive focus on public safety entities, issues and concerns evolved. This expanded the stakeholders and study interests to embrace law enforcement and emergency response agencies, and the public as well.

An advantage of having the separate but related research streams was that it improved the accuracy and generalizability of the overall study. The resulting research is more robust, accurate and applicable to this broader audience. The use of large national survey data such as the national survey of law enforcement agencies and public safety networks study survey together with multiple public safety agency after action reports and the in-depth case study of the CNYICC provided a broad view from across disciplines. Limiting the resources available for this research (including the availability of insider information) would have reduced the depth of investigation and data available. The results are as accurate and real as they are due to the volume and variety of resources involved.

An alternate means to effectively conduct the research for this dissertation would be to work collaboratively across disciplines in parallel with other researchers. Such an approach would bring researchers from Sociology, Political Science, Information Science, Criminal Justice, the emerging fields of Emergency and Crisis Management, Public Safety and others together. Engaging multiple perspectives through this method would lead to robust and comprehensive insights, understanding and solutions as well.

4. Future Work

Model Refinement

Future work stemming from this dissertation involves further investigation and refinement of the model for information sharing. It also should involve further consideration of the implications of edgeware and related wireless grids technology and its utility in this area as well as additional work on understanding social, policy and technological barriers to collaboration in the emergency response community.

In this dissertation, these three major areas of influence (Technical, Social, and Policy) on information sharing between law enforcement and emergency response entities are identified and better understood. The degree of influence of these areas, as well as trust as a factor that cuts across all of these areas, should be further investigated to assess their effect on cooperation and information sharing activity. The ultimate aim is to identify and implement actionable solutions.

Experience in broader government foreign relations may serve as an example for modeling or describing the sharing problems faced here. Foreign relations scenarios and hypothetical situations could be investigated that would potentially bring light to different aspects of the problem of working with mixed authority and interests as well as varying levels of trust. Thus, identifying successful practices and/or policies for information sharing in the international relations environment could be adapted to the interagency information sharing environment, with models constructed to more readily understand the interplay there. If found useful, they could inform future models of interagency information sharing.

Interoperability and Wireless Grids

Much research remains to be done on information interoperability in the context of emergency response systems. Technical solutions such as wireless grids edgeware applications allow cooperation and resource sharing to occur in the current blended environment. In the future, systems will continue to grow and platforms change, but they can retain functionality and interoperability through such an intermediary service. Having such a capability (e.g. wireless grids) will foster the identification and testing of new solutions and problems in emergency services to include technical, social, and policy factors. Issues such as the lack of common ontologies or definitions for identifying resources require further investigation. Information overload, e.g. having too much or too many resources to effectively manage or use them, is a concern. There remains a need for additional work to be done on the filtering of information or creation of intelligent dashboards for decision makers in crisis response to reduce information overload.

Social Emergency Response

Social emergency response is an emerging area of interest within the government and the academic community. The expanded role that non-traditional actors play in a “whole community” response to a crisis or emergency is gaining acknowledgement at federal and local government levels. Additional work in the area of social and policy influences is necessary with the goal of creating an environment more open to and accepting of these new configurations of responders.

Case Study Research

The case study of the CNYICC provides early insights regarding social, technical, policy, and other factors that influence how people form, implement and ultimately cooperate with interagency/public safety communications enhancements afforded by advancements in technology. This work is a part of other case studies that address collaboration and cooperation in this highly technologically infused environment. Future work should include additional case studies that involve public safety entities and consideration should be given to the notion of these studies including a broader range of stakeholders to further augment the literature and empirical data available in this important area.

VI. Appendix

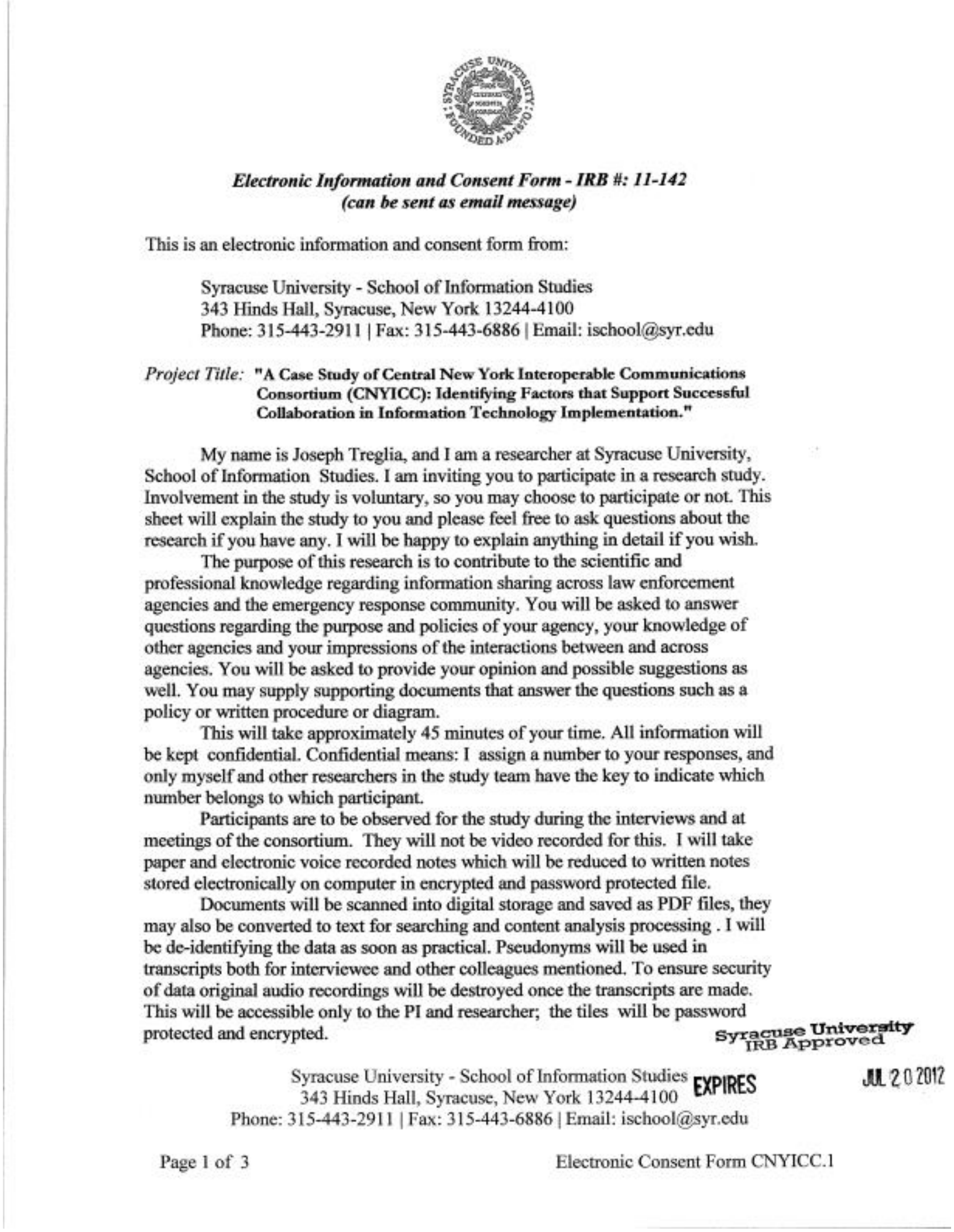
Appendix

A. Federal Initiatives on Information Sharing

There are a number of new and ongoing initiatives sponsored by the federal government that directly impact information sharing efforts at all levels. A number of these are briefly identified here (ISE, 2011). The Department of Homeland Security (DHS) was created as a federal cabinet level department charged with primary responsibilities of protecting U.S. territory from terrorist attacks and responding to natural disasters (DHS, 2011). DHS is concerned with the civilian sphere. The Intelligence Reform and Terrorism Prevention Act of 2004 created the Information Sharing Environment (ISE), as an approach to sharing terrorism-related information. A presidentially appointed Program Manager oversees operations assisted by the Information Sharing Council (ISC) consisting of 16 federal agency officials. The current Information Sharing Environment (ISE) combines policies, procedures, and technologies linking resources (people, systems, databases, and information) at all levels, including tribal entities and the private sector; the primary focus is "... any mission process, anywhere, which has a material impact on detecting, preventing, disrupting, responding to, or mitigating terrorist activity" (ISE, 2011). In 2010, the Department of Justice created the National Suspicious Activity and Reporting (SAR) Initiative (NSI) to assist participants at all levels in sharing and compatibility. Law enforcement information sharing initiatives include the FBI’s Criminal Justice Information Services (CJIS) Division with the following services; National Crime Information Center (NCIC), Integrated Automated Fingerprint Identification System (IAFIS), Uniform Crime Reporting Program, Law Enforcement On-line (LEO), six Regional Information Sharing System Network (RISSNET) centers, and the National Data Exchange (N-DEX) (ISE, 2011). The private sector is specifically addressed through DHS’s Critical Infrastructure and Key Resources (CIKR) initiatives integrated within the ISE.

Appendix

B. Case Study Consent Forms



Electronic Information and Consent Form - IRB #: 11-142
(can be sent as email message)

This is an electronic information and consent form from:

Syracuse University - School of Information Studies
343 Hinds Hall, Syracuse, New York 13244-4100
Phone: 315-443-2911 | Fax: 315-443-6886 | Email: ischool@syr.edu

Project Title: **"A Case Study of Central New York Interoperable Communications Consortium (CNYICC): Identifying Factors that Support Successful Collaboration in Information Technology Implementation."**

My name is Joseph Treglia, and I am a researcher at Syracuse University, School of Information Studies. I am inviting you to participate in a research study. Involvement in the study is voluntary, so you may choose to participate or not. This sheet will explain the study to you and please feel free to ask questions about the research if you have any. I will be happy to explain anything in detail if you wish.

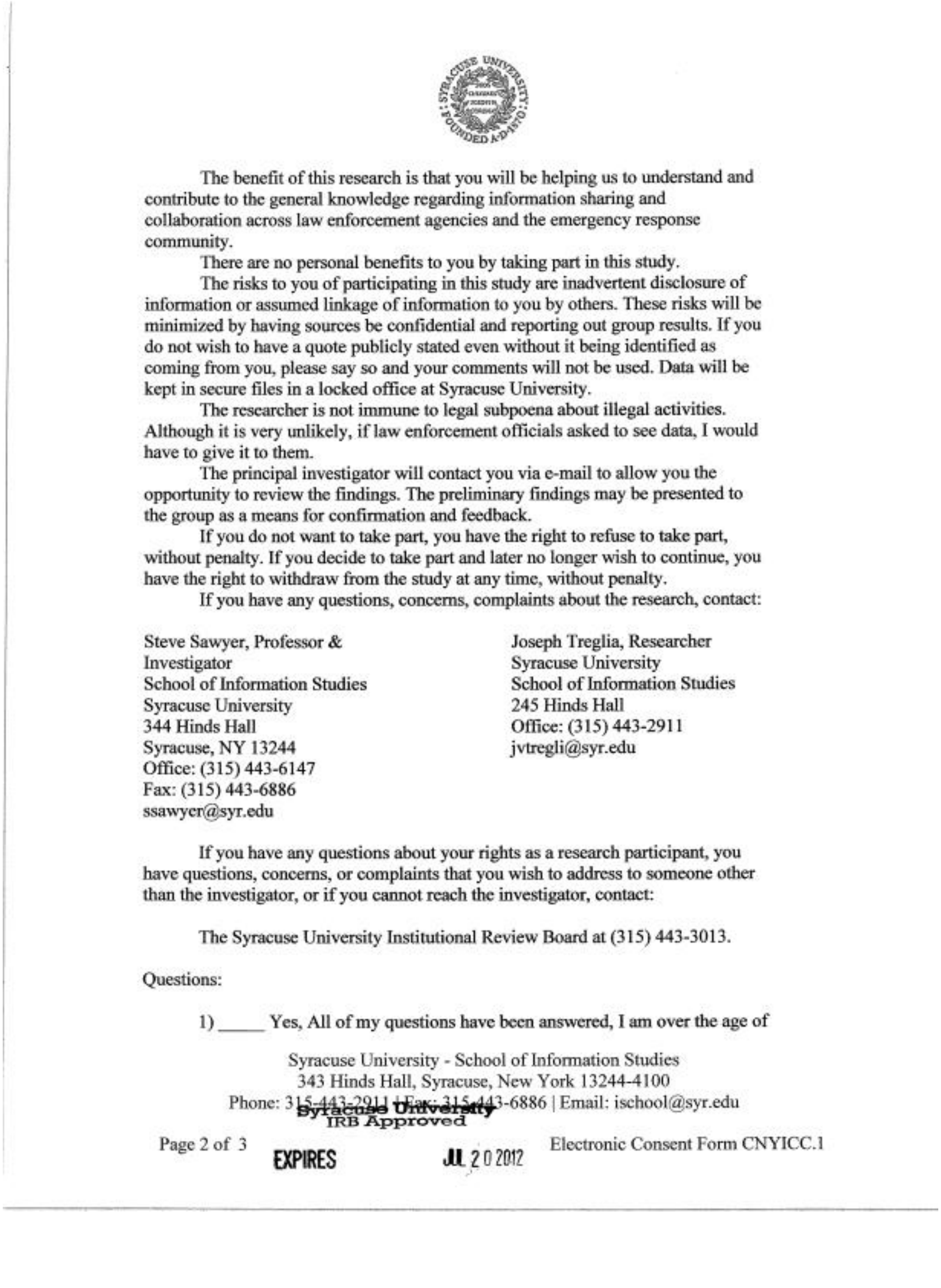
The purpose of this research is to contribute to the scientific and professional knowledge regarding information sharing across law enforcement agencies and the emergency response community. You will be asked to answer questions regarding the purpose and policies of your agency, your knowledge of other agencies and your impressions of the interactions between and across agencies. You will be asked to provide your opinion and possible suggestions as well. You may supply supporting documents that answer the questions such as a policy or written procedure or diagram.

This will take approximately 45 minutes of your time. All information will be kept confidential. Confidential means: I assign a number to your responses, and only myself and other researchers in the study team have the key to indicate which number belongs to which participant.

Participants are to be observed for the study during the interviews and at meetings of the consortium. They will not be video recorded for this. I will take paper and electronic voice recorded notes which will be reduced to written notes stored electronically on computer in encrypted and password protected file.

Documents will be scanned into digital storage and saved as PDF files, they may also be converted to text for searching and content analysis processing . I will be de-identifying the data as soon as practical. Pseudonyms will be used in transcripts both for interviewee and other colleagues mentioned. To ensure security of data original audio recordings will be destroyed once the transcripts are made. This will be accessible only to the PI and researcher; the tiles will be password protected and encrypted.

Syracuse University
IRB Approved
EXPIRES JUL 20 2012



The benefit of this research is that you will be helping us to understand and contribute to the general knowledge regarding information sharing and collaboration across law enforcement agencies and the emergency response community.

There are no personal benefits to you by taking part in this study.

The risks to you of participating in this study are inadvertent disclosure of information or assumed linkage of information to you by others. These risks will be minimized by having sources be confidential and reporting out group results. If you do not wish to have a quote publicly stated even without it being identified as coming from you, please say so and your comments will not be used. Data will be kept in secure files in a locked office at Syracuse University.

The researcher is not immune to legal subpoena about illegal activities. Although it is very unlikely, if law enforcement officials asked to see data, I would have to give it to them.

The principal investigator will contact you via e-mail to allow you the opportunity to review the findings. The preliminary findings may be presented to the group as a means for confirmation and feedback.

If you do not want to take part, you have the right to refuse to take part, without penalty. If you decide to take part and later no longer wish to continue, you have the right to withdraw from the study at any time, without penalty.

If you have any questions, concerns, complaints about the research, contact:

Steve Sawyer, Professor &
Investigator
School of Information Studies
Syracuse University
344 Hinds Hall
Syracuse, NY 13244
Office: (315) 443-6147
Fax: (315) 443-6886
ssawyer@syr.edu

Joseph Treglia, Researcher
Syracuse University
School of Information Studies
245 Hinds Hall
Office: (315) 443-2911
jvtregli@syr.edu

If you have any questions about your rights as a research participant, you have questions, concerns, or complaints that you wish to address to someone other than the investigator, or if you cannot reach the investigator, contact:

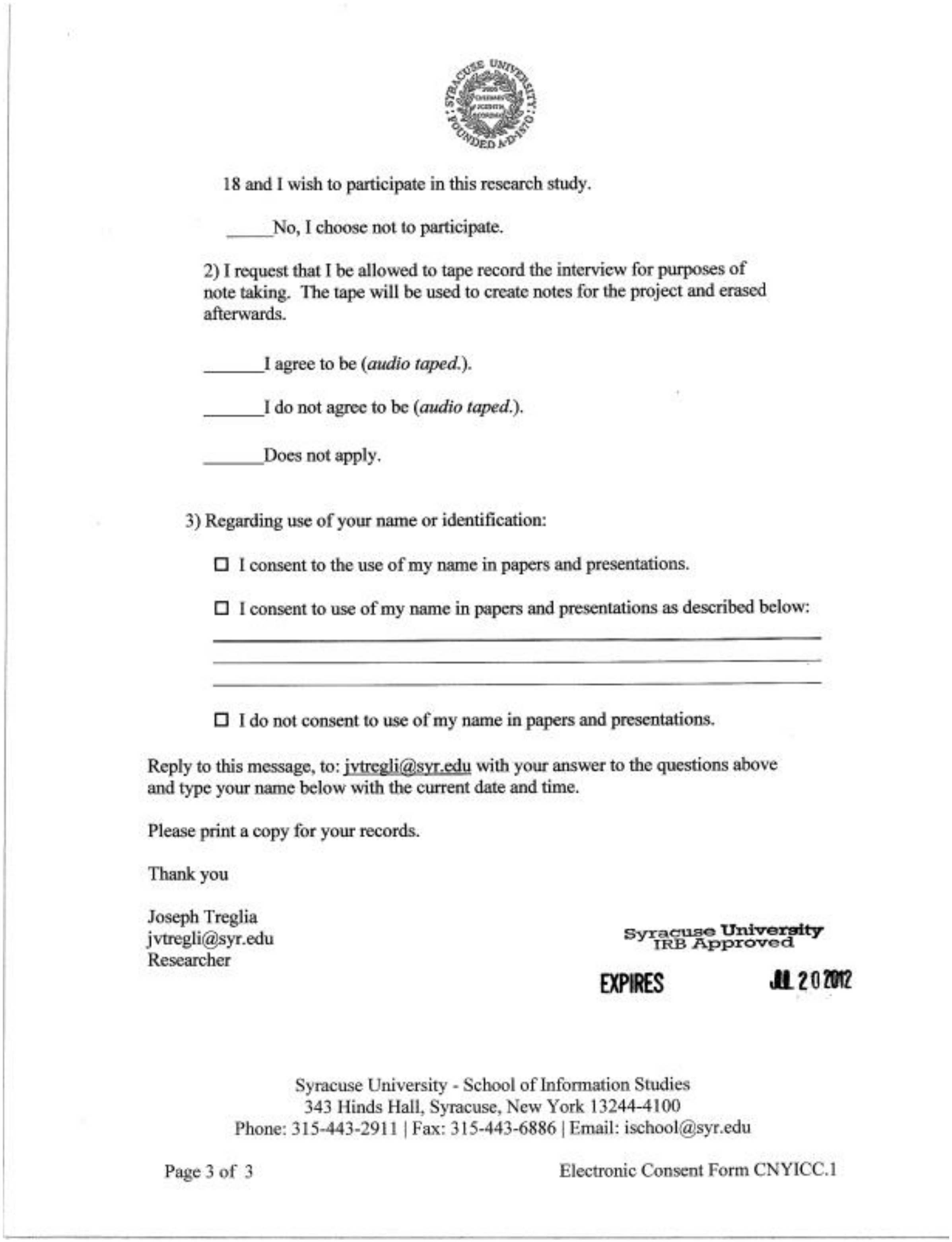
The Syracuse University Institutional Review Board at (315) 443-3013.

Questions:

1) _____ Yes, All of my questions have been answered, I am over the age of

Syracuse University
IRB Approved

EXPIRES JUL 20 2012



18 and I wish to participate in this research study.

_____No, I choose not to participate.

2) I request that I be allowed to tape record the interview for purposes of note taking. The tape will be used to create notes for the project and erased afterwards.

______I agree to be (*audio taped.*).

______I do not agree to be (*audio taped.*).

______Does not apply.

3) Regarding use of your name or identification:

□ I consent to the use of my name in papers and presentations.

□ I consent to use of my name in papers and presentations as described below:

____

____

____

□ I do not consent to use of my name in papers and presentations.

Reply to this message, to: jvtregli@syr.edu with your answer to the questions above and type your name below with the current date and time.

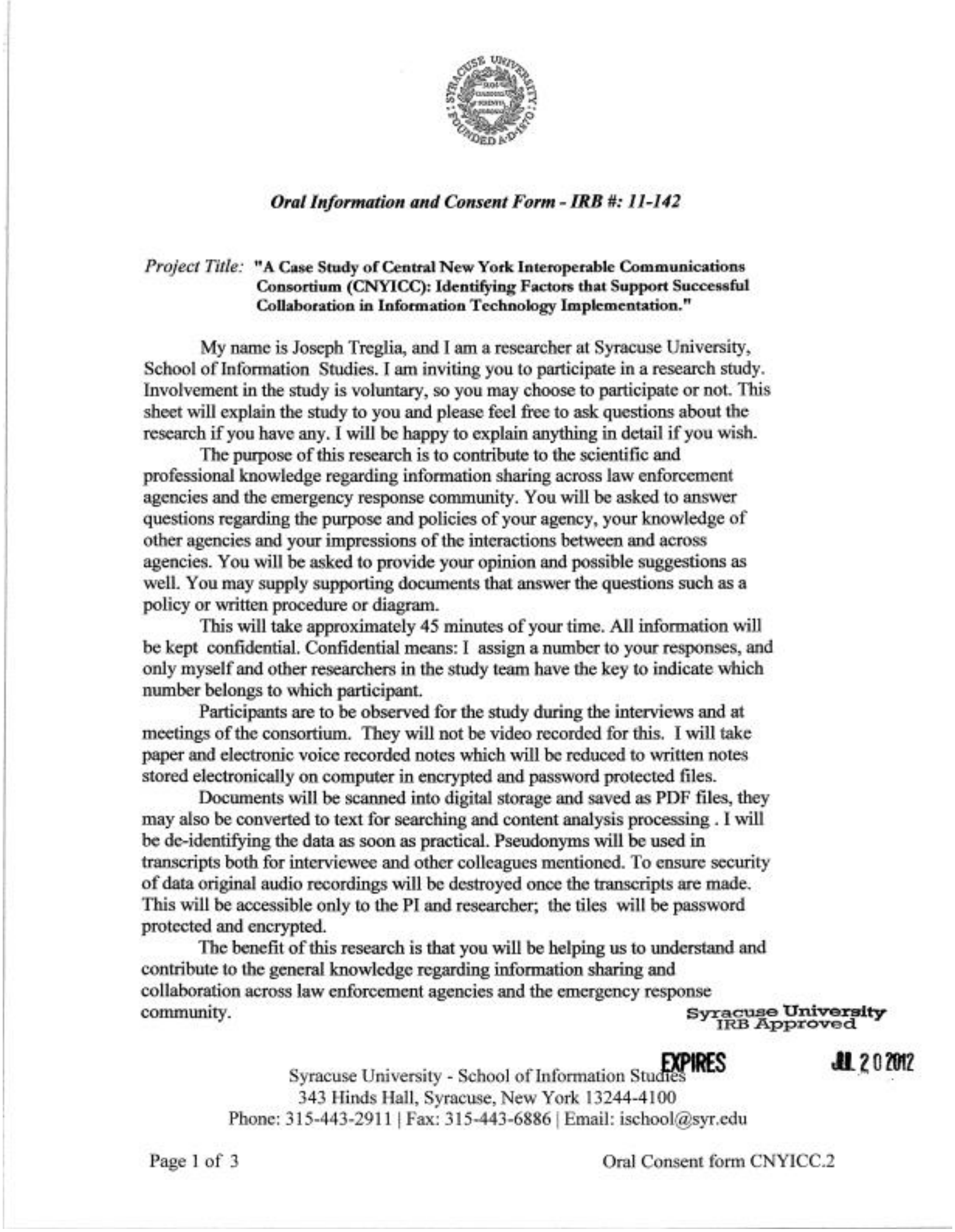
Please print a copy for your records.

Thank you

Joseph Treglia
jvtregli@syr.edu
Researcher

Syracuse University
IRB Approved

EXPIRES JUL 20 2012



Oral Information and Consent Form - IRB #: 11-142

Project Title: **"A Case Study of Central New York Interoperable Communications Consortium (CNYICC): Identifying Factors that Support Successful Collaboration in Information Technology Implementation."**

My name is Joseph Treglia, and I am a researcher at Syracuse University, School of Information Studies. I am inviting you to participate in a research study. Involvement in the study is voluntary, so you may choose to participate or not. This sheet will explain the study to you and please feel free to ask questions about the research if you have any. I will be happy to explain anything in detail if you wish.

The purpose of this research is to contribute to the scientific and professional knowledge regarding information sharing across law enforcement agencies and the emergency response community. You will be asked to answer questions regarding the purpose and policies of your agency, your knowledge of other agencies and your impressions of the interactions between and across agencies. You will be asked to provide your opinion and possible suggestions as well. You may supply supporting documents that answer the questions such as a policy or written procedure or diagram.

This will take approximately 45 minutes of your time. All information will be kept confidential. Confidential means: I assign a number to your responses, and only myself and other researchers in the study team have the key to indicate which number belongs to which participant.

Participants are to be observed for the study during the interviews and at meetings of the consortium. They will not be video recorded for this. I will take paper and electronic voice recorded notes which will be reduced to written notes stored electronically on computer in encrypted and password protected files.

Documents will be scanned into digital storage and saved as PDF files, they may also be converted to text for searching and content analysis processing . I will be de-identifying the data as soon as practical. Pseudonyms will be used in transcripts both for interviewee and other colleagues mentioned. To ensure security of data original audio recordings will be destroyed once the transcripts are made. This will be accessible only to the PI and researcher; the tiles will be password protected and encrypted.

The benefit of this research is that you will be helping us to understand and contribute to the general knowledge regarding information sharing and collaboration across law enforcement agencies and the emergency response community.

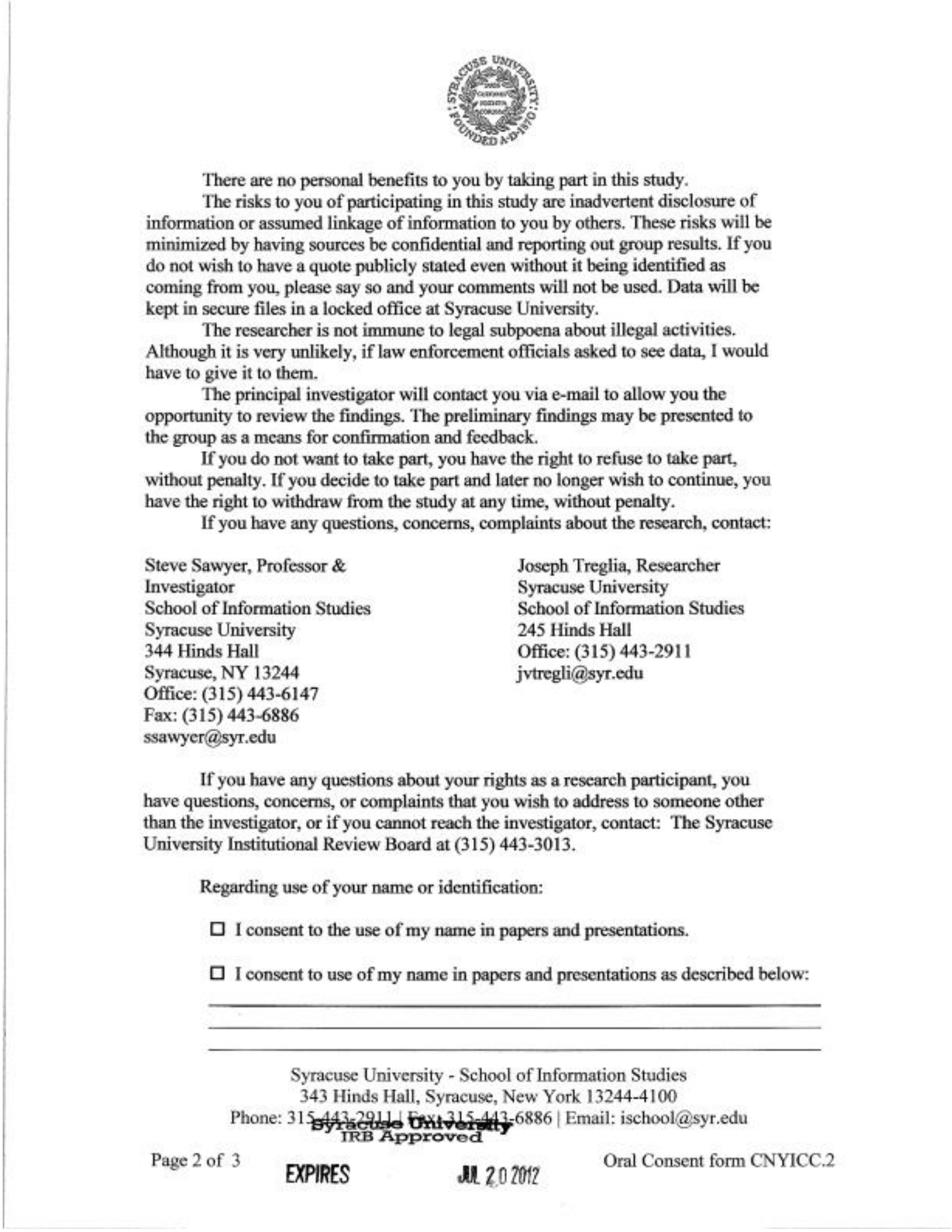
Syracuse University
IRB Approved

EXPIRES JUL 20 2012

Syracuse University - School of Information Studies
343 Hinds Hall, Syracuse, New York 13244-4100
Phone: 315-443-2911 | Fax: 315-443-6886 | Email: ischool@syr.edu

Page 1 of 3

Oral Consent form CNYICC.2



There are no personal benefits to you by taking part in this study.

The risks to you of participating in this study are inadvertent disclosure of information or assumed linkage of information to you by others. These risks will be minimized by having sources be confidential and reporting out group results. If you do not wish to have a quote publicly stated even without it being identified as coming from you, please say so and your comments will not be used. Data will be kept in secure files in a locked office at Syracuse University.

The researcher is not immune to legal subpoena about illegal activities. Although it is very unlikely, if law enforcement officials asked to see data, I would have to give it to them.

The principal investigator will contact you via e-mail to allow you the opportunity to review the findings. The preliminary findings may be presented to the group as a means for confirmation and feedback.

If you do not want to take part, you have the right to refuse to take part, without penalty. If you decide to take part and later no longer wish to continue, you have the right to withdraw from the study at any time, without penalty.

If you have any questions, concerns, complaints about the research, contact:

Steve Sawyer, Professor &
Investigator
School of Information Studies
Syracuse University
344 Hinds Hall
Syracuse, NY 13244
Office: (315) 443-6147
Fax: (315) 443-6886
ssawyer@syr.edu

Joseph Treglia, Researcher
Syracuse University
School of Information Studies
245 Hinds Hall
Office: (315) 443-2911
jvtregli@syr.edu

If you have any questions about your rights as a research participant, you have questions, concerns, or complaints that you wish to address to someone other than the investigator, or if you cannot reach the investigator, contact: The Syracuse University Institutional Review Board at (315) 443-3013.

Regarding use of your name or identification:

□ I consent to the use of my name in papers and presentations.

□ I consent to use of my name in papers and presentations as described below:

____

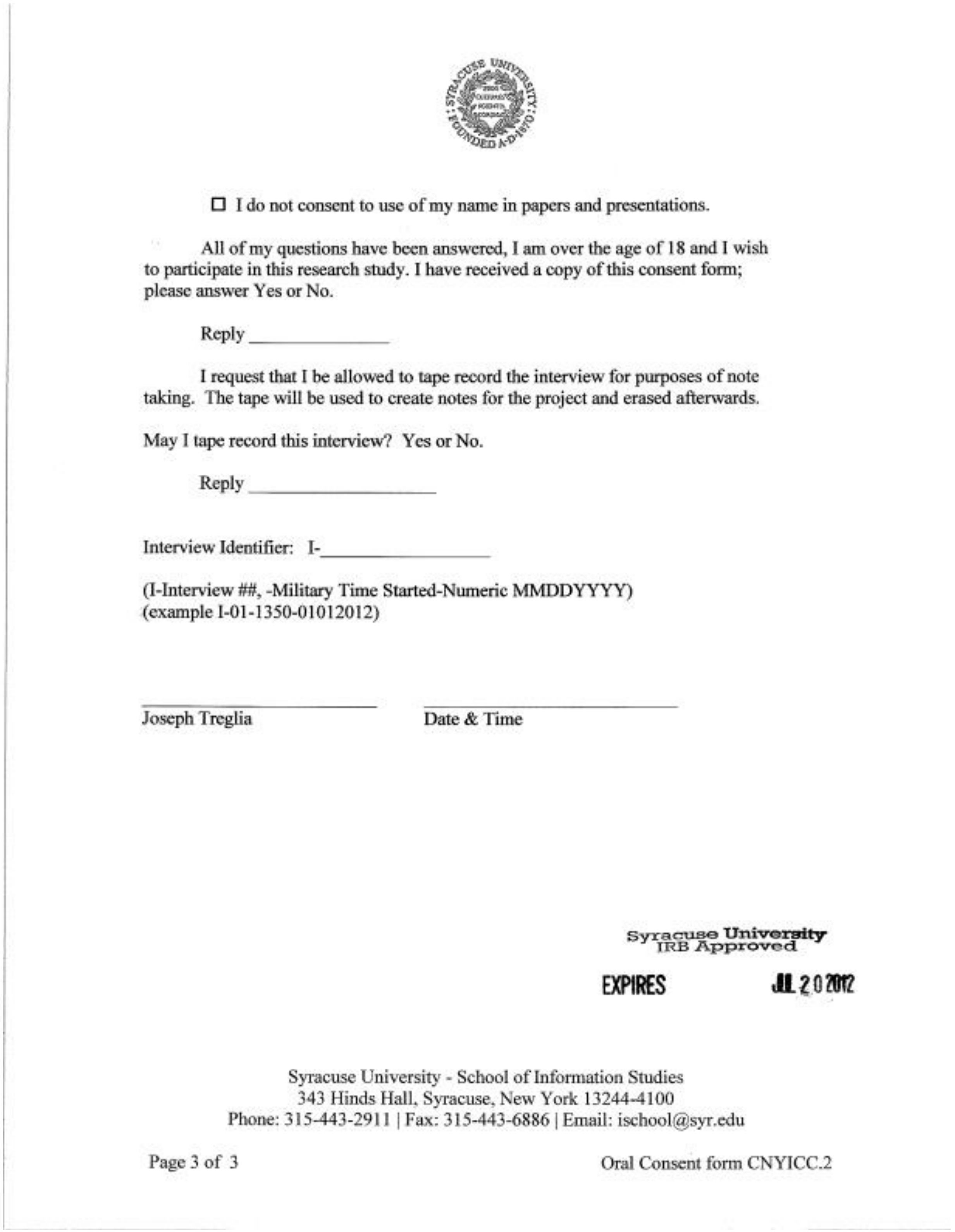
____

____

Syracuse University - School of Information Studies
343 Hinds Hall, Syracuse, New York 13244-4100
Phone: 315-443-2911 | Fax: 315-443-6886 | Email: ischool@syr.edu

Syracuse University
IRB Approved
EXPIRES JUL 20 2012

Page 2 of 3 Oral Consent form CNYICC.2



□ I do not consent to use of my name in papers and presentations.

All of my questions have been answered, I am over the age of 18 and I wish to participate in this research study. I have received a copy of this consent form; please answer Yes or No.

Reply ______________

I request that I be allowed to tape record the interview for purposes of note taking. The tape will be used to create notes for the project and erased afterwards.

May I tape record this interview? Yes or No.

Reply ___________________

Interview Identifier: I-________________

(I-Interview ##, -Military Time Started-Numeric MMDDYYYY)
(example I-01-1350-01012012)

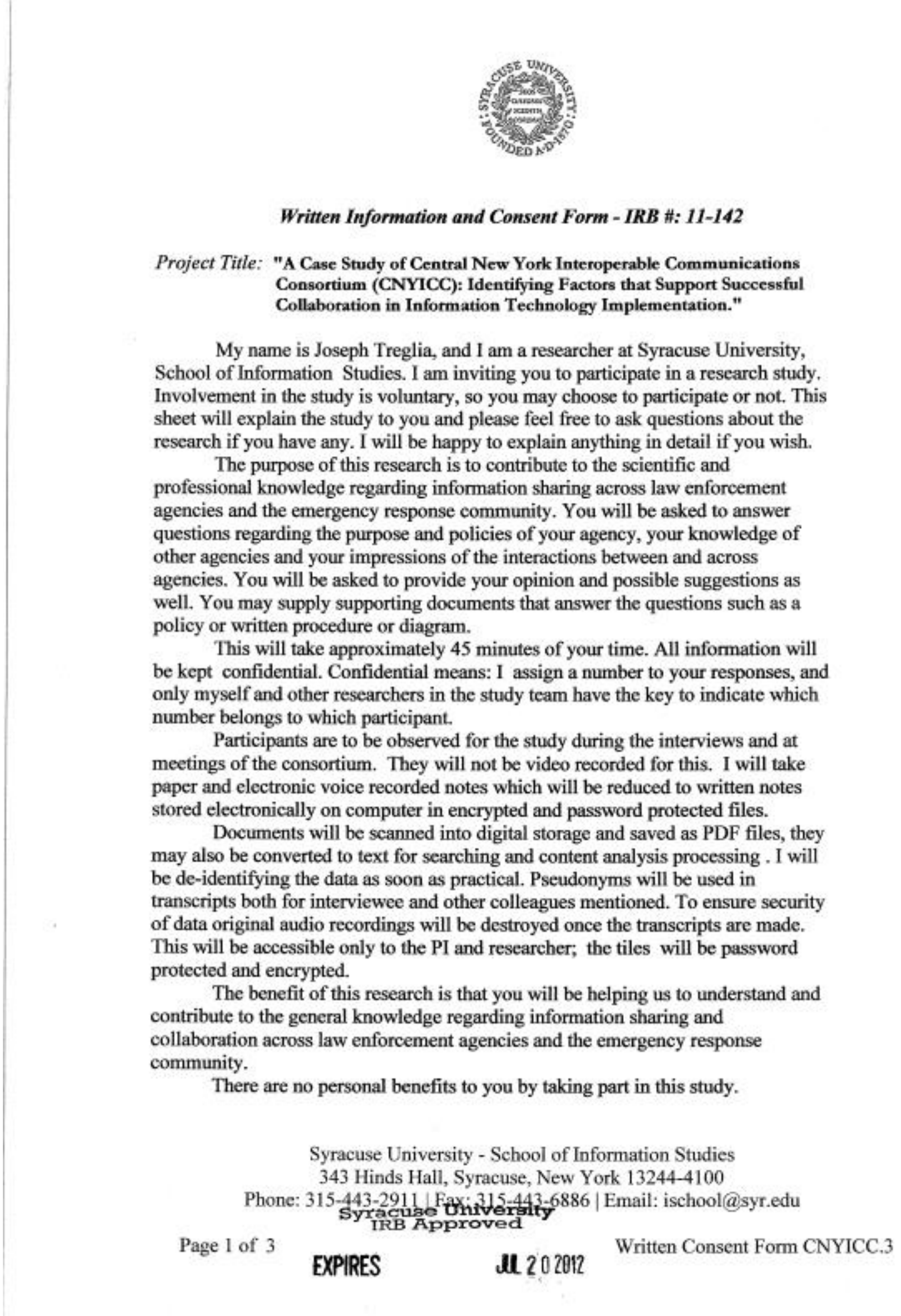
________________________ ________________________
Joseph Treglia Date & Time

Syracuse University
IRB Approved

EXPIRES JUL 20 2012

Syracuse University - School of Information Studies
343 Hinds Hall, Syracuse, New York 13244-4100
Phone: 315-443-2911 | Fax: 315-443-6886 | Email: ischool@syr.edu

Page 3 of 3 Oral Consent form CNYICC.2



Written Information and Consent Form - IRB #: 11-142

Project Title: **"A Case Study of Central New York Interoperable Communications Consortium (CNYICC): Identifying Factors that Support Successful Collaboration in Information Technology Implementation."**

My name is Joseph Treglia, and I am a researcher at Syracuse University, School of Information Studies. I am inviting you to participate in a research study. Involvement in the study is voluntary, so you may choose to participate or not. This sheet will explain the study to you and please feel free to ask questions about the research if you have any. I will be happy to explain anything in detail if you wish.

The purpose of this research is to contribute to the scientific and professional knowledge regarding information sharing across law enforcement agencies and the emergency response community. You will be asked to answer questions regarding the purpose and policies of your agency, your knowledge of other agencies and your impressions of the interactions between and across agencies. You will be asked to provide your opinion and possible suggestions as well. You may supply supporting documents that answer the questions such as a policy or written procedure or diagram.

This will take approximately 45 minutes of your time. All information will be kept confidential. Confidential means: I assign a number to your responses, and only myself and other researchers in the study team have the key to indicate which number belongs to which participant.

Participants are to be observed for the study during the interviews and at meetings of the consortium. They will not be video recorded for this. I will take paper and electronic voice recorded notes which will be reduced to written notes stored electronically on computer in encrypted and password protected files.

Documents will be scanned into digital storage and saved as PDF files, they may also be converted to text for searching and content analysis processing . I will be de-identifying the data as soon as practical. Pseudonyms will be used in transcripts both for interviewee and other colleagues mentioned. To ensure security of data original audio recordings will be destroyed once the transcripts are made. This will be accessible only to the PI and researcher; the tiles will be password protected and encrypted.

The benefit of this research is that you will be helping us to understand and contribute to the general knowledge regarding information sharing and collaboration across law enforcement agencies and the emergency response community.

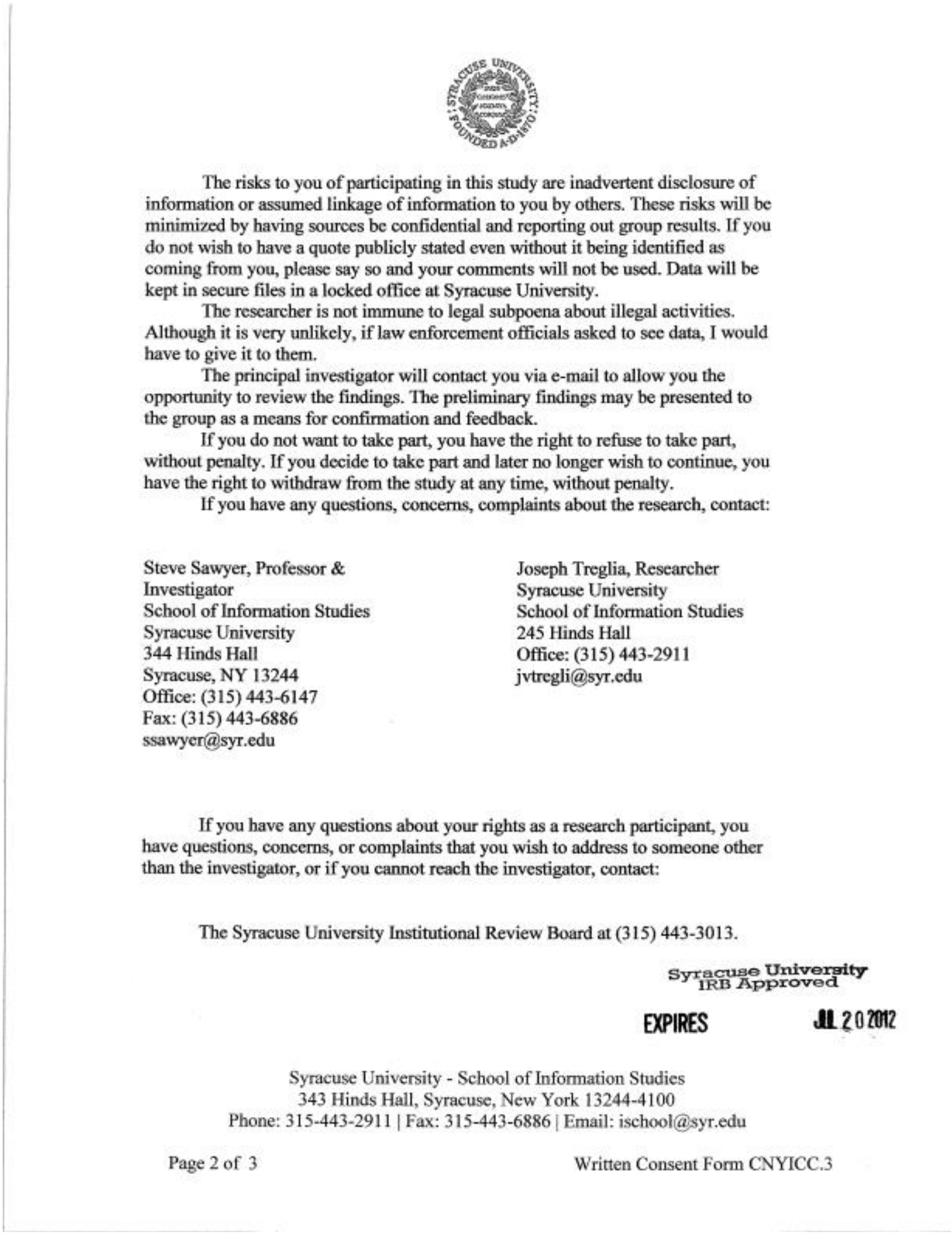
There are no personal benefits to you by taking part in this study.

Syracuse University - School of Information Studies
343 Hinds Hall, Syracuse, New York 13244-4100
Phone: 315-443-2911 | Fax: 315-443-6886 | Email: ischool@syr.edu

Syracuse University
IRB Approved

Page 1 of 3 Written Consent Form CNYICC.3

EXPIRES JUL 2 0 2012



The risks to you of participating in this study are inadvertent disclosure of information or assumed linkage of information to you by others. These risks will be minimized by having sources be confidential and reporting out group results. If you do not wish to have a quote publicly stated even without it being identified as coming from you, please say so and your comments will not be used. Data will be kept in secure files in a locked office at Syracuse University.

The researcher is not immune to legal subpoena about illegal activities. Although it is very unlikely, if law enforcement officials asked to see data, I would have to give it to them.

The principal investigator will contact you via e-mail to allow you the opportunity to review the findings. The preliminary findings may be presented to the group as a means for confirmation and feedback.

If you do not want to take part, you have the right to refuse to take part, without penalty. If you decide to take part and later no longer wish to continue, you have the right to withdraw from the study at any time, without penalty.

If you have any questions, concerns, complaints about the research, contact:

Steve Sawyer, Professor &
Investigator
School of Information Studies
Syracuse University
344 Hinds Hall
Syracuse, NY 13244
Office: (315) 443-6147
Fax: (315) 443-6886
ssawyer@syr.edu

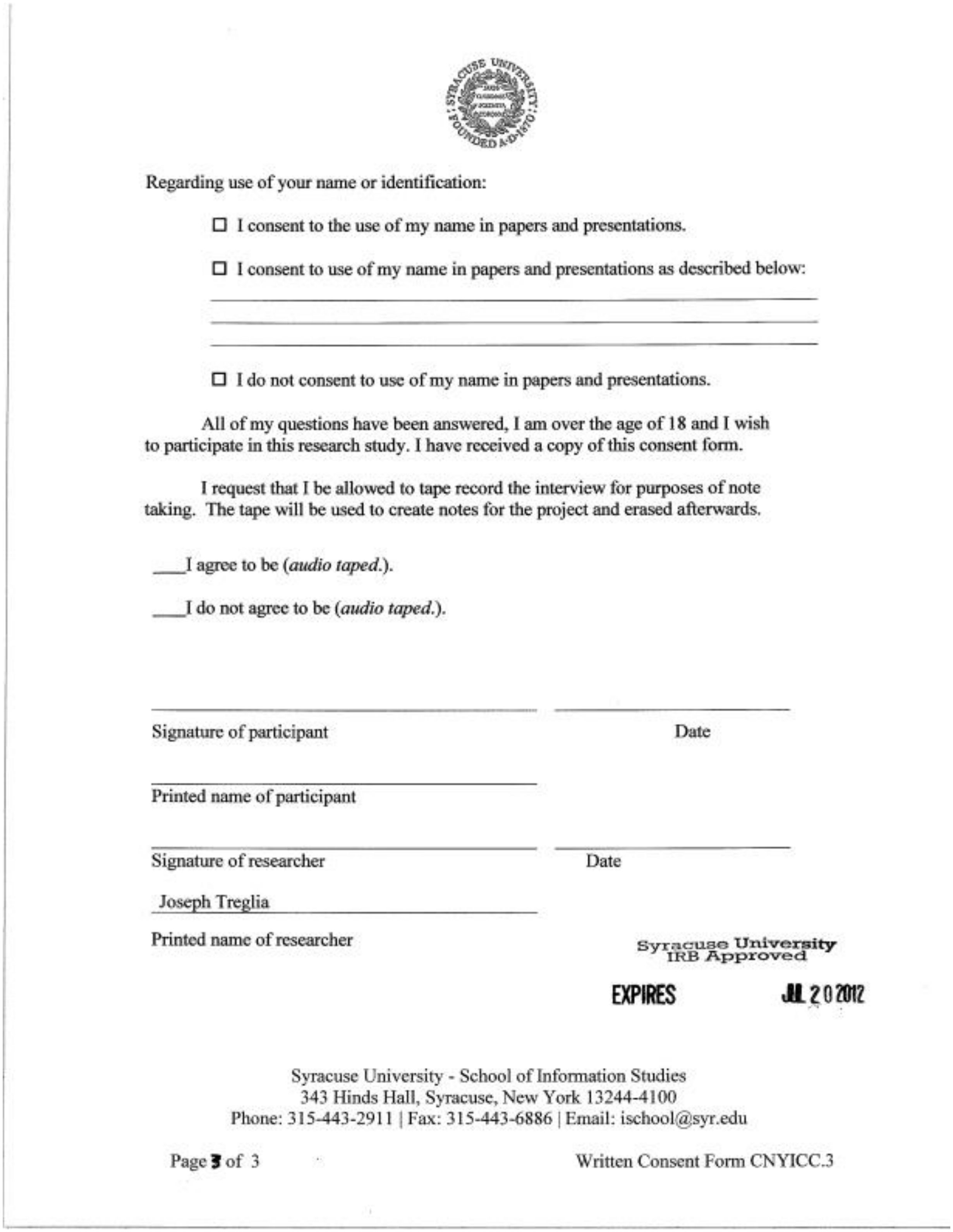
Joseph Treglia, Researcher
Syracuse University
School of Information Studies
245 Hinds Hall
Office: (315) 443-2911
jvtregli@syr.edu

If you have any questions about your rights as a research participant, you have questions, concerns, or complaints that you wish to address to someone other than the investigator, or if you cannot reach the investigator, contact:

The Syracuse University Institutional Review Board at (315) 443-3013.

Syracuse University
IRB Approved

EXPIRES JUL 20 2012



Regarding use of your name or identification:

- □ I consent to the use of my name in papers and presentations.
- □ I consent to use of my name in papers and presentations as described below:

____

____

____

- □ I do not consent to use of my name in papers and presentations.

All of my questions have been answered, I am over the age of 18 and I wish to participate in this research study. I have received a copy of this consent form.

I request that I be allowed to tape record the interview for purposes of note taking. The tape will be used to create notes for the project and erased afterwards.

___I agree to be (*audio taped.*).

___I do not agree to be (*audio taped.*).

______________________________ ______________________

Signature of participant Date

____

Printed name of participant

______________________________ ______________________

Signature of researcher Date

Joseph Treglia

Printed name of researcher

Syracuse University IRB Approved

EXPIRES JUL 20 2012

Syracuse University - School of Information Studies
343 Hinds Hall, Syracuse, New York 13244-4100
Phone: 315-443-2911 | Fax: 315-443-6886 | Email: ischool@syr.edu

Appendix

C. Interview Guide

Interview Protocol (IRB# 11-142): "A case study of Central New York Interoperable Communications Consortium (CNYICC): Identifying Factors that Support Successful Collaboration in Information Technology Implementation."

The goal of the study is to identify information sharing and collaboration barriers as well as facilitating factors. During interviews the goal will be to gather as much data about the person and their understanding of their purpose and activities so that patterns or solutions can be identified. The Interviewer should allow for broad and open ended questions and permit the participants to speak at length and let them move to new directions as well. The expectation is that we will not know all of the potential connections, causes and influences in advance and we will build on these though successive interviews and investigative research.

General Information

   a. Organization
   b. Location
   c. Interviewee or #
   d. Title
   e. Date Interviewed:
   f. Contact Person:
   g. Contact Person Title: Systems Manager

Interview questions guide:

2. Interviewee background
   a. Title
   b. Your background
   c. Describe role/job
   d. Mission
   e. Who do you report to
   f. How long in this position
   g. How long in company/government in this area
   h. Where have you worked previously
   i. Who did you know here prior to your job here
   j. Do you know people here apart from the job

3. Contacts
   a. What internal departments or divisions do you work with daily
   b. """weekly, and why
   c. """monthly, and why
   d. """yearly, and why
   e. """Other than yearly, and why
   f. What outside agencies or organizations do you work with daily
   g. """weekly, and why

- h. """"monthly, and why
- i. """"yearly, and why
- j. """"Other than yearly, and why

4. Stakeholders
   - a. Who are your stakeholders
   - b. Who are the most important stakeholders to you, why
   - c. What do you have to change an internal policy or procedure?

5. Technology architecture
   - a. What Technological means you have for sharing information or collaborating with other internal partners?
   - b. What Technological means you have for sharing information or collaborating with external partners or stakeholders?
   - c. How does Technology help with information sharing?
   - d. How does Technology hinder sharing information?

6. Cultural environment - perceived
   - a. How would you describe the culture of your organization as it related to information sharing?
   - b. What are the positives of this?
   - c. What are negatives of this?
   - d. Is culture something you can affect? How?

7. Policy implications & governance
   - a. What is the operating or organizational framework here?
   - b. How strict is it?
   - c. How does department/agency policy affect information sharing here?
   - d. How do outside laws/regulation affect information sharing here?
   - e. What do you have to change an internal policy or procedure?

8. Competition
   - a. Who competes with you for resources or other things?
   - b. Who do you compete with for resources or other things?
   - c. Does competition for resources affect your decision to share or not share certain information? Describe a case of this?

9. Consortium
   - a. When did you come in to the Consortium?
   - b. How did you come to participate in the consortium?
   - c. What about it is working well?
   - d. What about it is not working so well?
   - e. How do you describe your participation?
   - f. Why do you stay in this?
   - g. What could be done to improve the effectiveness of the Consortium?

For collaboration and information sharing it is important to be able to get information from the right person at the right time. This can be for a task, procedure, to verify information, administrative questions, where or how to request assistance, seeking feedback, advice or general information or opinion on position of where things stand or possible implications of a course of action.

Please list up to 10 people who you contact, formally or informally, to get information. These can be inside or outside the organization and on or off the job, list the most contacted to the least contacted (this does not necessarily reflect importance):

Person - Position - Agency - Type of information or Purpose of Contact

1
2
3
...10

How are these contacts initiated?

1
2
3
...10

You likely serve as a source of information for others; Please list up to 5 people who have contacted you for information, opinion or guidance.

Person - Position - Agency - Type of information or Purpose of Contact

1
2
3
...10

How are these contacts initiated?

1
2
3
...10

Information Sharing: In one-on-one in-depth interviews with this researcher participants will be asked the following base questions, this part focuses on the relationships with law enforcement agencies:

1. Describe a situation or experience where you shared information with a law enforcement agency, and

2. Describe a situation or experience where you did not share information with a law enforcement agency.
3. Repeat 1 & 2 for additional experience or situation.
4. What do you understand information to include?
5. What means does your agency have for sharing information with law enforcement agencies?

Concluding comments

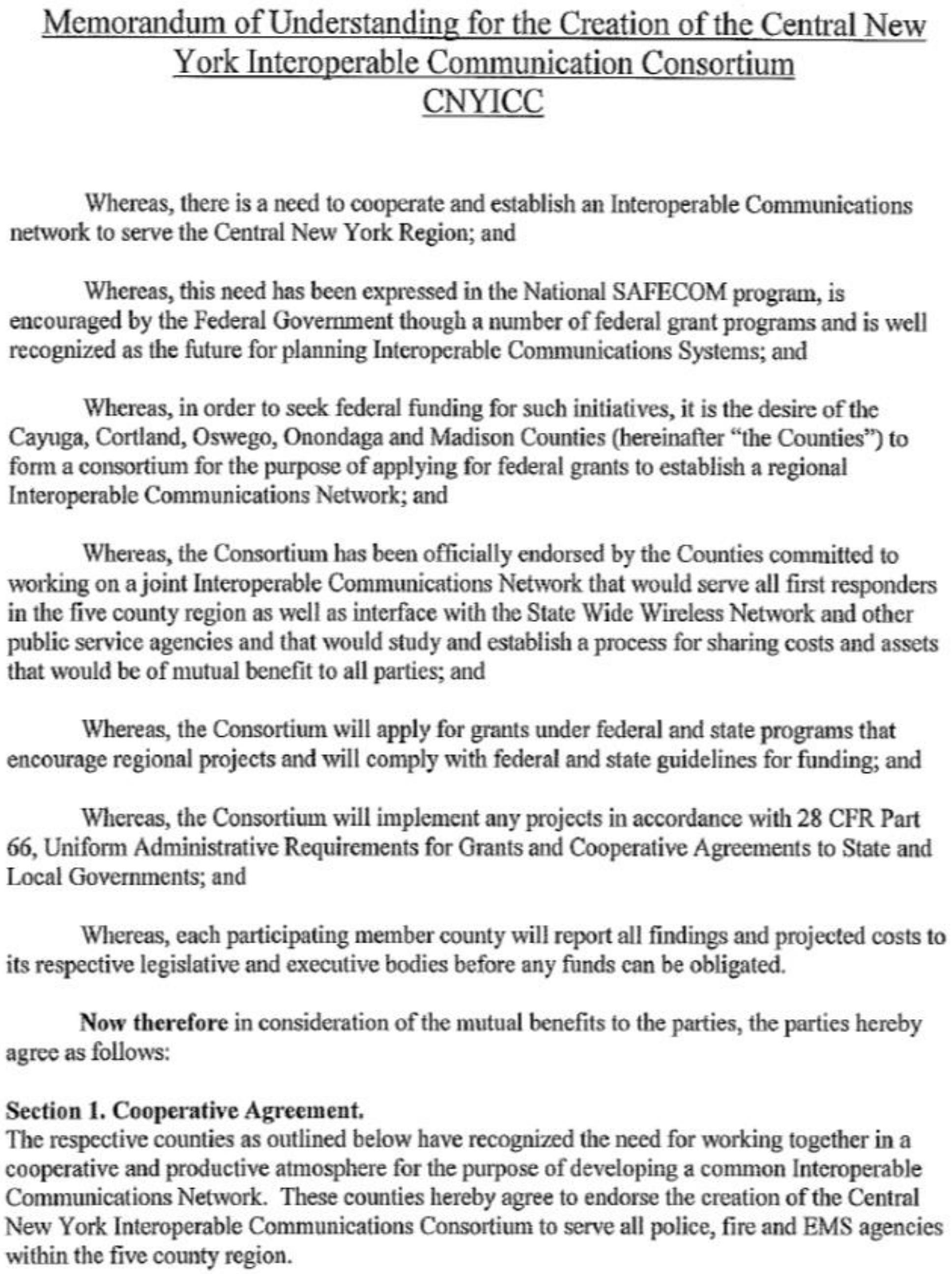
1. We will make our findings public at the end and as milestones are achieved.
2. We may need to return with more questions or for clarification as we learn more.
3. Is there something we can do to help you?

Impressions:

Other Notes:

Appendix

D. MOU for CNYICC



Memorandum of Understanding for the Creation of the Central New York Interoperable Communication Consortium CNYICC

Whereas, there is a need to cooperate and establish an Interoperable Communications network to serve the Central New York Region; and

Whereas, this need has been expressed in the National SAFECOM program, is encouraged by the Federal Government though a number of federal grant programs and is well recognized as the future for planning Interoperable Communications Systems; and

Whereas, in order to seek federal funding for such initiatives, it is the desire of the Cayuga, Cortland, Oswego, Onondaga and Madison Counties (hereinafter "the Counties") to form a consortium for the purpose of applying for federal grants to establish a regional Interoperable Communications Network; and

Whereas, the Consortium has been officially endorsed by the Counties committed to working on a joint Interoperable Communications Network that would serve all first responders in the five county region as well as interface with the State Wide Wireless Network and other public service agencies and that would study and establish a process for sharing costs and assets that would be of mutual benefit to all parties; and

Whereas, the Consortium will apply for grants under federal and state programs that encourage regional projects and will comply with federal and state guidelines for funding; and

Whereas, the Consortium will implement any projects in accordance with 28 CFR Part 66, Uniform Administrative Requirements for Grants and Cooperative Agreements to State and Local Governments; and

Whereas, each participating member county will report all findings and projected costs to its respective legislative and executive bodies before any funds can be obligated.

Now therefore in consideration of the mutual benefits to the parties, the parties hereby agree as follows:

Section 1. Cooperative Agreement.
The respective counties as outlined below have recognized the need for working together in a cooperative and productive atmosphere for the purpose of developing a common Interoperable Communications Network. These counties hereby agree to endorse the creation of the Central New York Interoperable Communications Consortium to serve all police, fire and EMS agencies within the five county region.

Section 2. Effective Date.

The conditions and procedures outlined in this Memorandum of Understanding shall be in full force and effect immediately upon execution of this agreement.

Section 3. Agreements.

The signatures of the following shall effectuate compliance with the terms and conditions of this Memorandum of Understanding.

In witness whereof, the parties have hereunto set their hands and seals as follows:

Onondaga County, by

Nicholas Pirro J.T. Date 11-13-07

Oswego County, by

Date 11/30/07

Madison County, by

Date 12/10/07

Cortland County, by

Marilyn E Brown Date 12/20/07

Cayuga County, by

George C Fearon Date 12 · 20 - 07

Appendix

E. CNYICC Policy & Procedure Proposed

Regional Authority for Coordination and Assignment of Interoperability Assets

The Consortium plans to establish a 24/7 team that is given the authority to assign, coordinate and respond with regional interoperability assets. This team is expected to include operational support, including personnel trained as Communications Unit Leaders (COML), as defined in the National Incident Management System (NIMS) model, as well as technical staff who are familiar with the detailed operation of interoperable equipment. A Regional Interoperability Committee is planned for development and a Regional Communication Coordinator will be assigned as a single point of contact for all agencies within the Consortium's jurisdiction.

Until such time as the Regional Interoperability Committee is developed and a Regional Communications Coordinator is assigned, each agency shall maintain responsibility for its own assets and contact one another's designated agency On Call Duty Officer, as annotated in Appendix xxx, when interoperability assets are requested.

Governance Structure

The Governance structure consists of an Executive Board, Administrative Committee, Operations, Technology, and Long Term Planning Subcommittees, and additional ad-hoc subcommittees including a Grants Subcommittee. An organizational diagram of the structure of the governance body follows:

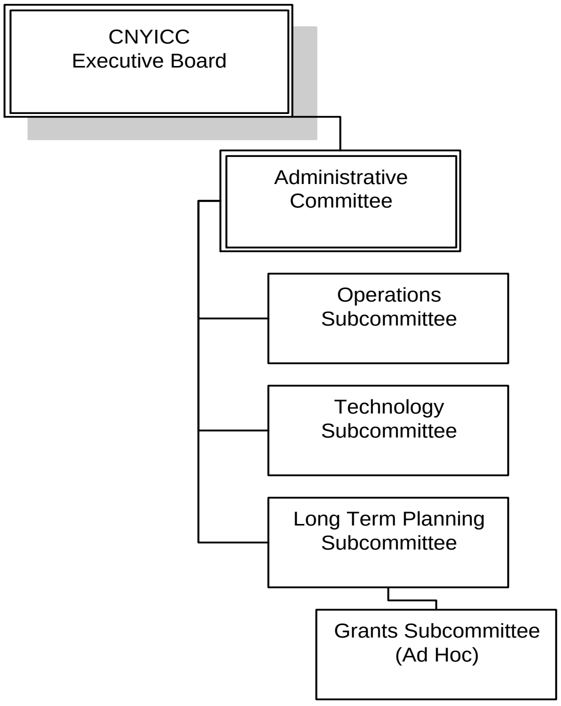


Figure 29: CNYICC Governance Proposed

Agreements regarding position capabilities:

The Executive Board shall consist of one member from each of the five counties and shall be an elected official.

The Administrative Committee shall consist of one member from each of the five counties, at the 911 Director or equivalent level.

Determination and designation of the Executive Board member shall take priority over the designation of the remaining subcommittee members.

A designee from New York State Police shall serve on the Executive Board as an Ad-hoc member, until such time that this position requires a full member position.

The Operations, Technology, and Long Term Planning subcommittees shall report to the Administrative Committee.

The Grants ad-hoc committee shall report to the Long Term Planning subcommittee.

Overall Responsibilities

The responsibilities of the Consortium's Governing body include:

Maintenance and update of the TIC Plan at regular intervals, or as critical updated information is identified.

Dissemination of updated plans to all participating agencies.

Establishment of training requirements in support of the TIC Plan.

Promotion of interoperable communications capabilities through trained communications personnel.

Initialization of Memoranda of Understanding (MOUs) and Agreements for interoperable communications.

Promotion of regular interoperable equipment / solutions testing, assist agencies with test evaluations, and dissemination of the results.

Continual re-evaluation of regional requirements as technology evolves and circumstances dictate.

Executive Board

The Executive Board shall consist of a representative from each Consortium member agency. This ensures that each agency within the region can maintain control over their respective agency operations while meeting the interoperability needs of all local, county and regional agencies. Board Members are appointed by their respective County Governing Body.

Until such time that an Executive Board is established, the Administrative Committee members will report to their respective local County governing body.

The responsibilities of the Executive Board include:

Development and maintenance of a set of Executive Board by-laws governing the Board

Acceptance and action upon requests for assistance from individual county governance boards

Development, maintenance, and recommendations for local County Governing body approval

- a long-term capital budget to enhance regional interoperability
- an annual budget to enhance regional interoperability

Review and action upon Operations and Technology Subcommittee recommendations

Allow for the creation of an advisory committee of peers, representative of the membership which may include state, regional, county, city and local jurisdictions and/or outside disciplines.

- This advisory committee will act in the interest of the Executive Board and will be selected by the membership of the Executive Board, in concert with the Executive Board Director

Member Role

The role of each Board Member is to represent all public safety jurisdictions and agencies within their respective county. This representation, based on County Governing Body approval, requires adequate decision making authority and financial commitment authority to facilitate regional interoperability.

Member Duties

The duties of this position include, but are not limited to:

Conduct its meetings in accordance with Roberts Rules of Order including electing a Chair (Convener) that will preside over the meetings. Other officers may or may not be elected at the discretion of the Board.

Adoption or rejection of governance agreements, operational changes, and technical modifications or enhancements as developed by the Administrative Committee.

Adoption or rejection of Administrative Committee's strategic plans.

Review policy, operational, and cost sharing matters necessary for the operation and maintenance of the Consortium's system

Perform any other responsibilities required to implement the agreed upon MOUs

Each Board Member must designate and name an alternate as a voting member if the Board Member cannot attend an Executive Board Meeting

Support the consensus decisions of the board once adopted by the board.

Member Appointment / Replacement Process

The process for appointing and/or replacing the Executive Board members include:

Executive Board members serve at the request of their County governing body and are reviewed on a biennial basis at the local level

Executive Board members may serve consecutive terms as deemed appropriate by the respective County governing body

Should an Executive Board Member be unable to complete a term in office, it is the responsibility of the appropriate County governing body to fill this vacancy within 90 days. *Note*: This is necessary in order to assure continuity of representation for all public safety jurisdictions / agencies within a county and potential disruption of Executive Board activities.

The Executive Board shall appoint an Executive Director from its membership. The Executive Board Director shall:

- Serve a two year term of office.
- Speak for the whole governance structure and the Consortium.
- Provide the opportunity for a united front (e.g., "one voice") for the governance of the Consortium.

Membership of this board has not yet been determined; once is has been determined, membership will be listed in Appendix A.

Administrative Committee

The Administrative Committee shall consist of a representative from each Consortium member agency. This ensures that each agency within the region can maintain control over their respective operability while meeting the interoperability needs of all local, county, and regional agencies. Committee members are appointed by their respective County Governing Body.

The responsibilities of the Administrative Committee include:

Assuring that the Executive Board is kept informed of all regional activities regarding interoperability and the impact that these activities will have on the CNYICC.

Development, maintenance, and recommendations for approval by the Executive Board:

- A long-term capital budget to enhance regional interoperability
- When appropriate, an annual budget to enhance regional interoperability

Development of strategic plans to

- Ensure regional interoperability, and
- Migration of radio communications assets to a standards-based-shared system-of-systems by 2015.

Review and act upon Operations and Technology Subcommittee recommendations.

Interface with the Syracuse UASI Director to meet Federal and State interoperability requirements.

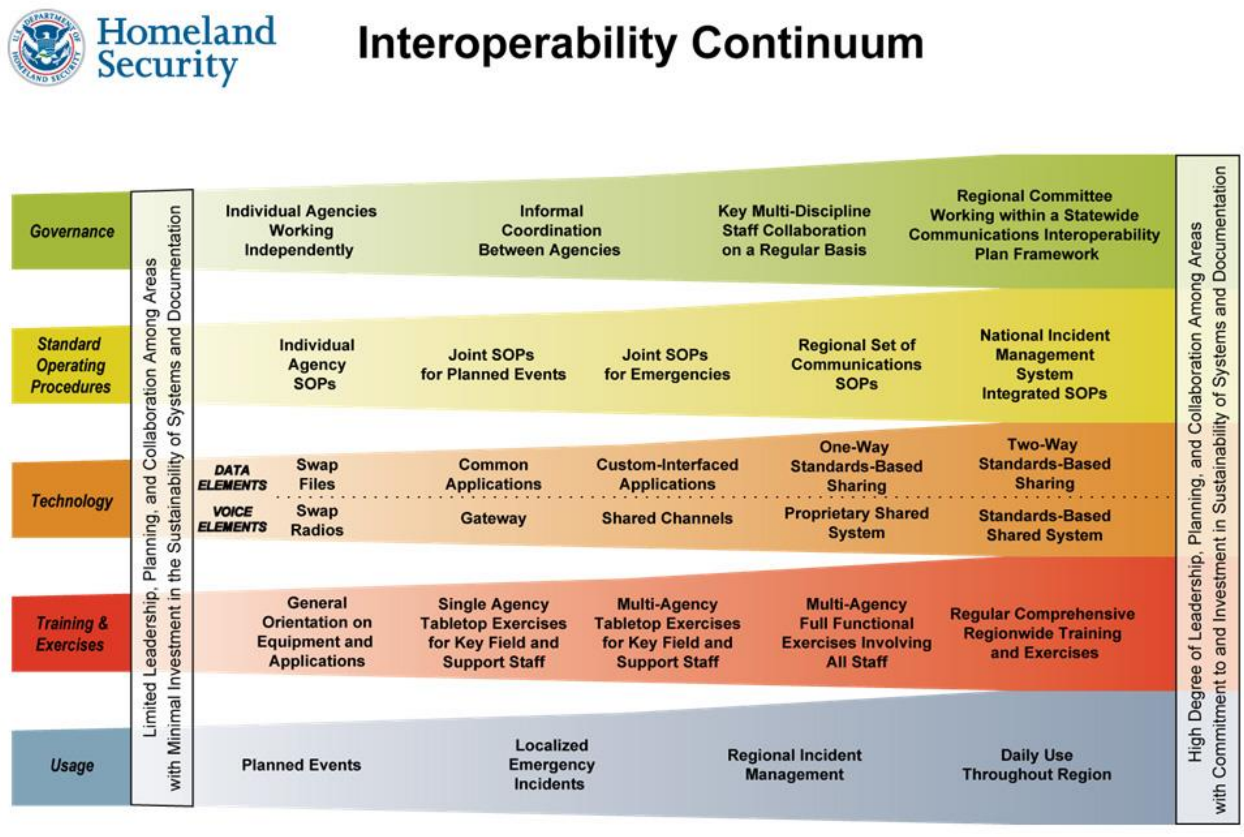
Development of governance agreements that provide supervision in the use of appropriated money, including money from relevant federal homeland security grants, for the purposes of designing, implementing, and maintaining a regional integrated public safety radio communications system that provides interoperability between first responders from local, state, tribal and federal agencies.

Oversight of the development, implementation, and training of personnel using a common regional SOP, consistent with National Incident Management System (NIMS), National Response Framework (NRF) and National Emergency Communications Plan (NECP).

Appendix

F. CNYICC Influence and Relationships

Source:
http://www.ok.gov/homeland/Interoperable_Communications/SAFECOM_Interoperability_Continuum/index.html (11/27/2011)



Homeland Security

Interoperability Continuum

Limited Leadership, Planning, and Collaboration Among Areas with Minimal Investment in the Sustainability of Systems and Documentation

Governance: Individual Agencies Working Independently — Informal Coordination Between Agencies — Key Multi-Discipline Staff Collaboration on a Regular Basis — Regional Committee Working within a Statewide Communications Interoperability Plan Framework

Standard Operating Procedures: Individual Agency SOPs — Joint SOPs for Planned Events — Joint SOPs for Emergencies — Regional Set of Communications SOPs — National Incident Management System Integrated SOPs

Technology:
DATA ELEMENTS: Swap Files — Common Applications — Custom-Interfaced Applications — One-Way Standards-Based Sharing — Two-Way Standards-Based Sharing
VOICE ELEMENTS: Swap Radios — Gateway — Shared Channels — Proprietary Shared System — Standards-Based Shared System

Training & Exercises: General Orientation on Equipment and Applications — Single Agency Tabletop Exercises for Key Field and Support Staff — Multi-Agency Tabletop Exercises for Key Field and Support Staff — Multi-Agency Full Functional Exercises Involving All Staff — Regular Comprehensive Regionwide Training and Exercises

Usage: Planned Events — Localized Emergency Incidents — Regional Incident Management — Daily Use Throughout Region

High Degree of Leadership, Planning, and Collaboration Among Areas with Commitment to and Investment in Sustainability of Systems and Documentation

Figure 30: Interoperability Continuum

The goal is to move from the minimal standards, (left side) of the continuum advancing to the maximum standard (right side) of the continuum.

Appendix

G. Public Safety Communications Evolution

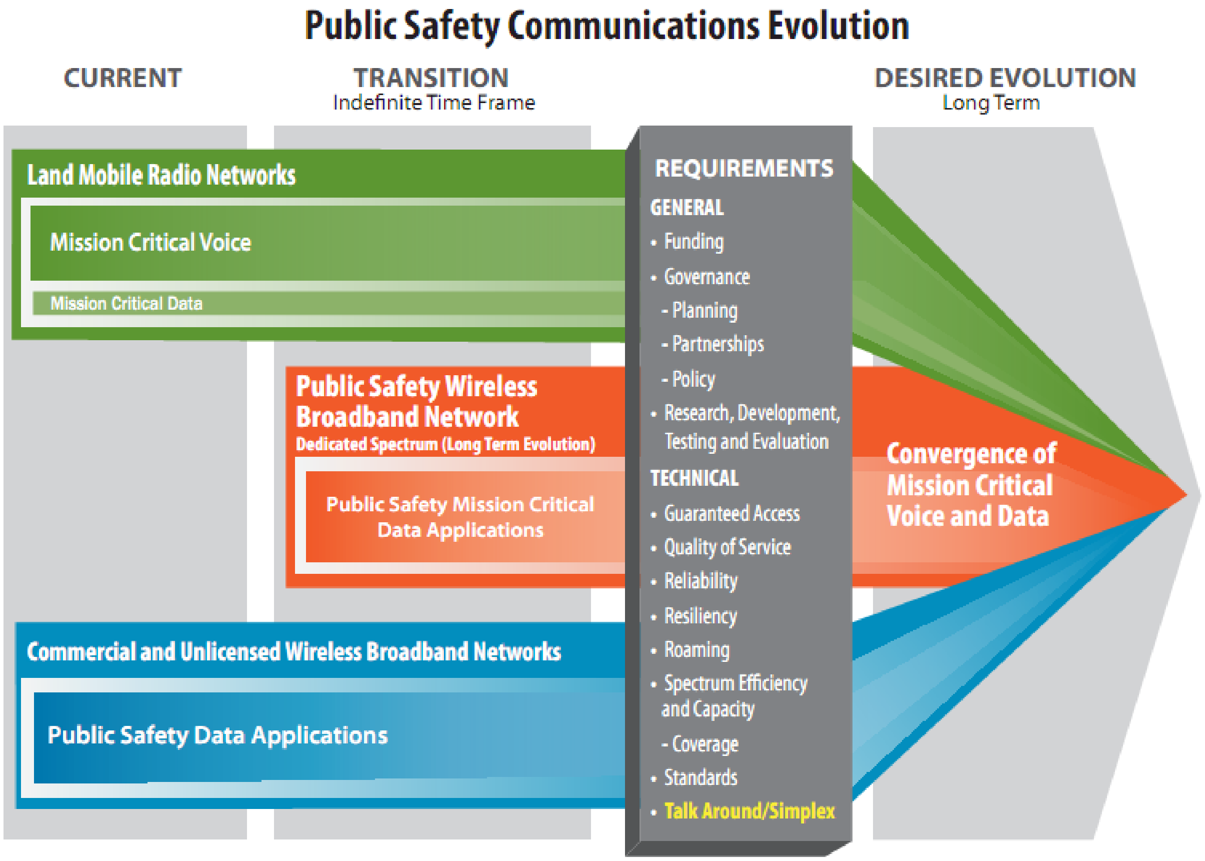

Public Safety Communications Evolution
CURRENT
TRANSITION
Indefinite Time Frame
DESIRED EVOLUTION
Long Term
Land Mobile Radio Networks
Mission Critical Voice
Mission Critical Data
Public Safety Wireless Broadband Network
Dedicated Spectrum (Long Term Evolution)
Public Safety Mission Critical Data Applications
Commercial and Unlicensed Wireless Broadband Networks
Public Safety Data Applications
REQUIREMENTS
GENERAL
• Funding
• Governance
- Planning
- Partnerships
- Policy
• Research, Development, Testing and Evaluation
TECHNICAL
• Guaranteed Access
• Quality of Service
• Reliability
• Resiliency
• Roaming
• Spectrum Efficiency and Capacity
- Coverage
• Standards
• Talk Around/Simplex
Convergence of Mission Critical Voice and Data

Figure 31: Public Safety Communications Evolution

Public safety communications evolution with long-term transition to convergence of systems (from NYS DHSES, 2011)

Appendix

H. Events and Activities Impacting CNYICC

Table 9: Events and Activities Impacting CNYICC

Date	*Federal Level Event*	*State Level Event*	*Local Level Event*	*Description*
1982	National Emergency Number Association (NENA)		CNYICC members all participate here	NENA's Mission is to foster the technological advancement, availability and implementation of a universal emergency 911 number system; NENA is widely recognized as a standard-setting organization; with more than 7,000 members in 48 chapters in the United States and internationally
1989	Project 25 (P25 or APCO-25) initiated			Suite of standards for digital radio communications by federal, state/province and local public safety agencies to enable interoperable communication with other emergency response agencies produced by the Association of Public Safety Communications Officials International (APCO), the National Association of State Telecommunications Directors (NASTD), selected Federal Agencies and the National Communications System (NCS). The published P25 standards suite is administered by the Telecommunications Industry Association (TIA Mobile and Personal Private Radio Standards Committee TR-8). Compliance was limited until it was tied to federal funding requests in 2007.
1991		911 Wireless Surcharge imposed	Counties not getting proposed revenues as anticipated	NYS Government imposes surcharge on all cell phones to fund local public safety communication costs; over $40 million annually with only small percentage to purpose.
1995	Project 25 - Phase I Completed			Defined the common air interface standard, which specified an FDMA access method, QPSK-C modulation, 9.6 kb/s data rate and DVSI vocoder

				with 12.5 KHz channel.
2001		Statewide Wireless Network (SWN) RFP initiated		In May 2001, NYS Office For Technology (OFT) announces intention to seek “competitive bids for estimated $300 million project to construct a statewide wireless communications system.” Advance notice of future release of SWN request for proposals (RFP) printed in Procurement Opportunities Newsletter/Contract Reporter, May 13, 2002.
2001	9/11 Terrorist Attack in US	9/11 Terrorist Attack in US	9/11 Terrorist Attack in US	Terrorists attack World Trade Center in NYC, the Pentagon in Arlington, Va. and an unconfirmed target in Washington, D.C.; lack of interoperable communication was an issue.
2003	Next Generation 911 (NG9-1-1 or NG911)	Next Generation 911 (NG9-1-1 or NG911)	Next Generation 911 (NG9-1-1 or NG911)	NINA supported National Initiative to enable public to transmit text, images, video and data to the 9-1-1 centers; published in NENA's Future Path Plan in 2001
2004	Narrowbanding Land Mobile Radio (LMR) ordered by FCC			FCC issues order issued mandating business, education, industrial, public safety, state and local governments VHF (150-174 MHz) and UHF (421-512 MHz) Private Land Mobile Radio (PLMR) licensees to change to narrowband (12.5 kHz bandwidth) systems by January 1, 2013.
2005	National Incident Management System (NIMS) use mandated by Presidential Directive	States adopt same		National Incident Management System (NIMS); Homeland Security Presidential Directive 5 (HSPD5) mandated all federal, state, and local agencies use NIMS for emergencies to receive federal funding. (Began with Federal Agencies in 2003)
2005	Incident Command System (ICS) use mandated by Presidential Directive	States adopt same		ICS is a subcomponent of the National Incident Management System (NIMS); Homeland Security Presidential Directive 5 (HSPD5) mandated all federal, state, and local agencies use NIMS for emergencies to receive federal funding.

2005	SAFECOM – Interoperability Continuum			SAFECOM program of Department of Homeland Security's OEC and OIC does planning, guidance, and policy documents including the Interoperability Continuum adopted as an organizing structure for DHS G&T's TIC Plan & required for funding.
2005	Hurricane Katrina	Hurricane Katrina	Hurricane Katrina	Hurricane Katrina struck the U.S. Gulf Coast destroying towns in Mississippi and Louisiana displacing millions; responder communication was inadequate
2005		Statewide Wireless Network (SWN) initiated		Statewide Wireless Network (SWN) is an effort to replace obsolete communications infrastructure in New York State with an integrated statewide radio network for State and local public safety and public service organizations.
2006			**CNYICC Discussions Initiated**	911 Directors meet at 911 association events and propose working together as consortium for benefit of all.
2006	Next Generation 911 (NG9-1-1 or NG911)			US Department of Transportation leads an initiative; research and development project to advance NG9-1-1
2007		Statewide Wireless Network (SWN) reporting required		State Technology Law section 403 enacted, creating new annual reporting requirements for costs associated with participation in SWN. State agency and public benefit corporations required to submit SWN-related expenditures to Office of the State Comptroller (OSC) by January 30, 2008
2007	Project 25 compliance verification from vendor required			2007 SAFECOM federal grant guidance recommends applicants using funds for Project 25 equipment must verify product's compliance by manufacturer.
2007			**CNYICC Formally Created (MOU)**	Central New York Interoperable Communications Consortium (CNYICC) formally created by Memorandum of Understanding (MOU) between five central New York

				counties; Cayuga, Cortland, Madison, Onondaga and Oswego
2008	The National Emergency Communications Plan (NECP)			US DHS release National Emergency Communications Plan (NECP) to improve emergency response communications; defining three goals that establish minimum levels of interoperable communications with a deadline for federal, state, local and tribal authorities' compliance attached to grants.
2009		Statewide Wireless Network (SWN) Cancelled		New York cancels the state's $2.1 billion contract to build a statewide wireless network for emergency workers following years of delays and technological problems
2009		Project 25 (P25) standards included at state level		Compliance with Project 25 standards is recommended; this is included in State Communications interoperability plan
2010			CNYICC Core Membership Change	A core founding leadership member of CNYICC left service and new member joined.
2010		911 landline Surcharge and Mortgage recording tax blocked by State		Additional mortgage recording tax and new fees for wireless and landline phones are proposed by counties to support 911 system upgrades and interoperability; denied by state legislature.
2011			911 landline Surcharge and Mortgage recording tax adopted by counties	Additional mortgage recording tax and new fees for wireless and landline phones are proposed by counties to support 911 system upgrades and interoperability; denied by state legislature.

Source: (Treglia, 2012)

Appendix

I. External Factors Impacting CNYICC

I.1 Statewide Wireless Network (SWN)

The New York State Statewide Wireless Network (SWN) was a project to replace the obsolete emergency communications infrastructure across the State. The goal was to implement a statewide mobile radio network for public safety and public service agencies. The SWN was to provide interoperable, interagency and intergovernmental communications allowing emergency personnel to communicate with one another. Local governments were allowed to opt into the system, but had to purchase their own equipment to do so. Control and governance of the system was in the hands of the State Office of Technology. The need for improved radio systems was apparent since 1996; however, interest in interoperable emergency communications systems heightened in the aftermath of September 11, 2001 (OSC, 2006).

The State attempted to form agreements with private firms to develop such a network unsuccessfully two times before initiating a competitive process to select vendor in 2002. The communications network, projected to cost $2 billion, would be the largest IT project undertaken in the state's history. The State Office for Technology awarded the contract to M/A-COM Inc. (Tyco Electronics), in April 2004. In September 2005, the Office for Technology (OFT) completed a lease purchase agreement contract to M/A-COM to design and build the SWN. New York State went on to spend over $100 million towards developing the statewide wireless network it hoped would provide public safety and public service agencies with interoperable communications statewide, only to have this effort fail. Following problems in several rounds of testing, the state officially terminated the contract with M/A-COM in January of 2009 for failing to deliver a satisfactory and acceptable public safety communications network (McKenna, 2009; Mayberry-Stewart, 2008).

I.2 Project 25 (P-25)

The U.S. Department of Commerce Public Safety Communications Research P25 project is a user-driven effort to create a suite of standards for digital land-mobile radio (LMR) systems for first responders. By design, practitioners participate in the standards development process alongside LMR manufacturers. The P25 began in 1989 to enable public safety agencies to communicate with each other, regardless of system manufacturer. It is the only open voluntary consensus standards development group focused on digital LMR communications for first responders (PSCR, 2011). Open standards in TIA TR-8/Project 25 define how LMR devices operate, and how key system interface standards can allow radios and infrastructure from various manufacturers to interoperate. This standards development process for congressionally mandated interoperability interfaces promotes more vendor solutions being created and offered. The PSCR, Public Safety Communications Research Program, ensures that public safety's technical needs are accurately represented with the commercial vendors and in P25 (PSCR, 2011).

I.3 Next Generation 911 (NG911)

Present day 911 systems in the United States were designed around telephone technology and cannot handle text, data, images, or video. Smart phones, computers, and other intelligent hand held devices are increasingly common in society and engagement with them by public safety communications systems will be essential. The Next Generation 911 (NG911) initiative is establishing a strategic foundation for public safety emergency communications services in a networked wireless mobile society. The concept of next generation 9-1-1 involves standardizing the technology underlying various 911 systems across the nation, using IP technology and Internet-based communication links, which will allow for greater access to databases of information to manage incidents and handle calls. Interconnecting the 911 Centers to allow unlimited transfers of calls, distribution of overflow 911 calls to other centers, and other call-handling features has been a long-standing goal. Having capability for the 911 systems to accept alternate multi-media information from citizens, including video, photos, and text messages is also part of this conceptualization. Additional advances include interconnecting with private services, such as for telematics, to handle automatic crash notification (ACN) and similar data. A final layer would include advanced features such as automatic routing for languages, mapping, and medical information access (USDOT, 2011).

It should be recognized that current E911 systems no longer meet user needs. The Next Generation 911 (NG911) networks will replace existing narrowband, circuit switched 911 networks, which do not support text messages, images and video, file transfer, and ready access to data such as telematics, building plans and medical records over common data networks. NG911 is a comprehensive system comprised of hardware, software, data and policies and procedures to (NENA, 2009):

- provide standardized interfaces from call and message services
- process all types of emergency calls including non-voice (multi-media) messages
- acquire and integrate additional data useful to call routing and handling
- deliver the calls/messages and data to the appropriate PSAPs and other appropriate emergency entities
- support data and communications needs for coordinated incident response and management
- provide a secure environment for emergency communications

NG911 can enable substantial improvements in available data and information sharing. The NG911 operates as a service system that involves a multitude of human procedures and system operations to control and manage additional services. Examples of this include establishment and maintenance of databases, IP network operations, security, trouble resolution, and auditing and validation procedures. Still, a true "standards based" NG911 system is not yet available as necessary standards are still being developed. National public safety organizations such as NENA (National Emergency Number Association) work to identify and promote the use of these standards in the field.

I.4 National Emergency Number Association (NENA)

NENA is an organization chartered to represent public safety and the 911 industry nationally. It is comprised of 911 Administrators from across the country. Its mission is to focus on development, evolution, and expansion of emergency communications and standards. They advise congress and the FCC on policy matters. NENA is responsible to define NG911, and to coordinate development and support of this as a system and service to the public, industry, and Public Safety entities generally (NENA, 2009).

I.5 SAFECOM

SAFECOM is a communications program of the Department of Homeland Security (DHS) established in 2001 by the Office of Management and Budget (OMB). SAFECOM provides research, development, testing, evaluation, guidance, tools, and templates regarding issues of interoperable communications to federal, state, local, and tribal emergency response agencies. SAFECOM is an emergency communications program of the Department of Homeland Security's Office of Emergency Communications (OEC) and Office for Interoperability and

Compatibility (OIC). SAFECOM is stakeholder driven, led by an Executive Committee comprised of state and local emergency responders, intergovernmental and national public safety communications associations. The SAFECOM Executive Committee (EC) and SAFECOM Emergency Response Council (ERC) both work with Federal communications programs and key emergency response stakeholders to address problems in multi-jurisdictional and cross-disciplinary resource coordination and communications (SAFECOM, 2011). SAFECOM was instrumental in creating the Interoperability Continuum (IC), the Statement of Requirements (SOR), the Statewide Communication Interoperability Plan (SCIP) Methodology, and the National Emergency Communications Plan (NECP) to improve communications and interoperability for emergency responder's nation-wide. The SAFECOM interoperability continuum is shown in the appendix. The Interoperability Continuum was designed as a tool to help emergency responders plan and implement interoperability solutions to include: governance, standard operating procedures, technology, training and exercises, and use of interoperable communications. The tool aids practitioners and policy makers assess and implement facets of both short- and long-term interoperability.

I.6 The National Emergency Communications Plan (NECP)

The National Emergency Communications Plan (NECP), established in 2008, was the first strategic plan for improving emergency response communications in the United States, complimenting homeland security and emergency communications legislation and activities, including Statewide Communication Interoperability Plans. NECP was created by the U.S. Department of Homeland Security's Office of Emergency Communications. The NECP sets common goals and priorities expected to enhance governance, planning, technology, training, exercises, and emergency response communication capabilities, and includes milestones to allow measurement of progress and improvements in emergency communications with a focus on operational aspects. The recommendations are meant to guide, but do not dictate, distribution of homeland security funds to assist authorities who implement the plan. The plan seeks to achieve compliance by all agencies with the guidance by 2013 (DHS NECP, 2011).

I.7 National Incident Management System (NIMS)

The National Incident Management System (NIMS) is a standardized model for command and control of emergency or crisis incidents proposed by the Federal Government in 2003. The present-day version provides for shared command structure and acknowledges stakeholder autonomy over data and resources. It was created through Homeland Security Presidential Directive Number Five (5). NIMS is a comprehensive national framework for incident management and New York State adopted the model as the State‘s command and control policy for use in coordinating the State‘s response to emergencies. NIMS enables responders at various levels to work together to manage crisis incidents of large and small scale size, or complexity (FEMA NIMS, 2011).

I.8 Incident Command System (ICS)

Related to NIMS is the Incident Command Structure (ICS). ICS more specifically describes the command and control structure and hierarchy for managing and coordinating resources at an incident. The common understanding of defined roles and responsibilities allows for more effective and efficient operations where multiple agencies are involved.

I.9 Narrowbanding

On January 1, 2013, public safety and business industrial land mobile radio (LMR) systems operating in the 150-512 MHz radio bands must begin operating using at least 12.5 kHz efficiency technology. This mandate and deadline is the result of an FCC effort from nearly two decades ago to ensure more efficient use of spectrum and provide for greater spectrum access for public safety and non-public safety users (FCC, 2011; RadioReference.com, 2011). Migration to the 12.5 kHz efficiency previously referred to as “refarming” and now “Narrowbanding” allows for the creation of additional channel capacity within the existing radio spectrum, supporting more total users. Each of these refers to the 1992 FCC plan to increase available spectrum in the VHF and UHF private land mobile bands. After January 1, 2013, licensees not operating at 12.5 KHz efficiency will be considered in violation of the FCC rules and could face enforcement action such as admonishment, fines, or loss of spectrum license.

VII. REFERENCES (CUMULATIVE)

44 USC § 3542(b)(1)

Abbott, A. (1988). *The system of professions: An essay on the division of expert labor*. University of Chicago Press.

Ackoff, R. L. (1971). Towards a system of systems concepts. *Management Science*, 17(11), 661-671.

Adam, N., Atluri, V., Chun, S., Ellenberger, J., Shafiq, B., Vaidya, J., & Xiong, H. (2008). "Secure information sharing and analysis for effective emergency management." In *Digital Government Society of North America*, 407-408. Montreal, Canada.

Agranoff, R., & McGuire, M. (2001). American federalism and the search for models of management. *Public Administration Review*, 61(6), 671−682.

Aiken, M., & Hage, J. (1966). "Organizational Alienation: A Comparative Analysis," *American Sociological Review*, 31 (August), p. 499.

Akbulut, A. (2003). An investigation of the factors that influence electronic information sharing between state and local agencies. Louisiana State University, Baton Rouge, LA. June 20. Retrieved from http://etd.lsu.edu/docs/available/etd-0619103-214616/

Akbulut, A., Kelle, P., Pawlowski, S., Schneider, H., & Looney, C. (2009). To share or not to share? Examining the factors influencing local agency electronic information sharing. *International Journal of Business Information Systems* 4, no. 2: 143 - 172. doi:10.1504/IJBIS.2009.022821.

Akerlof, G. A. (1970). The market for" lemons": Quality uncertainty and the market mechanism. *The quarterly journal of economics*, 84(3), 488-500.

Allen, M., Balloni, J., Hartnett, P., & Stayton, D. (2007). Memorandum of Understanding (MOU) for the creation of the Central New York Interoperable Communications Consortium (CNYICC).

Alter, S. (1999). A general, yet useful theory of information systems. *Communications of the AIS*, 1(3es), 3.

Angell, I. O., & Smithson, S. (1991). *Information Systems Management: Opportunity and Risk*. Palgrave Macmillan.

Argote, L., & Ingram, P. (2000). Knowledge Transfer: A Basis for Competitive Advantage in Firms. *Organizational Behavior and Human Decision Processes,* 82(1), 150-169. doi:06/obhd.2000.2893

Argote, L., McEvily, B., & Reagans, R. (2003). Managing knowledge in organizations: An integrative framework and review of emerging themes. *Management Science*, 49(4), 571-582. doi:Article

Ariño, A, & Reuer, J. J. (2006). *Strategic Alliances: Governance and Contracts*. Palgrave Macmillan.

Astley, W. G., & Van de Ven, A. H. (1983). Central perspectives and debates in organizational theory. *Administrative Science Quarterly* 28: 245–73.

Atabakhsh, H., Larson, C., Petersen, T., Violette, C., & Chen, H. (2004). Information sharing and collaboration policies within government agencies. *Lecture notes in computer science*, Vol. 3073/2004. (pp. 467-475)Springer: Berlin and Heidelberg.

Axelrod, R. (1981). The emergence of cooperation among egoists. *The American Political Science Review*, 306–318.

Axelrod, R. (1986). An evolutionary approach to norms. *The American Political Science Review*, 1095–1111.

Axelrod, R. M. (1997). *The complexity of cooperation: Agent-based models of competition and collaboration*. Princeton Univ Pr.

Axelrod, R., & Hamilton, W. D. (1981). The evolution of cooperation. *Science*, *211*(4489), 1390–1396.

Axelrod, R., & Keohane, R. O. (1985). Achieving cooperation under anarchy: Strategies and institutions. *World Politics*, *38*(1), 226–254.

Bardach, E. (2001). Developmental dynamics: Interagency collaboration as an emergent phenomenon. *Journal of Public Administration Research and Theory*, 11(2), 149−164.

Barley, S. R. (1990). The alignment of technology and structure through roles and networks. *Administrative Science Quarterly*, 35(1), 61-103.

Barr, J. L., Peddicord, A. M. ., Burtner, E. R., & Mahy, H. A. (2011). Current Domain Challenges in the Emergency Response Community. *Proceedings of the 8th International ISCRAM Conference–Lisbon* (Vol. 1).

Barron, D. J. (2003). Reclaiming home rule. *Harvard Law Review*, 2255–2386.

Benamati, J., Serva, M. A., & Fuller, M. A. (2006). Are Trust and Distrust Distinct Constructs? An Empirical Study of the Effects of Trust and Distrust among Online Banking Users. *System Sciences, 2006. HICSS ’06. Proceedings of the 39th Annual Hawaii*

International Conference on (Vol. 6, p. 121b). Presented at the System Sciences, 2006. HICSS '06. Proceedings of the 39th Annual Hawaii International Conference on.

Benbasat, I., Goldstein, D. K., & Mead, M. (1987). The case research strategy in studies of information systems. *MIS Quarterly*, 11(3), 369-386.

Ben-Ner, A., & Putterman, L. (2002). *Trust in the New Economy1* (HRRI Working Paper) (p. 36). Minnesota, US: Industrial Relations Center, University of Minnesota.

Bharati, P., & Chaudhury, A. (2004). An empirical investigation of decision-making satisfaction in web-based decision support systems. *Decis. Support Syst*., 37(2), 187-197.

Bijker, W. (1997). *Of Bicycles, Bakelites, and Bulbs: Toward a Theory of Sociotechnical Change (Inside Technology).* The MIT Press.

Binmore, K., & Dasgupta, P. (1986). Game theory: a survey. In K. Binmore and P. Dasgupta (eds), *Economic Organizations as Games*, Oxford: Basil Blackwell.

Birje, M. N., & Manvi, S. S. (2011). "An Efficient Method of Sharing Device Resource Status in Wireless Grids." *Multiagent and Grid Systems* 7, no. 4: 127–146.

Birje, M., & Manvi, S. (2010). "Monitoring and Status Representation of Devices in Wireless Grids." *Advances in Grid and Pervasive Computing*: 341–352.

BJS. (2007). *US Department of Justice, Bureau of Justice Statistics (BJS) Law Enforcement Statistics, August 8, 2007*. Retrieved May 9, 2008, from http://www.ojp.usdoj.gov/bjs/lawenf.htm.

BJS. (2011). US Department of Justice, Bureau of Justice Statistics (BJS). *Census of State and Local Law Enforcement Agencies, 2008*. July 26, 2011, NCJ 233982. http://bjs.ojp.usdoj.gov/index.cfm?ty=pbdetail&iid=2216

Blaikie, N. W. H. (1991). A critique of the use of triangulation in social research. *Quality and Quantity*, 25(2), 115-136. doi:10.1007/BF00145701

Blair, M. M., & Stout, L. A. (2001). Trust, trustworthiness, and the behavioral foundations of corporate law. *University of Pennsylvania Law Review*, 149(6), 1735-1810.

Bonoma, T. V. (1985). Case research in marketing: Opportunities, problems, and a process. *Journal of Marketing Research*, 22(2), 199-208.

Boon, S. D., & Holmes, J. G. (1991). The dynamics of interpersonal trust: Resolving uncertainty in the face of risk. In Hinde, R. A., & Groebel, J. (Eds.), *Cooperation and* *prosocial behavior.* Cambridge [England]; New York: Cambridge University Press, pp. 190–211.

Booth, K., & Wheeler, N. (2007). *Security dilemma: Fear, cooperation, and trust in world politics (First Edition.).* Palgrave Macmillan.

Bostrom, R. P., & Heinen, J. S., (1977). MIS problems and failures: A socio-technical perspective, *MIS Quarterly*, Vol. 1, No. 3, pp. 17-32

Botterell, A., & Addams-Moring, R. (2007). "Public warning in the networked age: open standards to the rescue?," *Commun. ACM*, 50, no. 3: 59-60.

Brafman, O., & Beckstrom, R. (2006). *The starfish and the spider: The unstoppable power of leaderless organizations*. Portfolio.

Brafman, O., & Beckstrom, R. (2008). *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations*. Portfolio.

Braman, S. (2008). Policy Research in an Evidence-Averse Environment. International Journal of Communication, 2, 433-449.

Brooks, T., Caicedo, C., & Park, J. (2012). Security challenges and countermeasures for trusted virtualized computing environments. *Internet Security (WorldCIS), 2012 World Congress on* (pp. 117–122). IEEE.

Caicedo, C. E. (2007). Software Defined Radio and Software Radio Technology: Concepts and Applications. *In proceeding of: International Telecommunications Research and Education Association ITERA*. 01/2007.

Bührs, T., & Bartlett, R. V. (1993). *Environmental policy in New Zealand: the politics of clean and green?* Oxford University Press Auckland.

Bulman, P. (2008). Communicating across state and county Lines: The Piedmont Regional Voice over Internet Protocol Project. *NIJ Journal*, 261. Retrieved February 22, 2009, from http://www.ojp.usdoj.gov/nij/journals/261/piedmont- voip.htm.

Burd, S. A., Cherkin, S. S., & Concannon, J. (2005). Information security in academic institutions: Emerging issues and remediation strategies. *Journal of Security Education*, 1(2), 55-68.

Business Wire. (2010). "Wireless innovation forum makes recommendation on the evolution of the SCA, Business Wire," Feb. 18, 2010. http://www.businesswire.com/news/home/20100218006690/en/Wireless-Innovation-Forum-Recommendation-Evolution-SCA. Accessed April 25, 2011.

Butterfield, F. (2009). F.B.I. agent linked to mob is guilty of corruption - New York Times. New York Times. February 22. Retrieved from http://query.nytimes.com/gst/fullpage.html?res=9407EFDB113BF93AA15756C0A9649C8B63 & sec= & spon= & pagewanted=all

Campbell, D. T. (1975). Degrees of freedom and the case study. *Comparative Political Studies*, 8(1), 178-191.

Canestraro, D. S., Pardo, T. A., Raup-Kounovsky, A. N., & Taratus, D. (2009). Regional telecommunication incident coordination: Sharing information for rapid response. *Information Polity*, 14(1), 113-126.

Cannon, J. P., & Homburg, C. (2001). Buyer-supplier relationships and customer firm costs. *The Journal of Marketing*, 29–43.

Cant, S., & Sharma, U. (1995). “The reluctant profession-homoeopathy and the search for legitimacy.” *Work, employment & society* 9(4):743.

Carter, D. L., & United States. (2004). *Law enforcement intelligence a guide for state, local, and tribal law enforcement agencies*. Washington, D.C.: U.S. Dept. of Justice, Office of Community Oriented Policing Services.

Carter, D. L. (2005). “Brief history of law enforcement intelligence: Past practice and recommendations for change.” *Trends in Organized Crime* 8(3):51-62. Retrieved February 15, 2008.

Cash, J. I., Jr., & Konsynski, B. R. (1985). IS redraws competitive boundaries. *Harvard Business Review*, 134−142.March–April.

Cater-Steel, A., & Al-Hakim, L. (2009). *Information Systems Research Methods, Epistemology, and Applications*. Idea Group Inc (IGI).

Center for Strategic and International Studies. (1998). *Wild atom: nuclear terrorism--Global Organized Crime Project*. Washington, DC: [s.n.].

Chakraborty, S., & Ray, I. (2006). Trust BAC: Integrating trust relationships into the RBAC model for access control in open systems. In Proceedings of the 11th ACM Symposium on Access Control Models and Technologies, Lake Tahoe, CA, June 2006.

Chan, H. C., & Teo, H. (2007). Evaluating the boundary conditions of the technology acceptance model: An exploratory investigation. *ACM Trans. Comput.-Hum. Interact.*, 14(2), 9. doi: 10.1145/1275511.1275515.

Charlton, J. R. H. (2004). “Delphi Technique.” In *The Sage encyclopedia of social science research methods*, edited by Michael S. Lewis, Alan Bryman, and Tim Futing Liao. Thousand Oaks Calif.: SAGE.

Chau, M., Atababhsh, H., Zeng, D., & Chen, H. (2002). *Building an infrastructure for law enforcement information sharing and collaboration: Design issues and challenges*. National Science Foundation. Retrieved February 4, 2008, from http://dlist.sir.arizona.edu/473/01/chau4.pdf.

Checkland, P. (1981). *Systems thinking, systems practice*. J. Wiley.

Checkland, P. (2000). Soft systems methodology: a thirty year retrospective. *Systems Research*, 17.

Checkland, P., & Scholes, J. (1999). *Soft Systems Methodology in Action* (New Sub.). Wiley.

Chen, H., Zeng, D., Atabakhsh, H., Wyzga, W., & Schroeder, J. (2003). COPLINK: managing law enforcement data and knowledge. *Communications of the ACM*, 46(1), 28-34.

Chen, H., Dacier, M., Moens, M. F., Paass, G., & Yang, C. C. (2009). Proceedings of the ACM SIGKDD Workshop on CyberSecurity and Intelligence Informatics. *ACM*.

Chen, Q. (2009). *Cognitive gateway design to promote interoperability, coverage, and throughput in heterogeneous communications systems*. PhD dissertation, Department of Electrical and Computer Engineering, Virginia Tech, Blacksburg, Virginia.

Chen, X., Newman, T. R., Datla, D., Bose, T., & Reed, J. H. (2009). The impact of channel variations on wireless distributed computing networks. Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE (pp. 1-6). *IEEE*.

Cherns, A., (1976), The principles of sociotechnical design, *Human Relations*, Vol. 29, No. 8, pp. 783-792.

Cherns, A., (1987), Principles of Sociotechnical Design Revisited, *Human Relations*, Vol. 40, No. 3, pp. 153-162.

Choudrie, J., & Dwivedi, Y. K. (2005). Investigating the research approaches for examining technology adoption issues. *Journal of Research Practice*, 1(1), D1.

Churchman, C. W. (1979). *The Systems Approach* (revised and updated) New York: Dell Publishing.

Ciborra, C. (2002). *The labyrinths of information: challenging the wisdom of systems*. Oxford University Press, USA.

Clark, J. (2008), Remarks by director John Clark at the operation orange crush press conference, September 18. 2008. USMarshals.gov. Government Agency. Retrieved November 27, 2008, from http://www.usmarshals.gov/news/chron/2008/091808.htm.

Clark, J.P. (1965). “Isolation of the Police: A Comparison of the British and American Situations.” *Journal of Criminal Law, Criminology and Police Science* 56:307.

Cohen, G. A. (2000). Karl Marx’s theory of history: a defence. Oxford Univ Press.

Collins, R. (1979). The Credential society: An historical sociology of education and stratification. Academic Press (New York).

Colquitt, J. A., Scott, B. A., & LePine, J. A. (2007). Trust, trustworthiness, and trust propensity: A meta-analytic test of their unique relationships with risk taking and job performance. Journal of Applied Psychology, 92(4), 909-926.

Colvin, C. A., & Goh, A. (2005). Validation of the technology acceptance model for police. Journal of Criminal Justice, 33(1), 89-95.

Cook, K. S., Hardin, R., & Levi, M. (2007). *Cooperation Without Trust?* Russell Sage Foundation Publications.

Copeland, T. E. (2006). Surprise, Intelligence Failure, and Mass Casualty Terrorism.

Couprie, D., Goodbrand, A., Li, B., & Zhu, D. (2007). Soft Systems Methodology. Calgary, AB: University of Calgary.

Creswell, J. W. (1994). *Research design: Qualitative and quantitative research approaches*. Thousand Oaks, CA: Sage.

Creswell, J. W. (2012). *Qualitative inquiry and research design: Choosing among five approaches*. SAGE Publications, Incorporated.

Creswell, J. W., & Clark, V. L. P. (2007). *Designing and conducting mixed methods research*. Wiley Online Library.

Cresswell, A. M. (2004). *Return on investment in information technology: A guide for managers*. Center for Technology in Government, University at Albany, SUNY.

Cresswell, A., Pardo, T., & Canestraro, D. (2006). Digital Capability Assessment for eGovernment: A Multi-dimensional Approach. In *Electronic Government* (pp. 293–304).

Cresswell, A. M., Pardo, T. A., & Hassan, S. (2007). Assessing capability for justice information sharing. *In Proceedings of the 8th annual international conference on Digital government research: bridging disciplines & domains* (pp. 122-130). Philadelphia, Pennsylvania: Digital Government Society of North America.

Cross, R., Parker, A., Prusak, L., & Borgatti, S. P. (2001). Knowing what we know:: Supporting knowledge creation and sharing in social networks. *Organizational Dynamics*, 30(2), 100-120. doi:10.1016/S0090-2616(01)00046-8

Currion, P., de Silva, C., & Van de Walle, B. (2007). “Open source software for disaster management,” Communications of the ACM 50, no. 3: 61-65.

da Cruz, S., Chirigati, F., Dahis, R., Campos, M., & Mattoso, M. (2008). Using explicit control processes in distributed workflows to gather provenance. *In Provenance and Annotation of Data and Processes* (pp. 186-199).

Dasgupta, P., & Serageldin, I. (2000). *Social capital a multifaceted perspective*. Washington, D.C.: World Bank.

Datla, D., Chen, X., Tsou, T., Raghunandan, S., Hasan, H. and Reed, J.H. (2011). “Wireless distributed computing network: a survey of research challenges”, *IEEE Communication Magazine*, accepted for publication, April 2011.

Davenport, E. (2008). “Social informatics and sociotechnical research—a view from the UK.” *Journal of Information Science* 34(4):519.

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, 13(3), 319-340.

Dawes, S. S. (1996). Interagency information sharing: Expected benefits, manageable risks. *Journal of Policy Analysis and Management*, 15(3), 377−394.

Dawes, S. S. (2008). “Governance in the information age: a research framework for an uncertain future.” Pp. 290*-297 in Proceedings of the 2008 international conference on Digital government research*. Digital Government Society of North America.

Dawes, S. S., Cresswell, A. M., & Pardo, Theresa A. (2009). From “need to know” to “need to share”: Tangled problems, information boundaries, and the building of public sector knowledge networks. *Public Administration Review*, 69(3), 392-402. doi:10.1111/j.1540-6210.2009.01987_2.x

Dawson, E., Reid, J., Salim, F., & Burdon, M. (2010). Information sharing in the 21st century: progress and challenges. *In Proceedings of the Eighth Australasian Conference on Information Security - Volume 105*, AISC \uc0\u8217{}10 (p. 2–2). Darlinghurst, Australia, Australia: Australian Computer Society, Inc. Retrieved from http://portal.acm.org.libezproxy2.syr.edu/citation.cfm?id=1862266.1862268

Delbecq, A. L., Van de Ven, A. H., & Gustafson, D. H. (1975). *Group techniques for program planning: A guide to nominal group and Delphi processes*. Glenview, IL: Scott, Foresman, and Co.

Dempsey, J. X. (2000). Overview of current criminal justice information systems (pp. 101-106). Toronto, Ontario, Canada: *ACM*. doi:10.1145/332186.332261

Deverell, E., & Olsson, E. (2010). “Organizational culture effects on strategy and adaptability in crisis management.” *Risk Management* 12(2): 116-134. Retrieved August 15, 2011.

Diesing, P. (1992). *How Does Social Science Work?: Reflections on Practice* (p. 432). University of Pittsburgh Press.

Dezalay, Y., & Garth, B. (1996). “Fussing about the forum: Categories and definitions as stakes in a professional competition.” *Law & Social Inquiry* 21(2):285-312.

DHS NECP. (2011). U.S. Department of Homeland Security, National Emergency Communications Plan. Website (retrieved 12/26/2011) http://www.dhs.gov/xnews/releases/pr_1217529182375.shtm

Dillinger, M., & Buljore, S. (2003). Reconfigurable systems in a heterogeneous environment. *Software defined radio: architectures, systems, and functions*, 3.

DiMaggio, P. J., & Powell, W. W. (1983). “The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields.” *American Sociological Review* 48(2):147-160.

Dinesh, D., Volos, H.I., Hasan, S.M., Reed, J.H. and Bose, T. (2011). “Wireless distributed computing in cognitive radio networks.” *Ad Hoc Networks* in Press, Uncorrected Proof. Retrieved May 4.

Dispatch. (2012). Dispatch Magazine On-Line, http://911dispatch.com *Facts & Figures*, retrieved June 17, 2012.

Doney, P. M., Cannon, J. P., & Mullen, M. R. (1998). Understanding the influence of national culture on the development of trust. *Academy of Management Review*, 23(3), 601-620.

Douglas, James (1987), " *Political Theories of Nonprofit Organizations." In The Nonprofit Sector*, edited by Walter W. Powell. New Haven and London: Yale University Press.

Drake, D. B., Steckler, N. A., & Koch, M. J. (2004). Information sharing in and across government agencies: The role and influence of scientist, politician, and bureaucrat subcultures. *Social Science Computer Review*, 22(1), 67-84. doi:10.1177/0894439303259889

DuFour, R., & Eaker, R. (1998). *Professional learning communities at work: Best practices for enhancing student achievement.* Bloomington.

Dutton W. H, Gillett S. E, McKnight L. W & Peltu M. (2004). "Bridging broadband internet divides: reconfiguring access to enhance communicative power." *Journal of Information Technology*.

Dyer, J. H., & Chu, W. (2003). The role of trustworthiness in reducing transaction costs and improving performance: empirical evidence from the United States, Japan, and Korea. *Organization Science*, 14(1), 57(13).

Eisenhardt, K. M. (1989). Agency theory: An assessment and review. *Academy of management review*, 57–74.

Emery, F. E. (1997). “The next thirty years: Concepts, methods and anticipations.” *Human Relations* 50(8):885-935.

Farkas, M. A., & Manning, P. K. (1997). The Occupational Culture of Corrections and Police Officers. *Journal of Crime and Justice* 20(2):51-68.

FBI. (2011). United States Federal Bureau of Investigation. About us, web site http://fbi.gov/about-us. August 20, 2011.

FCC. (2011). “Narrowbanding.” Federal Communications Commission - Public Safety and Homeland Security Bureau. Retrieved November 28, 2011 (http://transition.fcc.gov/pshs/public-safety-spectrum/narrowbanding.html).

Fedorowicz, J., Gogan, J. L., & Culnan, M. J. (2010). Barriers to interorganizational information sharing in e-Government: A stakeholder analysis. *The Information Society: An International Journal*, 26(5), 315. doi:10.1080/01972243.2010.511556

Fedorowicz, J., Gogan, J. L., & Williams, C. B. (2006). The challenge of Washington, DC: *IBM Center for the Business of Government Monograph*.interagency integration: Lessons learned in five eGovernment cases.

Fedorowicz, J., Gogan, J. L., & Williams, C. B. (2007). A collaborative network for first responders: Lessons from the CapWIN case. *Government Information Quarterly*, 24 (4), 785-807.

Fedorowicz, J., Markus, M. L., Sawyer, S., Tyworth, M., & Williams, C. B. (2006). Design principles for public safety response mobilization. *Proceedings of the 2006 international conference on Digital government research* (pp. 466–467). ACM.

Fedorowicz, J., Sawyer, S., Williams, C., Markus, M. L., Tyworth, M., Jacobson, D., Gantman, S., et al. (2011). Design observations regarding public safety networks. *Proceedings of the 12th Annual International Digital Government Research Conference: Digital Government Innovation in Challenging Times* (pp. 272–281). ACM.

FEMA. (2011). “FEMA: Emergency Managers and Personnel.” Retrieved June 16, 2011 (http://www.fema.gov/emergency).

FEMA. (2011). U.S. Federal Emergency Management Agency (FEMA). Website (Retrieved 12/26/2011) http://www.fema.gov

FEMA NIMS. (2011). U.S. Federal Emergency Management Agency, National Incident Management System (NIMS). Website (Retrieved 12/26/2011) http://www.fema.gov/emergency/nims/AboutNIMS.shtm

Fernández-Medina, E., & Yagüe, M. I. (2008). Guest Editorial: State of standards in the information systems security area. *Computer Standards & Interfaces*, 30(6), 339-340

Fichman, R. G., & Kemerer, C. F. (1997). The assimilation of software process innovations: An organizational learning perspective. *Management Science*, 1345-1363.

Fitzek, F. H., & Katz, M. D. (2007). *Cognitive wireless networks: concepts, methodologies and visions inspiring the age of enlightenment of wireless communications*. Springer.

Fjeldstad, O. H. (2004). *Decentralisation and corruption. A review of the literature*. Chr. Michelsen Institute.

Flyvbjerg, B. (1998). *Rationality and power: Democracy in practice*. Chicago: University of Chicago Press.

Flyvbjerg, B. (2001) *Making social science matter: Why social inquiry fails and how it can succeed again.* Cambridge, UK: Cambridge University Press.

Flyvbjerg, B. (2006). “Five misunderstandings about case-study research.” *Qualitative inquiry* 12(2):219.

Forrest, J. S. (2006). Information policies and practices of knowledge management (KM) as related to the development of the Global Aviation Information Network (GAIN): An applied case study and taxonomy development. *Ph.D. dissertation, Nova Southeastern University, United States -- Florida*. Retrieved February 4, 2012, from Dissertations & Theses: Full Text.(Publication No. AAT 3226963).

Foster, I., Kesselman, C., & Tuecke, S. (2001). The anatomy of the grid: Enabling scalable virtual organizations. *International Journal of High Performance Computing Applications,* 15(3), 200 -222. doi:10.1177/109434200101500302

Foster, I., & Kesselman, C. (2004). The Grid 2: Blueprint for a new computing infrastructure. Morgan Kaufmann, San Francisco, California.

Franz, C. R., & Robey, D. (1984). An investigation of user-led system design: rational and political perspectives. *Communications of the ACM*, 27(12), 1202-1209.

Freeman, R. E. (1984). Strategic Management: a stakeholder approach. *Boston: Pitman*.

Freeman, R. E. (2010). *Strategic Management: A Stakeholder Approach*. Cambridge University Press.

Freeman, R. E., Harrison, J. S., Wicks, A. C., Parmar, B. L., & De Colle, S. (2010). *Stakeholder theory: The state of the art*. Cambridge University Press.

Freidson, E. (1988). *Professional powers: A study of the institutionalization of formal knowledge*. University of Chicago Press.

Gailmard, S. (2010). Politics, Principal–Agent Problems, and Public Service Motivation. *International Public Management Journal*, 13(1), 35–45.

Gambetta, D. (2000). Can we trust trust? In Gambetta (Eds.), Trust: Making and breaking cooperative relations, electronic edition, Department of Sociology, University of Oxford (electronic edition., p. 213–237). Oxford: University of Oxford. Retrieved from http://www.sociology.ox.ac.uk/papers/ gambetta213-237.pdf

Gao, J. (2005). Information sharing, trust in automation, and cooperation for multi-operator multi-automation systems. Thesis (Ph. D.)--University of Iowa, 2005.

Gaynor, M., Brander, S., Pearce, A., & Post, K. (2008). Open Infrastructure for a Nationwide Emergency Services Network. *International Journal of Information Systems for Crisis Response and Management* (Vol. 1, pp. 31–46).

Geertz, C. (1995). *After the fact: Two countries, four decades, one anthropologist*. Cambridge, MA: Harvard University Press.

Gefen, D. (2000). E-commerce: the role of familiarity and trust. *Omega* 28 (6), 725–737

Gerdes, A. (2010). Revealing preconditions for trustful collaboration in CSCL. *International Journal of Computer-Supported Collaborative Learning,* 5(3), 345-353.

German, M., & Stanley, J. (2008). Fusion Center Update - ACLU, July. Retrieved October 19, 2008, from http://www.aclu.org/pdfs/privacy/fusion_update_20080729.pdf.

Gil-Garcia, J. R., Chengalur-Smith, I. S., & Duchessi, P. (2007). Collaborative e-Government: impediments and benefits of information-sharing projects in the public sector. *European Journal of Information Systems*, 16(2), 121-133.

Gil-Garcia, J. R., Chun, S. A., & Janssen, M. (2009). Government information sharing and integration: Combining the social and the technical. *Information Polity*, 14(1), 1-10. doi:10.3233/IP-2009-0176

Gil-Garcia, J., Guler, A., Pardo, T., & Burke, G. (2010). Trust in Government Cross-Boundary Information Sharing Initiatives: Identifying the Determinants. In Hawaii International Conference on System Sciences, 0:1-10. Los Alamitos, CA, USA: *IEEE Computer Society*.

Glaser, B. G., & Strauss, L.A. (1967). *The discovery of grounded theory: Strategies for qualitative research*. Aldine Pub. Co.

Glomseth, R., Gottschalk, P., & Solli-Saether, H. (2007). Occupational culture as determinant of knowledge sharing and performance in police investigations. *International Journal of the Sociology of Law* 35, no. 2 (June): 96-107. doi:10.1016/j.ijsl.2007.03.003

Gonzalez, R & Bharosa, N. (2009). "A framework linking information quality dimensions and coordination challenges during interagency crisis response." Pp. 1-10 *in Hawaii International Conference on System Sciences*, vol. 0. Los Alamitos, CA, USA: IEEE Computer Society.

Goodhue, D. L. (1995). Understanding user evaluations of information systems. *Manage. Sci.*, 41(12), 1827-1844.

Graper, E. D. (1921). *American police administration: a handbook on police organization and methods of administration in American cities.* The Macmillan Company.

Graphia, R. (2010). An exploratory study of the perceived utility and effectiveness of state fusion centers. Rutgers The State University of New Jersey - Newark, United States -- New Jersey.

Greene, J. C. (2008). Is mixed methods social inquiry a distinctive methodology? *Journal of mixed methods research*, *2*(1), 7–22.

Greene, J. C., Caracelli, V. J., & Graham, W. F. (1989). Toward a conceptual framework for mixed-method evaluation designs. *Educational evaluation and policy analysis*, *11*(3), 255–274.

Greenwood, R., Suddaby R., & Hinings, C. R. (2002). "Theorizing change: The role of professional associations in the transformation of institutionalized fields." *Academy of management journal* 58-80.

Gupta, E. (2000). Information System. *Bajaj, Ankit 197 Bakry, Mohamed Abd El Latif 28 Bala, Shashi 414 Baporikar, Neeta 118*, 97.

Hage, J. (1965). "An Axiomatic Theory of Organizations," *Administrative Science Quarterly*, 10 (December), p. 295.

Hall, R. H., Johnson, N. J., & Haas, J. E. (1967). Organizational Size, Complexity, and Formalization. *American Sociological Review*, *32*(6), 903–912. doi:10.2307/2092844

Hall, R. H., & Tolbert, P. S. (2004). *Organizations: Structures, processes, and outcomes* (9th ed). New York: Prentice Hall.

Halliday, T. C. (1987). *Beyond monopoly: lawyers, state crises, and professional empowerment*. University of Chicago Press.

Handy, C.B. (1976). *Understanding organizations*. Oxford University Press.

Handy, C.B. (1996). *Beyond certainty: the changing worlds of organizations.* Harvard Business Press.

Harrison, T., Gil-Garcia, J.R., Pardo, T.A., & Fiona, T. (2006). "Learning about interoperability for emergency response: Geographic Information Technologies and the World Trade Center Crisis," *The Thirty-Ninth Annual Hawaii International Conference on System Sciences,* Computer Society Press, Hawaii.

Hauck, R. V. (2005). Should they share or not? An investigation on the use of communication and knowledge sharing technology in a police organization. *The University of Arizona*, United States -- Arizona.

He, A., Amanna, A., Tsou,T., Chen, X., Datla, D., Newman, T., Reed, J., & Bose, T. (2011). "Green Communications: A New Paradigm for Creating Cost Effective Wireless Systems," *Journal of Communications*, accepted for publication, March.

Headayetullah, M., & Pradhan, G. K. (2009). A novel trust-based information sharing protocol for secure communication between government agencies. *European Journal of Scientific Research*, 34(3), 442–454.

Headland, T. N., Pike, K. L., & Harris, M. (1990). *Emics and etics: The insider/outsider debate* (Vol. 9). Sage Newbury Park, CA.

Heller, F. (1997). Sociotechnology and the Environment. *Human Relations*, Vol. 50, No 5, pp. 605-624.

Hicks, J. (2004). Law Enforcement Technology Standards Council and Standard Functional Requirements. *Police Chief Magazine*, 71(6). Retrieved from http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=320&issue_id=62004

Hinde, R. A., & Jo Groebel (Eds.). (1991). *Cooperation and prosocial behaviour*. Cambridge [England]; New York: Cambridge University Press.

Hofstede, G., Neuijen, B., Ohayv, D. D., & Sanders, G. (1990). Measuring organizational cultures: A qualitative and quantitative study across twenty cases. *Administrative science quarterly,* 286–316.

Homey, J., Osgood, D. W., & Marshall, I. H. (1995). Criminal careers in the short-term: Intra-individual variability in crime and its relation to local life circumstances. *American Sociological Review*, 60(5), 655-673.

Hong, D., Suh, E., & Koo, C. (2011). Developing strategies for overcoming barriers to knowledge sharing based on conversational knowledge management: A case study of a financial company. *Expert Systems with Applications* 38(12):14417-14427.November.

Hughey, E.P., & Bell, H.M. (2011). Does comprehensive emergency management work? *Risk, Hazards, and Crisis in Public Policy,* 2 (1), 1-33.

Huijboom, N. (2007). Social capital and ICT adoption in the public sector (pp. 140-147). Philadelphia, Pennsylvania: *Digital Government Society of North America*.

Human, S. E., & Provan, K. G. (2000). Legitimacy building in the evolution of small-firm multilateral networks: A comparative study of success and demise. *Administrative Science Quarterly*, 45(2), 327-365.

Humenn, P., Chin, S.-K., Kosiyatrakul, T., Older, S., & Northrup, T. (2004). A trusted information sharing project. Syracuse. Retrieved from http://webdev.maxwell.syr.edu/insct/Research/IS%20Page/SU%20Trust-Sharing%20Project.pdf

IDABC (2008). Interoperable Delivery of European eGovernment services to public Administrations, Businesses and Citizens. *European Interoperability Framework*, V2.0 (draft). URL: http://ec.europa.eu/idabc/servlets/Doc?id=31597

Ingram, P., & Lifschitz, A. (2006). Kinship in the shadow of the corporation: The Interbuilder Network in Clyde River Shipbuilding, 17111990. *American Sociological Review*, 71, 334-352.

Ipe, M. (2003). Knowledge sharing in organizations: a conceptual framework. *Human Resource Development Review*, 2(4), 337.

ISAC. (2004). Information Sharing and Analysis Center White Paper. Vetting and trust for communication among ISACs and government entities. Retrieved October 23, 2008, from http://www.isaccouncil.org/pub/Vetting_and_Trust_013104.pdf.

ISE. (2011). Information Sharing Environment. Information sharing site that focuses on counterterrorism and areas of national security. *ISE.gov.*, Government Agency. Retrieved March 25, 2011, from http://www.ise.gov/

ISOC, (2010). The Internet Society. "The Internet Rises to the Challenge of Public Warning," Nonprofit Society, Internet Society - Public Warning Network Challenge, http://www.isoc.org.

IT.OJP. (2010). IT.OJP.GOV Home. Office of Justice Programs. Information Sharing News - NIJ. Retrieved November 22, 2010, from http://it.ojp.gov/default.aspx

Ivkovic, S. K., & Shelley, T. O. (2005). The Bosnian police and police integrity: A continuing story. *European Journal of Criminology*, 2(4), 428-464. doi:10.1177/1477370805056057.

Jacobs, J. B., & Blitsa, D. (2008). Sharing criminal records: The United States, the European Union and Interpol compared. *Loyola of Los Angeles International and Comparative Law Review*, 30, 125.

Jarvenpaa, S. L., & Staples, D. S. (2000). The use of collaborative electronic media for information sharing: An exploratory study of determinants. *The Journal of Strategic Information Systems*, 9(2–3), 129-154.

Jeffries, F. L. (2002). Subjective norms, dispositional trust, and initial trust development. *Journal of Behavioral and Applied Management*, 3(2), 129 - 139.

Jin, Q. (2002). Design of a virtual community based interactive learning environment. *Information Sciences*, 140(1-2), 171-191.

Jing, F., & Pengzhu, Z. (2007). A case study of G2G information sharing in the Chinese context. In Proceedings of the 8th annual international conference on Digital government research: bridging disciplines & domains (pp.234-235). Philadelphia, Pennsylvania: *Digital Government Society of North America*.

Kaarst-Brown, M. L. (1999). Five symbolic roles of the external consultant–integrating change, power and symbolism. *Journal of Organizational Change Management*, 12(6), 540–561.

Kaarst-Brown, M. L., & Guzman, I. R. (2008). Decisions, Decisions: Ethnography or Mixed-Method Approaches to Study Cultural Issues in IS Research. In *Cultural Attitudes Toward Technology and Communications (CATaC).* Editors, F. Sudweeks, H. Hrachovec and C. Ess. Nimes, France, Murdoch University Press. 6: 11--25.

Kaarst-Brown, M. L., & Robey, D. (1999). More on myth, magic and metaphor: Cultural insights into the management of information technology in organizations. *Information Technology & People*, 12(2), 192–218.

Kaplan, A. (1998). *The conduct of inquiry*. Transaction Publishers.

Kean, T. H., & Hamilton, L. (2004). *Nine/eleven Commission report, final report of the National Commission on Terrorist Attacks Upon the United States*. WW Norton & Company.

Kemp, C. G. (2005). *Regional readiness for intelligence information sharing to support homeland security.* Retrieved from http://proquest.umi.com/pqdweb?did=994247051&Fmt=7&clientId=3739&RQT=309&VName=PQD

Kemp, R. L., Wagman, D., & Canada, B. (2003). *Homeland security: Best practices for local government,* edited by Roger L. Kemp. Washington, D.C.: International City/County Management Association.

Kim, S., & Lee, H. (2006). The impact of organizational context and information technology on employee knowledge-sharing capabilities. *Public Administration Review*, 66(3), 370-385.

Kingdon, J. W. (1997). *Agendas, Alternatives, and Public Policies*. 2nd ed. Pearson Education.

Koroma, J., Li, W., & Kazakos, D. (2003). A generalized model for network survivability. In Proceedings of the 2003 conference on Diversity in computing (pp. 47-51). Atlanta, Georgia, USA: *ACM*. doi: 10.1145/948542.948552.

Kothari, A., MacLean, L., Edwards, N., & Hobbs, A. (2011). Indicators at the interface: managing policymaker-researcher collaboration. *Knowledge Management Research & Practice*, *9*, 203–214. doi:10.1057/kmrp.2011.16

Koufaris, M., & Hampton-Sosa, W. (2004). The development of initial trust in an online company by new customers. *Inf. Manage.*, 41(3), 377-397.

Kovács, G., & Spens, K. M. (2011). Trends and developments in humanitarian logistics–a gap analysis. *International Journal of Physical Distribution & Logistics Management*, *41*(1), 32–45.

Krosgaard, M. A., Brodt, S. E., & Whitener, E. M. (2002). Trust in the face of conflict: The role of managerial trustworthy behavior and organizational context. *Journal of Applied Psychology*, 87(2), 312.

Kshemendra, N. P. (2010). Information sharing environment: Annual report to the congress (Annual Report to Congress) (p. 102). Washington, D.C. *Information Sharing Environment*.

Kuehn, A., Spichiger, A., & Riedl, R. (2009). Interoperabilität und standards im e-Government, in: E. Schweighofer (ed.) Tagungsband des 12. *Int. Rechtsinformatik Symposions*. OCG Books, Vienna.

Kuenzel, E., & Welscher, H. (2009). *"Management Model for Successful Collaboration in the Public Sector*." [Managing Collaboration] Federal Ministry for Economic Cooperation and Development.

Kuhn, A. (1974). *The Logic of Social Systems.* San Francisco: Jossey-Bass.

Kulik, C. T., Bainbridge, H. T. J., & Cregan, C. (2008). Known by the company we keep: Stigma-by-association effects in the workplace. *Academy of Management Review*, 33(1), 216-230. doi: Article.

Kulkarni, U., Ravindran, S., & Freeze, R. (2007). A knowledge management success model: Theoretical development and empirical validation. *J. Manage. Inf. Syst*., 23(3), 309-347.

Lai, V. S., & Mahapatra, R. K. (1997). Exploring the research in information technology implementation. *Inf. Manage*., 32(4), 187-201.

Lamb, R., Sawyer, S., & Kling, R. (2000). A Social Informatics Perspective on Socio-Technical Networks. *AMCIS 2000 Proceedings.* Paper 1, 6.

Lampathaki, F., Mouzakitis, S., Gionis, G., Charalabidis, Y., & Askounis, D. (2009). Business to business interoperability: A current review of XML data integration standards. *Computer Standards & Interfaces*, 31(6), 1045-1055.

Lax, D. A., & Sebenius, J. K. (1986). *The manager as negotiator: Bargaining for cooperation and competitive gain.* New York: Free Press.

Leavitt, H. J., (1965). Applied organization change in industry: Structural, technical, and human approaches; new perspectives in organizational research, in March, J.G (ed.) *Handbook of Organizations*, Chicago, Rand McNally, p55-71.

Leavitt, M. O., Spelling, M., & Gonzales, A. R. (2007*). Report to the President on issues raised by the Virginia Tech tragedy* (No. NCJ 218878) (p. 26). Rockville, MD 20849: National Institute of Justice/NCJRS. Retrieved from http://www.hhs.gov/vtreport.pdf

Lee, C. (2006). The role of trust in information sharing: A study of relationships of the interorganizational network of real property assessors in New York state. Ph.D. diss., State University of New York at Albany, *In Dissertations & Theses: Full Text* [database on-line]; available from http://www.proquest.com.libezproxy2.syr.edu (publication number AAT 3251091; accessed April 23, 2011).

Lee, H. (2008). Cyber crime and challenges for crime investigation in the information era. In Intelligence and Security Informatics, 2008. ISI 2008. *IEEE International Conference on (pp. xxv-xxvi)*. doi:10.1109/ISI.2008.4565011.

Lee, J. N., Huynh, M., & Hirschheim, R. (2008). An integrative model of trust on IT outsourcing: Examining a bilateral perspective. *Information Systems Frontiers*, 10(2), 145-163. doi:10.1007/s10796-008-9066-7

Lee, J., & Rao, H. R. (2007). Exploring the causes and effects of inter-agency information sharing systems adoption in the anti/counter-terrorism and disaster management domains. *In Proceedings of the 8th annual international conference on Digital government research: bridging disciplines & domains* (pp. 155-163). Philadelphia, Pennsylvania: Digital Government Research Center.

Legris, P., Ingham, J., & Collerette, P. (2003). Why do people use information technology?: a critical review of the technology acceptance model. *Inf. Manage*., 40(3), 191-204.

LEITSC. (2009). “LEITSC” Home Page and Information. Retrieved January 22, 2009 (http://www.leitsc.org/AboutUs.htm#Governance).

LEITSC OJP. (2012). “Training and Technical Assistance Opportunities: Law Enforcement Information Technology Standards Council (LEITSC).” *U.S. Department of Justice, Office of Justice Programs.* Retrieved February 5, 2012 (http://it.ojp.gov/default.aspx?area=implementationAssistance&page=1938).

LEPSC. (2009). Law Enforcement-Private Security Consortium. Operation partnership: trends and practices in law enforcement and private security collaborations *(Research Report No. e08094224) (p. 144). Washington, DC: U.S. Department of Justice*. Retrieved from http://www.ilj.org/publications/docs/Operation_Partnership_Private_Security.pdf

Levin, D. Z., & Cross, R. (2004). The strength of weak ties you can trust: The mediating role of trust in effective knowledge transfer. *Management Science*, 50(11), 1477-1490.

Levitt, H. (1993). Former NY deputy commish indicted, December 11, 1993. Retrieved November 22, 2009, from http://nypdconfidential.com/columns/2003/031211.html

Lewin, K. (1951), *Field Theory in Social Science*, Harper and Row, New York, NY.

Lewis, M., & Slack, N. (2003). *Operations management: critical perspectives on business and management*. Routledge.

Li, G., Sun, H., Gao, H., Yu, H., & Cai, Y. (2009). “A Survey on Wireless Grids and Clouds.” In *Grid and Cooperative Computing, 2009. GCC’09. Eighth International Conference On*, 261–267. IEEE.

Li, H., Gong, S., Lai, L., Han, Z., Qiu, R. Q., &Yang, D. (2012). “Efficient and Secure Wireless Communications for Advanced Metering Infrastructure in Smart Grids.” *Smart Grid, IEEE Transactions On* 3, no. 3: 1540–1551.

Li, X., Hess, T. J., & Valacich, J. S. (2008). Why do we trust new technology? A study of initial trust formation with organizational information systems. *The Journal of Strategic Information Systems*, 17(1), 39-71. doi:10.1016/j.jsis.2008.01.001.

Lieberman, J. (2007). Confronting the terrorist threat to the homeland: Six years after 9/11. 342 Dirksen senate office building, Washington, D.C.: Federal News Service. Retrieved May 8, 2008, from http://www.fas.org/irp/congress/2007_hr/091007transcript.pd f.

Lin, C., Hu, P. J. H., & Chen, H. (2004). Technology implementation management in law enforcement: COPLINK system usability and user acceptance evaluations. *Social Science Computer Review*, 22(1), 24.

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry* (Vol. 75). Sage Publications, Inc.

Linstone, H. A., & Turoff, M. (1976). *The Delphi method: Techniques and applications* (Vol. 18). Addison-Wesley.

Lipnack, J., & Stamps, J. (1994). *The age of the network: organizing principles for the 21st century*. John Wiley & Sons Inc.

Longstaff, P. H. (2003). Can unpredictable systems be managed? Systems, Man and Cybernetics, 2003. *IEEE International Conference on* (Vol. 2, pp. 2013–2020). IEEE.

Longstaff, P. H., & Yang, S.U. (2008). “Communication management and trust: their role in building resilience to ‘surprises’ such as natural disasters, pandemic flu, and terrorism.” *Ecology and Society* 13(1): 3.

Longstaff, P. H. (2009). Managing surprises in complex systems: multidisciplinary perspectives on resilience. *Ecology and Society*, 14(1), 49.

Longstaff, P., Mergel, I., & Armstrong, N. (2009). Workshop report: resilience in post-conflict reconstruction and natural disasters. *Workshop Report: Resilience in Post-Conflict Reconstruction and Natural Disasters* (March 9, 2009).

Longstaff, P. H., Armstrong, N. J., Perrin, K., Parker, W. M., & Hidek, M. A. (2010). Building resilient communities: A preliminary framework for assessment. *Homeland security affairs*, 6(3), 1–23.

Luna-Reyes, L. F., Andersen, D. F., Richardson, G. P., Pardo, T. A., & Cresswell, A. M. (2007). Emergence of the governance structure for information integration across governmental agencies: a system dynamics approach. *In Proceedings of the 8th annual international conference on Digital government research: bridging disciplines* \ & domains (pp. 47-56). Philadelphia, Pennsylvania: Digital Government Society of North America

Luna-Reyes, L. F., Black, L. J., Cresswell, A. M., & Pardo, T. A. (2008). Knowledge sharing and trust in collaborative requirements analysis. *System Dynamics Review*, 24(3), 265-297. doi:10.1002/sdr.404

Lyytinen, K., & Rose, G. M. (2003). The disruptive nature of information technology innovations: the case of internet computing in systems development organizations. *MIS Quarterly*, 557-596.

Majchrzak, A. (1984). *Methods of policy research. Applied social research methods series*, Vol. 3. Newbury Park, CA: Sage.

Manvi, S. S., & Birje, M. N. (2009). “Wireless Grid Computing: A Survey.” *IETE Journal of Education* 50, no. 3: 119.

Marincioni, F. (2007). “Information technologies and the sharing of disaster knowledge: the critical role of professional culture.” *Disasters* 31(4): 459-476.

Marks, D. E., & Sun, I. Y. (2007). The impact of 9/11 on organizational development among state and local law enforcement agencies. *Journal of Contemporary Criminal Justice*, 23(2), 159-173.

Marks, D. E. (2006). *Policing and terrorism: The impact of 9/11 on the organizational structure of state and local police departments in the United States*. Retrieved from http://proquest.umi.com/pqdweb?did=1037890231&Fmt=7&clientId=3739&RQT=309&VName=PQD

Marsden, J., Treglia, J., & McKnight, L. (2012). Dynamic Emergency Response Communication: The intelligent Deployable Augmented Wireless Gateway (iDAWG). Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), 2012 IEEE International Multi-Disciplinary Conference on. *Presented at the Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), 2012 IEEE International Multi-Disciplinary Conference on, New Orleans, USA: IEEE.*

Martensson, M. (2000). A critical review of knowledge management as a management tool. *Journal of Knowledge Management*, 4(3), 204-216.

Martin, K. (2004). “Domestic Intelligence and Civil Liberties.” *SAIS Review* 24(1):7. Retrieved November 14, 2008.

Mattessich, P. W., Murray-Close, M., & Monsey, B. R. (2001). *Collaboration: What Makes It Work, 2nd Edition: A Review of Research Literature on Factors Influencing Successful Collaboration* (2nd ed.). Amherst H. Wilder Foundation.

Mayberry-Stewart, D. (2008). *2008 New York State Statewide Wireless Network Annual Report*. Retrieved from http://www.cio.ny.gov/assets/documents/RevisedSWNAnnulaReport3.pdf

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *The Academy of Management Review*, 20(3), 709–734.

McEvily, B., & Tortoriello, M. (2011). Measuring trust in organisational research: Review and recommendations. *Journal of Trust Research*, *1*(1), 23–63. doi:10.1080/21515581.2011.552424

Mckay, J. (2008). Statement of John McKay, Former United States Attorney For the Western District of Washington, Before the Subcommittee on Intelligence, Information Sharing And Terrorism Risk Assessment Committee on Homeland Security United States House of Representatives (Washington, D.C., 2008), Retrieved October 18, 2008, from http://webdev.maxwell.syr.edu/insct/Research/IS%20Page/M cKay%20Testimony.pdf.

McKenna, C. (2009). *NY Statewide Wireless Interoperable Communication Network Refocused on Regional Systems*. Retrieved from http://www.govtech.com/public-safety/99355764.html

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-Commerce: An integrative typology. *Info. Sys. Research*, 13(3), 334-359.

McKnight, L. W. (2007). *"The future of the internet is not the internet: open communications policy and the future wireless grid(s).”* Washington, D.C.: NSF/OECD. http://www.oecd.org/dataoecd/18/42/38057172.pdf.

McKnight, L. W., & Anius, D. (2002).*Virtual Markets in Wireless Grids: Peering Policy Obstacles*,30th Annual TPRC, Alexandria, VA, and Sept. 28-30, 2002.

McKnight, L.W., & Howison, J. (2003). *"Toward a sharing protocol for wireless grids."* Int’l Conference on Computer, *Communication & Control Technologies* (CCCT '03), Orlando, Fl, July 31-August 2, 2003.

McKnight, L. W., Howison, J., & Bradner, S. (2004). Guest editors' introduction: Wireless grids--distributed resource sharing by mobile, nomadic, and fixed devices. *Internet Computing*, IEEE, 8(4), 24-31.

McKnight, L. W., Katz, R. L., & Vaaler, P. M. (2001). *Creative destruction: Business survival strategies in the global internet economy*, MIT Press.

McKnight, L., & Kuehn, A. (2011). *Creative Destruction: Schumpeterian Innovation in the Cyber Age. "Leadership in Science and Technology: A Reference Handbook*." Forthcoming: Sage.

McKnight, L., Lehr, W., & Howison, J. (2007). "Coordinating User and Device Behavior in Wireless Grids." in F.H.P. Fitzek and M.D. Katz. Eds. *Cognitive Wireless Networks: Concepts, Methodologies and Visions Inspiring the Age of Enlightenment of Wireless Communications,* Springer. pp. 679-697.

McKnight, L., Sharif, R., & Wijngaert, V. D. (2005). *Wireless grids: assessing a new technology from a user perspective, Designing Ubiquitous Information Environments: Socio-Technical Issues and Challenges*. http://dx.doi.org/10.1007/0-387-28918-6_14.

McKnight, L. W., Treglia, J., & Kuehn, A. (2010). "Wireless Grids or Personal Infrastructure: Policy Implications of an Emergent Open Standard." in *TPRC 38th Research Conference on Communication, Information and Internet Policy*. Arlington, VA.

McMamara, T. E. (2006). *Information Sharing Environment Implementation Plan*. Washington, D.C. Retrieved from http://webdev.maxwell.syr.edu/insct/Research/IS%20Page/ISE%20Imp%20Plan%202006.pdf

Meese, E. III. (1998). "Federalism in Law Enforcement » Publications » The Federalist Society." The Federalist Society. Retrieved August 27, 2011 (http://www.fed-soc.org/publications/detail/federalism-in-law-enforcement).

Mendonça, D., Jefferson, T., & Harrald, J. (2007). "Collaborative adhocracies and mix-and-match technologies in emergency management," *Commun. ACM* 50, no. 3: 44-49.

Merriam-Webster. (2012). *Merriam-Webster dictionary online*. Accessed from http://www.merriam-webster.com, June, 30, 2012.

Miller, G. J. (2005). The political Evolution of Principal-Agent Models. *Annual Review of Political Science,* 8(1): 203-225.

Milward, H. B., & Provan, K. G. (1998). Principles for controlling agents: The political economy of network structure. *Journal of Public Administration Research and Theory*, 8(2), 203-221.

Milward, H. B., & Provan, K. G. (2006). A manager's guide to choosing and using collaborative networks. *Report published by the IBM Center for the Business of Government,* Washington, DC.

Mingers, J. (2001). Combining IS research methods: towards a pluralist methodology. *Information systems research*, *12*(3), 240–259.

Mintrom, M. (2003). *People skills for policy analysts.* Georgetown University Press.

MITRE. (2009).MITRE Cross-Boundary Information Sharing (XBIS) Lab. Retrieved 21:46:39, September 4, 2009 from http://www.mitre.org/tech/xbis/

Mohtashami, M. (2006). The antecedents and impacts of information processing effectiveness in inter-organizational collaborative software development. *Ph.D. dissertation, Rutgers The State University of New Jersey - Newark, United States -- New Jersey*. Retrieved April 23, 2011, from Dissertations & Theses: Full Text.(Publication No. AAT 3247644).

Montgomery, D. (1987). *The Fall of the House of Labor: The Workplace, the State, and American Labor Activism, 1865-1920*. Cambridge: Cambridge University Press.

Moore, M.H. (1995). *Creating public value: strategic management in government.* Harvard University Press.

Morris, B., Tanner, C., & D'Alessandro, J. (2010). Enabling trust through continuous compliance assurance. Information Technology: New Generations, Third International Conference on (Vol. 0, pp. 708-713). Los Alamitos, CA, USA: *IEEE Computer Society*. doi:http://doi.ieeecomputersociety.org/10.1109/ITNG.2010.172

Moynihan. (2005). Leveraging collaborative networks in infrequent emergency situations. *Report published by the IBM Center for the Business of Government*. Washington, DC.

Mulki, F., Zheng, L., Yang, T. M., & Pardo, T. A. (2008). International research program in cross-boundary information sharing. *Proceedings of the 2008 international conference on Digital government research* (pp. 409-410). Montreal, Canada: Digital Government Society of North America.

Mumford, E. (2000). Socio-technical design: an unfulfilled promise or a future opportunity? *Organizational and social perspectives on information technology: IFIP TC8 WG8. 2 International Working Conference on the Social and Organizational Perspective on Research and Practice in Information Technology, June 9-11, 2000,* Aalborg, Denmark (p. 33). Springer Netherlands.

Mumford, E. (2003). *Redesigning human systems*. Irm Press.

Mumford, E., Land, F. F., Hawgood, J., (1980), Training the Systems Analyst of the 1980's: Four New Design Tools to Assist the Design Process, in Lucas, H., Land, F.F., Lincoln, T., and Supper, K., (eds.), *The Information Systems Environment*, North Holland.

National Research Council. (2007). “Successful Response Starts with a Map: Improving Geospatial Support for Disaster Management”, *National Academies Press*, page 2.

NCR. (2009). National Capital Region (NCR) Project Team, 2009 Presidential Inauguration *Regional After-Action Report (AAR) Summary*. Washington, D.C.: Department of Homeland Security, National Captial Region Retrieved (http://www.mwcog.org/uploads/pub-documents/zVZYXQ20091023164715.pdf).

NCR Project Team. (2009). *2009 Presidential Inauguration Regional After-Action Report (AAR) Summary* (After-Action Report) (p. 44). Washington, D.C.: Department of Homeland Security, National Captial Region.

NENA. (2009). “What is NG911?” Retrieved November 28, 2011 (http://www.ems1.com/ems-products/communications/articles/588619-What-is-NG911/).

Newburn, T., & Webb, B. (1999). *Understanding and preventing police corruption: Lessons from the literature.* No.: ISBN 1-84082-82-2600, 64.

Newman, T.R., Hasan, S.M.S., Depoy, D., Bose, T., & Reed, J.H. (2010)."Designing and deploying a building-wide cognitive radio network testbed," *Communications Magazine*, IEEE, vol.48, no.9, pp.106-112, Sept.

Nicholson, H. (1996). “A spy story: U.S. charges top CIA official with selling secrets to Russians - Harold Nicholson - Cover Story, December 6, 1996.” Retrieved February 22, 2009 (http://findarticles.com/p/articles/mi_m0EPF/is_n13_v96/ai_18973163).

NIEM. (2007). "Introduction to the National Information Exchange Model (NIEM).” Https://www.niem.gov/documentsdb/Documents/Overview/NIEM_Introduction.pdf. NIEM. Retrieved August 27, 2011.

NIEM. (2011). National Information Exchange Model (NIEM). National Information Exchange Model. Http://www.niem.gov/index.php. *NIEM.* Retrieved March 25, 2011.

NIEM. (2011a). “NIEM - Past Honorees.” Retrieved August 27, 2011 (https://www.niem.gov/about/best-of-niem/Pages/past-honorees.aspx).

NIST, (2005). “International standards and innovation: Opening markets for american workers and exporters (+$2 million),” February 6, 2005, http://www.nist.gov/ public affairs/factsheet/intl_standards.html.

Niu, J. (2007). Circles of trust: A comparison of the size and composition of trust circles in Canada and in China. Retrieved from http://proquest.umi.com/pqdweb?did=1276413271 & Fmt=7 & clientId=3739 & RQT=309 & VName=PQD.

Nivolianitou, Z., & Synodinou, B. (2011). Towards emergency management of natural disasters and critical accidents: The Greek experience. *Journal of Environmental Management*, *92*(10), 2657–2665. doi:10.1016/j.jenvman.2011.06.003

Nonaka, I., & von Krogh, G. (2009). Perspective—tacit knowledge and knowledge conversion: Controversy and advancement in organizational knowledge creation theory. Organization Science, 20, 635–652. doi:10.1287/orsc.1080.0412

Nonaka, I. (1991). *The knowledge-creating company.* Harvard Business Review, 69(6), 96-104.

Nordin, M., Pauleen, D. J., & Gorman, G. E. (2009). Investigating KM antecedents: KM in the criminal justice system. *Journal of Knowledge Management*, 13(2), 4-20.

NYS DHSES. (2011). SCIP 2010 - Statewide Communications Interoperability Plan Update Year 2010. Albany, NY: New York State Department of Homeland Security and Emergency Services Retrieved November 28, 2011 (www.dhses.ny.gov/oiec/documents/NewYorkSCIP2010.pdf).

NYS DHSES. (2011). Statewide Communications Interoperability Plan - State of New York. Albany, NY: New York State Department of Homeland Security and Emergency Services. December 31, 2011. Retrieved from www.dhses.ny.gov/oiec/documents/NewYorkSCIP2010.pdf

Oakerson, R. J. (1993). "Reciprocity: A bottom-up view of political development." In Vincent Ostrom, David Feeney, and Hartmut Picht, eds., *Rethinking institutional analysis and development: Issues, alternatives, and choices*, pp. 141–58. San Francisco: ICS Press.

O'Brien, J., & Marakas, G. (2008). *Management Information Systems* (9th ed.). McGraw-Hill/Irwin.

O'Neill, A. (2006). Drug bust leads to huge police corruption probe - CNN.com. November 3. Retrieved February 22, 2009, from http://www.cnn.com/2006/LAW/11/02/sheriff.indictment/index.html

Orlikowski, W. J. (2002). Knowing in practice: Enacting a collective capability in distributed organizing. *Organization Science*, 13(3), 249-273.

Orlikowski, W. J. (2007). Sociomaterial practices: Exploring technology at work. *Organization Studies*, 28(9), 1435-1448.

OSC. (2006). Office of the State Comptroller. Statewide Wireless Network - Briefing Document for State Officials. Albany, NY: Office of State Comptroller Retrieved (http://www.osc.state.ny.us).

Ostrom, E. (1990). *Governing the commons: The evolution of institutions for collective action*. Cambridge, England: Cambridge Univ. Press.

Ostrom, E. (1994). *Neither market nor state: Governance of common-pool resources in the twenty-first century*. International Food Policy Research Institute.

Ostrom, E. (2003). Toward a behavioral theory linking, trust, reciprocity, and reputation. In E. Ostrom & J. Walker (Eds.), *Trust and reciprocity: Interdisciplinary lessons from experimental research* (pp. 19-79). NY: Russell Sage Foundation.

Ostrom, E. (2009). *What is social capital? Social capital: Reaching out, reaching in* (pp. 17–38). Northampton, MA, US: Edward Elgar Publishing.

Ostrom, E., & Walker, J. (2003). *In E. Ostrom and J. Walker (Eds.), Introduction*. *Trust and reciprocity: Interdisciplinary lessons from experimental research* (pp. 3-18). New York: Russell Sage Foundation.

Ostrom, E., & Walker, J. (2005). *Trust and Reciprocity: Interdisciplinary Lessons from Experimental Research*. Russell Sage Foundation.

Padgett, D. (2008). *Qualitative methods in social work research* (Vol. 36). Sage Publications, Inc.

Palen, P., Anderson, K., Mark, G., Martin, J., Sicker, D., Palmer, M. and Grunwald, D. (2010). “A vision for technology-mediated support for public participation & assistance in mass emergencies & disasters.” P. 8 in *Proceedings of the 2010 ACM-BCS Visions of Computer Science Conference*. British Computer Society.

Paoline, Eugene A., III. (2003). Taking Stock: Toward a Richer Understanding of Police Culture. *Journal of Criminal Justice* 31(3):199-214.

Pardo. T. (2006). Knowledge sharing in cross-boundary information system development in the public sector. *Information Technology and Management*, 7(4), 293-313. doi:10.1007/s10799-006-0278-6

Pardo, T., Cresswell, A., Thompson, F., & Zhang, J. (2006). Knowledge sharing in cross-boundary information system development in the public sector. *Information Technology and Management*, 7(4), 293-313. doi: 10.1007/s10799-006-0278-6.

Pardo, T., Gil-Garcia, J., & Burke, G. (2008). Governance structures in cross-boundary information sharing: Lessons from state and local criminal justice initiatives. In

Proceedings of the 41st Annual Hawaii Int'l Conference on System Sciences. *IEEE Computer Society.*

Pardo, T., Gil-Garcia, J., & Burke, G. (2008b). Building response capacity through cross-boundary information sharing: The critical role of trust *(Working Paper No. No. 06-2008)* (p. 11). Albany, NY: Center for Technology in Government, University at Albany.

Pardo, T., Gil-Garcia, J., & Burke, G. (2008c). Sustainable cross-boundary information sharing. *Digital Government, Integrated Series In Information Systems* (Vol. 17, pp. 421-438). Springer US. Retrieved from http://dx.doi.org/10.1007/978-0-387-71611-4_21

Pardo, T., & Tayi, G. (2007). Interorganizational information integration: A key enabler for digital government. *Government Information Quarterly*, 24(4), 691-715. doi:10.1016/j.giq.2007.08.004

Park, J., An, G., & Chandra D. (2007). Trusted P2P computing environments with role-based access control (RBAC*). IET (The Institution of Engineering and Technology, formerly IEE) Information Security*, 1(1):27-35.

Park, J., Chandramohan, P., Suresh, A., & Giordano, J. (2009). Component survivability for mission-critical distributed systems. *Journal of Automatic and Trusted Computing* (JoATC). In press.

Park, J. S., & Devarajan, G. (2007). Fine-Grained and Scalable Message Protection in Sensitive Organizations. *Journal of Software*, 2(6), 65.

Park, J., Kang, M., & Froscher, J. (2001). A secure workflow system for dynamic cooperation. In Michel Dupuy and Pierre Paradinas, editors, Trusted Information: The New Decade Challenge, pages167–182. Kluwer Academic Publishers, 2001. *Proceedings of the 16th IFIP TC11 International Conference on Information Security (IFIP/SEC),* Paris, France, June 11-13.

Park, J., & Ram, S. (2004). "Information systems interoperability: What lies beneath?," *ACM Trans. Inf. Syst.* 22, no. 4: 595-632.

Park, J., Sandhu, R., & Ahn, G. (2001). Role-based access control on the Web. *ACM Transactions on Information and System Security (TISSEC),* 4(1):37–71.

Park, J., Suresh, A., An, G., & Giordano, J. (2006). A framework of multiple-aspect component-testing for trusted collaboration in mission-critical systems. *In Proceedings of the IEEE Workshop on Trusted Collaboration (TrustCol),* Atlanta, Georgia, November 17-20. IEEE Computer Society.

Parry, K. W. (1999). Enhancing adaptability: leadership strategies to accommodate change in local government settings. *Journal of Organizational Change Management*, *12*(2), 134–157. doi:10.1108/09534819910263677

Peha, J. M. (2005). "Protecting Public Safety With Better Communications Systems," *IEEE Communications*, March.

Phan, M. C. T., Styles, C. W., & Patterson, P. G. (2005). Relational competency's role in Southeast Asia business partnerships. *Journal of business research*, *58*(2), 173–184.

Pittman, E. (2011). "Government, Industry Converge to Discuss Information Sharing Issues." Emergency Management. Retrieved January 11, 2011 (http://www.emergencymgmt.com/safety/Government-Industry-Converge-to-Discuss-Information-Sharing-Issues.html).

Plecas, D., McCormick, A. V., Levine, J., Neal, P., & Cohen, I. M. (2010). Evidence-based solution to information sharing between criminal justice agencies *(Research Paper)* (p. 21). Vancouver, B.C., Canada: Royal Canadian Mounted Police.

Podolny, J. M., & Page, K. L. (1998). Network forms of organization. *Annual review of sociology*, 57-76.

Powell, W. W., & DiMaggio, P. J. (1991). *The new institutionalism in organizational analysis*. University of Chicago Press.

Powell, W. W., & Steinberg, R. (2006). *The nonprofit sector: a research handbook*. Yale University Press.

Powner, D. A. (2008). Critical infrastructure protection: Further efforts needed to integrate planning for and response to disruptions on converged voice and data networks (No. GAO-08-607) (p. 27). *Washington, D.C. GAO*. Retrieved from http://www.gao.gov/products/GAO-08-607

Provan, K. G., & Milward, H. B. (2001). Do networks really work? A framework for evaluating public-sector organizational networks. *Public Administration Review,* 61(4), 414−424.

Provan, K. G., Fish, A., & Sydow, J. (2007). Interorganizational networks at the network level: A review of the empirical literature on whole networks. *Journal of management*, 33(3), 479.

PSCR. (2011). "The Public Safety Communications Research Program." Retrieved December 23, 2011 (http://www.pscr.gov/projects/lmr/p25_stds_dev/p25_stds_dev.php).

PSN. (2011) The Public Safety Networks Study of Bentley College, Syracuse University & Penn State, projects #IIS-0534877 & #IIS-0534889, sponsored by the National Science Foundation, http://publicsafetynetworksstudy.org

Pugh, D. S., Hickson, D. J., Hinings, C. R., Mcddonald, K. M., Turner, C., & Lupton, T. (1963). "A Scheme for Organizational Analysis," *Administrative Science Quarterly*, 8 (December), p. 305.

Quarantelli, E.L. (1997). Ten criteria for evaluating the management of community disasters. *Disasters* 21 (1), 39-56.

Rabbit, E. (2009). Preparing for the worst: An analysis of homeland security collaboration among state government agencies. Georgetown University, United States -- District of Columbia.

RadioReference.com. (2011). "Narrowbanding - The RadioReference Wiki." Radio Reference - Narrowbanding. Retrieved November 28, 2011 (http://wiki.radioreference.com/index.php/Refarming).

Ragin, C. C. (1994). *Constructing Social Research: The Unity and Diversity of Method*. Pine Forge Press.

Ragin, C. C., & Becker, H. S. (Eds.). (1992). *What is a case? Exploring the foundations of social inquiry*. Cambridge, UK: Cambridge University Press.

Raiser. (2008). Trust in Transition: Cross-country and firm evidence. Journal of Law Economics & Organization, October. Retrieved from http://libezproxy.syr.edu/login?url=http://proquest.umi.com/pqdweb?did=1550889401 & Fmt=7 & clientId=3739 & RQT=309 & VName=PQD

Randol, M. A. (2009). Terrorism information sharing and the nationwide suspicious activity report initiative: Background and issues for congress (CRS Report for Congress No. R40901) (p. 26). Washington, D.C. Congressional Research Service. Retrieved from http://stinet.dtic.mil/oai/oai? & verb=getRecord & metadataPrefix=html & identifier=ADA509767

Rauchhaus, R. W. (2009). Principal-Agent Problems in Humanitarian Intervention: Moral Hazards, Adverse Selection, and the Commitment Dilemma. *International Studies Quarterly*, 53(4), 871–884. doi:10.1111/j.1468-2478.2009.00560.x

Ray, I., & Chakraborty, S. (2004). A vector model of trust for developing trustworthy systems. In Samarati, P., Ryan, P., Gollmann, D., & Molva, R., editors, *Computer Security-ESORICS, Proceedings of the9th European Symposium on Research in Computer Security*, September 13-15, 2004, Sophia Antipolis, France. LNCS3193, Springer.

Razavi, M. N., & Iverson, L. (2006). A grounded theory of information sharing behavior in a personal learning space. In *Proceedings of the 2006 20th anniversary conference on Computer supported cooperative work* (pp. 459-468). Banff, Alberta, Canada: ACM. doi: 10.1145/1180875.1180946.

Rethemeyer, R. K. (2005). Conceptualizing and measuring collaborative networks. *Public Administration Review*, 65(1), 117-121.

Ridings, C. M., Gefen, D., & Arinze, B. (2002). Some antecedents and effects of trust in virtual communities. *The Journal of Strategic Information Systems,* 11(3-4), 271–295.

Roberts, A., & Roberts, J. M. Jr. (2006). *Police Innovations and the Structure of Informal Communication Between Police Agencies: Network and LEMAS Data*. Washington, D.C.: US Department of Justice Retrieved February 22, 2009 (http://www.ncjrs.gov/pdffiles1/nij/grants/216150.pdf).

Rocco, E. (1998). Trust breaks down in electronic contexts but can be repaired by some initial face-to-face contact. *In Proceedings of the SIGCHI conference on Human factors in computing systems* (pp. 496-502). Los Angeles, California, United States: ACM Press/Addison-Wesley Publishing Co.

Rocheleau, B. (1996). Interorganizational and interdepartmental information sharing. In G. D. Garson and S. S. Nagel, (Eds.) *Advances in social science and computers,* (pp.183-204). Greenwich, CN: JAI Press.

Rogers, E. M. (1995). *Diffusion of innovations*. Free Pr.

Rose, J., & Jones, M. (2005). The double dance of agency: A socio-theoretic account of how machines and humans interact. *Systems, Signs & Actions*, 1(1), 19–37.

Ross, W., & LaCroix, J. (1996). Multiple meanings of trust in negotiation theory and research: A literature review and integrative model. *International Journal of Conflict Management*, 7(4), 314-360. doi:10.1108/eb022786

Roundcount, T. (2010). *The perceptions of superintendents and emergency responders concerning the usefulness of Geographical Information Systems in Illinois school district's crisis response procedures*. Saint Louis University, United States -- Missouri.

Rousseau, D., Sitkin, S., Burt, R., & Camerer, C. (1998). Not so different after all: a cross-descipline view of trust. *Academy of Management Review*, 23(3), 393–404.

Rubin, H. J., & Rubin, I. (2005). *Qualitative interviewing: The art of hearing data*. Sage Publications, Inc.

Ruef, M., & Scott, W. R. (1998). "A multidimensional model of organizational legitimacy: Hospital survival in changing institutional environments." *Administrative Science Quarterly* 877-904.

Ruppel, C., Underwood-Queen, L., & Harrington, S. J. (2003). e-Commerce: The roles of trust, security, and type of e-Commerce involvement. *e-Service Journal*, 2(2), 25-45.

Ryan, D. (2006). "Getting the Word Out: Notes on the Social Organization of Notification*," *Sociological Theory*, vol. 24, pp. 228-254.

SAFECOM. (2011). Multi-band radio project of the Department of Homeland Security. Http://www.safecomprogram.gov/SAFECOM/currentprojects/mbr/

SAFECOM. (2011). U.S. Federal Emergency Management Agency, *SAFECOM Program*, www.safecomprogram.gov/default.aspx

Sales, N. A. (2010). Sales, Nathan Alexander, Share and Share Alike: Intelligence Agencies and Information Sharing (April 21, 2009). George Mason Law & Economics Research Paper No. 09-24; *George Washington Law Review*, Vol. 78, No. 2, pp. 279-352, February 2010. From SSRN: http://ssrn.com/abstract=1392917.

Sample Survey of Law Enforcement Agencies [Computer file], (2006). ICPSR04411-v1. Ann Arbor, MI: Inter-university *Consortium for Political and Social Research* [producer and distributor].

Sass, M. D. (2006). *Collaboration as information sharing: The effect of dispositional trust and situational perceptions of power on collaborative outcomes.* The George Washington University.

Sawyer, S., & Fedorowicz, J. (2012). Designing Collaborative Networks: Lessons Learned from Public Safety. *IBM Center for The Business of Government - Collaborating Across Boundaries Series*.

Sawyer, S., Fedorowicz, J., Tyworth, M., Markus, M. L., & Williams, C. B. (2007). A taxonomy for public safety networks. *Proceedings of the 8th annual international conference on Digital government research: bridging disciplines & domains* (pp. 240–241). Digital Government Society of North America.

Sawyer, S., & Rosenbaum, H. (2000). Social informatics in the information sciences: Current activities and emerging directions. *Informing Science*, *3*(2), 89–89.

Sawyer, S., Schrier, R., Fedorowicz, J., Dias, M., Williams, C., & Tyworth, M. (2012). Architectural patterns of US public safety networks: a fuzzy set qualitative comparison analysis. *Proceedings of the 13th Annual International Conference on Digital Government Research* (pp. 49–57). ACM.

Scholl, H. J. (2011). HICSS-44 44th Hawaii Int’l Conference on System Sciences E-Government TraCK January 4-7, 2011 The Grand Hyatt Kauai, Koloa, HI/USA. Hawaii Int’l Conference on System Sciences. Retrieved March 25, 2011, from http://faculty.washington.edu/jscholl/hicss44/Welcome.html

Schooley, B. L. (2007). Inter-organizational systems analysis to improve time-critical public services: The case of mobile emergency medical services. The Claremont Graduate University. Retrieved from http://proquest.umi.com/pqdweb?did=1390309161 & Fmt=7 & clientId=3739 & RQT=309 & VName=PQD.

Schoorman, F. D., Mayer, R. C., & Davis, J. H. (2007). An integrative model of organizational trust: Past, present, and future. *Academy of Management Review*, 32(2), 344-354. doi: Article.

Schutt, R. (2006). *Investigating the social world : the process and practice of research. 5th ed.* Thousand Oaks Calif.; London: Pine Forge Press; SAGE Publications.

Schutt, R. K. (2004). *Investigating the social world*. Pine Forge Press.

Scott, E. D. (2006). Factors influencing user-level success in police information sharing: An examination of Florida's FINDER system. Retrieved from http://proquest.umi.com/pqdweb?did=1251886251 & Fmt=7 & clientId=3739 & RQT=309 & VName=PQD.

Scott, W. R, & Backman, E. V. (1990). “Institutional theory and the medical care sector.” *Innovations in health care delivery: Insights for organization theory* 20:52.

Serra da Cruz, S., Chirigati, F., Dahis, R., Campos, M., & Mattoso, M. (2008). Using explicit control processes in distributed workflows to gather provenance. *In Provenance and Annotation of Data and Processes* (pp. 186-199). Retrieved February 22, 2009, from http://dx.doi.org/10.1007/978-3-540-89965-5_20.

Shaw, P. (1997). Intervening in the shadow systems of organizations Consulting from a complexity perspective. *Journal of Organizational Change Management,* 10(3), 235.

Singh, P., Park, I., Lee, J., & Rao, H. (2009). “Information sharing: A study of information attributes and their relative significance during catastrophic events.” *Cyber-Security and Global Information Assurance: Threat Analysis and Response Solutions*, IGI Publishers 27.

Sparrow, M. K., Moore, M. H., & Kennedy, D. M.(1992). *Beyond 911: a new era for policing*. Basic Books.

Stacey, R. (1996). *Complexity and creativity in organizations* (1st ed., p. 312). Berrett-Koehler Publishers.

Stair, R., & Reynolds, G. (2011). *Principles of information systems*. Course Technology.

Staples, D. S., & Webster, J. (2008). Exploring the effects of trust, task interdependence and virtualness on knowledge sharing in teams. *Information Systems Journal*, 18, 617 - 640. doi:10.1111/j.1365-2575.2007.00244.x

Stone, E. F. (1978). *Research methods in organizational behavior*. Scott, Foresman.

Strauss, A., & Corbin, J. (1990). *Basics of Qualitative Research*. Newbury Park: Sage.

Stvilia, B, Gasser, L., Twidale, M., & Smith, L. (2007). "A framework for information quality assessment." *Journal of the American Society for Information Science and Technology* 58(12):1720-1733. Retrieved April 23, 2011.

Suministrado, J. P. (2004). The emergent field of knowledge management: An overview. *Notes on Business Education, De La Sallee University - College of Business and Economics, Center for Business and Economics Research and Development (CBERD)*, 7(1), 6.

Swire, P. P. (2006). "Privacy and Information Sharing in the War on Terrorism." *Ohio State Public Law Working Paper No. 63.* Retrieved March 14, 2008 (http://ssrn.com/paper=899626).

Tashakkori, A., & Teddlie, C. (1998). *Mixed methodology: Combining qualitative and quantitative approaches* (Vol. 46). Sage Publications, Incorporated.

Thayer, J. B. (1889). Presumptions and the Law of Evidence. *Harvard Law Review*, 3(4), 141–166.

Thomas, J. (1985). Force field analysis: A new way to evaluate your strategy. *Long Range Planning*, 18(6), 54-59

Thomson, A. M. (1999). AmeriCorps organizational networks: Six case studies of Indiana AmeriCorps programs. National Service Fellows Program. *Report for the Corporation for National Service,* Washington, DC: Corporation for National and Community Service.

Thompson, E. D., & Kaarst-Brown, M. L. (2005). Sensitive information: A review and research agenda. *Journal of the American Society for Information Science and Technology*, 56(3), 245–257.

Thompson & Morgan. (2010). *Thompson-Morgan.com* Website. http://www.thompson-morgan.com/flowers/flower-plants/flowers-for-cutting-plants/lisianthus-blue-lagoon/p3897TM, accessed 12/5/2010).

Thompson, A. M., Perry, J. L., & Miller, T. K. (2008). Linking Collaboration Processes and Outcomes; Foundation for Advancing Empirical Theory. *In: Big Ideas in Collaborative Public Management.* Edited by Lisa Blomgren Bingham and Rosemary O' Leary. Armonk, N.Y: M.E. Sharpe Inc.

Thomson, A. M., Perry, J. L., & Miller, T. K. (2009). "Conceptualizing and measuring collaboration." *Journal of Public Administration Research and Theory* 19(1):23-56.

Thuraisingham, B. (2008) Chapter 1. Assured Information Sharing: *Technologies: Challenges and Directions, Intelligence and Security Informatics: Applications and Technique*, Editors: H. Chen and C. C. Yang, Springer-Verlag.

Tiwana, A. (2000). *The knowledge management toolkit: practical techniques for building a knowledge management system*. Upper Saddle River, NJ, USA: Prentice Hall PTR.

Tolbert, P. S., & Zucker, L. G. (1999). "The institutionalization of institutional theory." *Studying Organization: Theory & Method* 169-184.

Treglia, J. (2008*). "Two Cans on a String: Technical Social & Legal Barriers to Effective Information Sharing Among Federal, Tribal, State & Local Law Enforcement Agencies in the United States."* Poster in proceedings of iConference 2009 - iSociety: Research, Education, Engagement. University of North Carolina at Chapel Hill, NC, February 8-11, 2009.

Treglia, J. (2008a). *Improving intelligence information sharing between federal, state and local law enforcement agencies in the United States*. Unpublished manuscript.

Treglia, J. (2008b). Actionable factors affecting intelligence information sharing between federal, state and local law enforcement agencies in the United States. *Poster presented at the AGEP Academic Excellence Symposium*, Syracuse University.

Treglia, J. (2009). Two Cans on a String: Technical Social & Legal Barriers to Effective Information Sharing Among Federal, Tribal, State & Local Law Enforcement Agencies in the United States, *Poster in proceedings of iConference 2009 - iSociety: Research, Education, Engagement.* University of North Carolina at Chapel Hill, NC, February 8-11, 2009.

Treglia, J. (2010). A classification of agents and entities influencing law enforcement agencies in the United States. *Proceedings of the iConference on iMPACTS, poster. Presented at the iConference,* Urbana-Champaign, NC: *Ideals*.

Treglia, J. (2012). "Cooperation that Works – Lessons from the CNYICC; A Multi-jurisdictional Public Safety Communications Consortium." *NYSAC News (Winter).*

Treglia, J. V., & Park, J. S. (2009). Towards trusted intelligence information sharing. *Proceedings of the ACM SIGKDD Workshop on CyberSecurity and Intelligence Informatics* (pp. 45-52). Paris, France: ACM.

Treglia, J. V., McKnight, L. W., Kuehn, A., Ramnarine-Rieks, A., Venkatesh, M., & Bose, T. (2011). Interoperability by 'Edgeware': Wireless Grids for Emergency Response. In *Proceedings of the 2011 44th Hawaii International Conference on System Sciences (HICSS '11). IEEE Computer Society,* Washington, DC, USA, 1-10. DOI=10.1109/HICSS.2011.251

Treglia, J. V., McKnight, L. W., Venkatesh, M., Bose, T., Volos, H., Van Aardt, J., & McKeown, D. (2011). Wireless Grid Edgeware for Collaboration in Infrastructureless Wireless Networks, Intelligent Distributed Augmented Wireless Gateways (iDAWG), Neighborhood Notification and Advanced Situational Awareness Systems (ASAS*). TPRC 39th Research Conference on Communication, Information and Internet Policy, hosted by George Mason University School of Law, Arlington, VA* (p. 20). Presented at the TPRC: The 39th Research Conference on Communication, Information and Internet Policy, Arlington, VA: TPRC.

Treglia, J., Ramnarine-Rieks, A., & McKnight, L. (2010). Collaboration in a wireless grid innovation testbed by virtual consortium. *Networks for Grid Applications*: *Third International ICST Conference, Gridnets 2009, Athens, Greece, September 8-9, 2009, Revised Selected Papers* (p. 139). Springer.

Trist, E., & Murray, H. (1993), *The Social Engagement of Social Science: A Tavistock Anthology (vol. II)* , Philadelphia , University of Pennsylvania Press.

Trist, E. (1981). The evolution of socio-technical systems. *Occasional paper*, 2.

Turoff, M. (1970). “The design of a policy Delphi.” *Technological Forecasting and Social Change* 2(2):149-171).

Turoff, M. (2002). “Past and future emergency response information systems,” *Communications of the ACM* , 45, no. 4: 32.

United States. (2004). Federal law enforcement information on use of investigation and arrest statistics. Washington, D.C. *U.S. General Accounting Office*.

United States. Executive Office of the President, & United States. Assistant to the President for Homeland Security and Counterterrorism. (2006). *The federal response to Hurricane Katrina : lessons learned.* Washington, D.C.: White House.

United States. (2007; 2007b). Building the information sharing environment: Addressing the challenges of implementation: hearing before the subcommittee on intelligence, information sharing, and terrorism risk assessment of the committee on homeland security, U.S. House of Representatives, One Hundred Ninth Congress, Second Session, May 10, 2006. *Washington: U.S. G.P.O.*

United States. (2007c). Federal support for homeland security information sharing: role of the information sharing program manager: Hearing before the subcommittee on intelligence, information sharing, and terrorism risk assessment of the Committee on Homeland Security, House of Representatives, One Hundred Ninth Congress, First Session, November 8, 2005 (p. 58). *Washington: U.S. G.P.O*. Retrieved from http://www.gpoaccess.gov/congress/index.html.

USDEA. (2011). *United States Drug Enforcement Administration*. Agency mission, web page http://www.justice.gov/dea/agency/mission.htm. August 22, 2011.

USDHS. (2011). *"About." DHS.* Retrieved February 5, 2012 (http://www.dhs.gov/xabout/).

USDOD. (2007). *Department of defense information sharing strategy* (p. 24). Washington, D.C.: Department of Defense, Information Sharing Executive, Office of the Chief Information Officer.

USDOJ. (2004). Applying security practices to justice information sharing. Global justice information sharing initiative - *Security Working Group - United States Department of Justice*, Version 2.0, 124.

USDOJ. (2006). Applying wireless security practices to justice information sharing. Global justice information sharing initiative - *United States Department of Justice*, 124.

USDOJ. (2008). United States Department of Justice. *Federal Assistance from U.S. Department of Justice, FY 2008*, summary. Retrieved February 22, 2009, from http://www.usaspending.gov/faads/faads.php?datype=T & det ail=-1 & database=faads & fiscal_year=2008 & maj_agency_cat=15.

USDOJ. (2011). *"Programs: Justice Assistance Grant (JAG)."* Retrieved February 4, 2012 (http://www.ojp.usdoj.gov/BJA/grant/jag.html).

USDOJ BJS. (2006). U.S. Dept. of Justice, Bureau of Justice Statistics. Law enforcement management and administrative statistics (LEMAS): 2003 USDOT. (2011). "Research and Innovative Technology Administration (RITA) - United States Department of Transportation (USDOT, US DOT or DOT)." *U.S. Department of Transportation - Research and Innovative Technology Administration*. Retrieved November 28, 2011 (http://www.its.dot.gov/ng911/).

USFA. (2011). USFA search the national fire department census database. U.S. Fire Administration; National Fire Department Census Database. *Government Information*, February 11. Retrieved February 13, 2011, from http://www.usfa.dhs.gov/applications/census/

USSS (2011). United States Secret Service web site, *National Special Security Events*. http://www.secretservice.gov/nsse.shtml, Retrieved April 3, 2011.

Uzzi, B. (1997). Social structure and competition in interfirm networks: The paradox of embeddedness. *Administrative science quarterly*, 42(1), 35-67.

van de Wijngaert, L., & Blondia, C. (2004). Improving MIP handover latency using location information. *Transactions*, 45(10), 2246-2253.

van de Wijngaert, L., & Bouwman, H. (2009). “Would you share? Predicting the potential use of a new technology.” *Telematics and Informatics* 26(1):85-102.

Van Hoy, J. (1993). “Intraprofessional politics and professional regulation.” *Work and occupations* 20(1):90.

Vann, I. (2005). In Garson G. (Ed.), Testing the Rocheleau data sharing model on North Carolina law enforcement agencies. *Dissertation, United States -- North Carolina: North Carolina State University*.

Vaughn, R. B., Henning, R., & Siraj, A. (2003). Information assurance measures and metrics - state of practice and proposed taxonomy (p. 10 pp.). *Presented at the System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference on.*

Veil, S.R., Buehner, T., & Palenchar, M.J. (2011). “A Work-In-Process Literature Review: Incorporating Social Media in Risk and Crisis Communication.” *Journal of Contingencies and Crisis Management* 19(2): 110-122. Retrieved August 11, 2011.

Venezia, P. (2010). Why do we trust Google? | Internet integration - InfoWorld. *InfoWorld*. Online News, July 2. Retrieved December 18, 2010, from http://www.infoworld.com/t/internet-integration/why-do-we-trust-google-415?page=0,1

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). USER ACCEPTANCE OF INFORMATION TECHNOLOGY: TOWARD A UNIFIED VIEW. *MIS Quarterly*, 27(3), 425-478. doi:Article

Volos, H.I., & Bruehrer. (2010). “Cognitive Engine Design for Link Adaptation: An Application to Multi-Antenna Systems”, *IEEE Transactions on Wireless Communications*, vol. 9, no. 9, pp. 2902-2913, 2010.

Von Bertalanffy, L. (1972). The history and status of general systems theory. *The Academy of Management Journal*, 15(4), 407-426.

Waddock, S. (2011). We Are All Stakeholders of Gaia: A Normative Perspective on Stakeholder Thinking. *Organization & Environment*, *24*(2), 192–212.

Wade, M. (2009). *Theories used in IS research*.Wiki. Retrieved November 14, 2009, from http://www.fsc.yorku.ca/york/istheory/wiki/index.php/Main_Page

Walker, J., & Ostrom, E. (2007). Trust and reciprocity as foundations for cooperation: Individuals, institutions, and context. *Capstone Meeting of the RSF Trust Initiative at the Russell Sage Foundation*.

Walonick, D. S. (1993). *"General Systems Theory."* General Systems Theory. Retrieved May 25, 2011 (http://statpac.org/walonick/systems-theory.htm).

Wasserman, R. (2010). *Guidance for Building Communities of Trust*. Washington, DC: U.S. Dept. of Justice.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare fo the future: Writing a literature review. *MIS Quarterly*, 26(2).

Weick, K. E. (1984). Theoretical assumptions and research methodology selection. In F. W. McFarlan (Ed.), *The Information systems research challenge, Research colloquium* (Harvard University. Graduate School of Business Administration) (pp. 111-132). Boston, Mass: Harvard Business School Press.

Weimer, D. L., & Vining, A. R. (1992). *Policy Analysis: Concepts and Practice*. 2nd ed. Englewood Cliffs, N.J: Prentice Hall.

Weiss, J. A. (1987). "Pathways to cooperation among public agencies." *Journal of Policy Analysis and Management.* 7(1):94-117.

Weiss, R. S. (2004). In their own words: making the most of qualitative interviews. *Contexts*, 3(4), 44.

Westphal, I., Thoben, K.-D., & Seifert, M. (2008). Managing collaboration performance to govern virtual organizations. *Journal of Intelligent Manufacturing*, *21*, 311–320. doi:10.1007/s10845-008-0182-5

Whitehouse. (2007). *Report of the security clearance oversight group consistent with Title III of the Intelligence Reform and Terrorism Prevention Act of 2004.* Retrieved March 16, 2008, from http://www.whitehouse.gov/omb/pubpress/2007/sc_report_to_congress.pdf.

Wick, D., Franzoni, D., & Lustig, B. (Producers) & Scott, R. (Director). (2000). *"Gladiator" [Motion picture]*. United States: DreamWorks Home Entertainment.

Wieviorka, M. (1992). Case studies: History or sociology? In C. C. Ragin & H. S. Becker (Eds.), *What is a case? Exploring the foundations of social Inquiry* (pp. 159-172). Cambridge, UK: Cambridge University Press.

WiGiT. (2010). *Wireless Grids Innovation Testbed*, Syracuse University School of Information Studies, Wireless Grids Lab, Hinds Hall, Syracuse, NY.

Willem, A., & Buelens, M. (2007). Knowledge sharing in public sector organizations: The effect of organizational characteristics on interdepartmental knowledge sharing. *Journal of Public Administration Research and Theory*, 17(4), 581-606.

Williams, C., Dias, M., Fedorowicz, J., Jacobson, D., Vilvovsky, S., Sawyer, S., & Tyworth, M. (2009). The formation of inter-organizational information sharing networks in public safety: Cartographic insights on rational choice and institutional explanations. *Information Polity*, 14(1), 13-29. doi:10.3233/IP-2009-0170

Williams, C. B., Fedorowicz, J., & Tomasino, A. P. (2010). Governmental factors associated with state-wide interagency collaboration initiatives. *Proceedings of the 11th Annual International Digital Government Research Conference on Public Administration Online: Challenges and Opportunities* (pp. 14-22). Puebla, Mexico: Digital Government Society of North America.

Wilson, T. D. (2010). Information sharing: an exploration of the literature and some propositions. *Information Research*, 15(4), 9.

Winkler, M. M. (2008). When "extraordinary" means illegal: International law and European reaction to the United States rendition program. *Loyola of Los Angeles International and Comparative Law Review*, 30(33), 44.

Wood, D., & Gray, B. (1991). Towards a comprehensive theory of collaboration. *Journal of Applied Behavioral Science* 27: 139–62.

Xiong, L. (2005). *Resilient reputation and trust management: Models and techniques. Georgia Institute of Technology*.

Xiong, L., & Liu, L. (2004). Peer Trust: supporting reputation-based trust for peer-to-peer electronic communities. *Knowledge and Data Engineering, IEEE Transactions on*, 16(7), 843-857. doi:10.1109/TKDE.2004.1318566.

Yang, C. C. (2008). Information sharing and privacy protection of terrorist or *criminal social networks. Intelligence and Security Informatics, 2008. ISI 2008. IEEE International Conference on (pp. 40-45). Presented at the Intelligence and Security Informatics, 2008. ISI 2008. IEEE International Conference on.* doi:10.1109/ISI.2008.4565027

Yang, T. M., & Maxwell, T. A. (2011). Information-sharing in public organizations: A literature review of interpersonal, intra-organizational and inter-organizational success factors. *Government Information Quarterly*, 28(2), 164–175.

Yin, R. K. (2008). Case study research: Design and methods. 4th ed. Sage Publications, Inc.

Young, S. J., & Jamieson, L. M. (2001). Delivery methodology of the Delphi: a comparison of two approaches. *Journal of Park and Recreation Administration,* 19(1), 42–58.

Young-Ybarra, C., & Wiersema, M. (1999). Strategic Flexibility in Information Technology Alliances: The Influence of Transaction Cost Economics and Social Exchange Theory. *Organisation Science*, 10(4): 439-459.

Yousuf, M. I. (2007). "The Delphi technique." *Essays in Education* 20:80-9.

Zaheer, A., McEvily, B., & Perrone, V. (1998). Does trust matter? Exploring the effects of interorganizational and interpersonal trust on performance. *Organization Science,* 9(2), 141-159.

Zargar, S. T., Weiss, M. B. H., Caicedo, C. E., & Joshi, J. B. D. (2009, December*). Security in Dynamic Spectrum Access Systems: A Survey,* Working Paper. Retrieved October 9, 2012, from http://d-scholarship.pitt.edu/2823/

Zhang, H. (2005). Algorithms for performance and trust in peer-to-peer systems. *Dissertation, University of Southern California*. Retrieved from http://proquest.umi.com/pqdweb?did=1027494451&Fmt=7&clientId=3739&RQT=309&VName=PQD

Zhang, J., Dawes, S. S., & Sarkis, J. (2005). Exploring stakeholders' expectations of the benefits and barriers of e-Government knowledge sharing. *The Journal of Enterprise Information Managemen*t, 18(5), 548−567.

Zheng, L. (2009). *Leadership Behaviors in Cross-boundary Information Sharing and Integration: Comparing the US and China*. ProQuest.

Zheng, L., Dawes, S., & Pardo, T. A. (2009). Leadership behaviors in cross-boundary information sharing and integration: comparing the US and China. *Proceedings of the 3rd International Conference on Theory and Practice of Electronic Governance (pp. 43-50). ACM.*

Zheng, J., Veinott, E., Bos, N., Olson, J. S., & Olson, G. M. (2002). Trust without touch: jumpstarting long-distance trust with initial social activities. *Proceedings of the SIGCHI conference on Human factors in computing systems: Changing our world, changing ourselves* (pp. 141–146). ACM.

VIII. End

Vita

Joseph V. Treglia

Ph.D. in Information Science & Technology, *Syracuse University,* May 2013

Master's Degree in Information Resources Management *Syracuse University,* 1995

Graduate Certificate in Telecommunications & Network Management, SU, 1994

Bachelor's Degree in Political Science/Liberal Arts *Syracuse University,* 1988

Short Biography:

Joseph Treglia is Special Assistant to the Sheriff for the Madison County Office of the Sheriff. He has 25 years' experience in law enforcement and criminal justice and was a Director for a large nonprofit human services agency (ARISE, Inc., serving people with disabilities) in Central New York. He is an Instructor in both the School of Information Studies and Martin J. Whitman School of Management at Syracuse University and Assistant Director of the Wireless Grids Lab. He has a PhD in Information Science & Technology and Master of Science in Information Resources Management both from Syracuse University's School of Information Studies (iSchool). He was a National Science Foundation (NSF) Scholar in the Federal Cyber Service Program (SFS). He founded United Information Services, an internet services and information systems consulting group. He has taught or prepared courses on Homeland Security, Organizational Information Security and Management Principles, among others. His work has been published and presented locally and internationally including: ACM SIGKDD Workshop on Cyber Security and Intelligence Informatics (CSI-KDD) in Paris, France; International Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (ICST) Conference in Athens, Greece, the Hawaiian International Conference on System Sciences (HICSS), Hawaii; Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), New Orleans, LA, and the NYS Cyber Security Conference, Albany, NY. His research interests include crisis response and management, trusted information sharing, information assurance, cyber security issues, intelligence and information sharing within and across organizations.

ADJUNCT INSTRUCTOR- SYRACUSE UNIVERSITY SCHOOL OF INFORMATION STUDIES AND WHITMAN SCHOOL OF MANAGEMENT

2012 – 2013	Management Principles (Graduate level)
2008 – 2010	Introduction to Management Information Systems (MIS) UG
1993 – 2010	Organizational Information Security, IT Procurement, and Office Systems Design & Management at graduate and undergraduate levels

ASSISTANT DIRECTOR – WIRELESS GRIDS LABORATORY

Syracuse University based research consortium. Assist Director with staff oversight and operation of the lab; identify and pursue new projects, grant proposals and coordinate multidisciplinary research projects and activity. Web site *http://wglab.net,* 2007 to present

MADISON COUNTY SHERIFF'S OFFICE

Special Assistant to the Sheriff, County Law Enforcement Agency. Involved in proposal and policy development, program development, and special projects. 2002 to present

DIRECTOR - INTEGRATED RECREATIONAL SERVICES & MADISON COUNTY PROGRAMS

ARISE, Inc., Syracuse, NY. Direct budget and operations for Madison County Programs and Recreation Programs in Central New York. Directed and Managed Day Hab, Res Hab and Respite programs in Madison and Oneida County. Managed Federal and State Grant Projects. Create, oversee and coordinate design, development, instruction of programs and services for persons with developmental disabilities. Insure Quality in programs in accordance with Federal, State and local standards. Liaison with government, private and not-for-profit agencies and the public. Sought grant opportunities & funding from government and non-government entities. Directed ARISE & SKI, ARISE at the Farm, and created the ARISE & FISH program, and after-school programs among others, 2002 – 2006.

Publication and Presentations:

Treglia, Joseph. "Three Essays on Law Enforcement and Emergency Response Information Sharing and Collaboration: An Insider Perspective." Dissertation, Syracuse University, New York, United States, 2013.

Treglia, Joseph. "Cooperation that Works – Lessons from the CNYICC; A Multi-jurisdictional Public Safety Communications Consortium." *NYSAC News* (Winter), 2012.

Marsden, Janet, Joseph Treglia, and Lee McKnight. "Dynamic Emergency Response Communication: The intelligent Deployable Augmented Wireless Gateway (iDAWG)." in *Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), 2012 IEEE International Multi-Disciplinary Conference on*. New Orleans, USA: IEEE, March 6-8, 2012. (forthcoming)

Treglia, Joseph, McKnight, Lee, Venkatesh, Murali, Bose, Tamal, Volos, Haris, Van Aardt, Jan, McKeown, Don, Mishra, Sumita, Lee, Myung. "Social Emergency Response Technology

Policy." in *TPRC 38th Research Conference on Communication, Information and Internet Policy, hosted by George Mason University School of Law, Arlington, VA*. Arlington, VA, September 23-25, 2011.

Treglia, Joseph and Venkatesh, Murali. "iDAWG: Intelligent Deployable Augmented Wireless Gateway." Presentation to *National Law Enforcement Telecommunications System (NLETS) Annual Business Meeting,* June 27-28, 2011. Published in proceedings.

Treglia, Joseph, McKnight, Lee, Kuehn, Andreas, Ramnarine-Rieks, Angela, Venkatesh, Murali and Bose, Tamal. "Interoperability by 'Edgeware': Wireless Grids for Emergency Response." in Proceedings of *HICSS-44, 44th Hawaii Int'l Conference on System Sciences, E-Government Track*, January 4-7, 2011, The Grand Hyatt Kauai, Koloa, HI/USA.

McKnight, Lee W., Treglia, Joseph, Kuehn, Andreas. "Wireless Grids or Personal Infrastructure: Policy Implications of an Emergent Open Standard." in *TPRC 38th Research Conference on Communication, Information and Internet Policy*, hosted by George Mason University School of Law, Arlington, VA, October 1-3, 2010.

Treglia, Joseph. "Developing Practical Cyber Security Policy Using a Multidimensional Approach." Presentation *accepted for13th Annual 2010 NYS Cyber Security Conference*, Empire State Plaza Convention Center - Albany, NY, June 16 - 17, 2010.

Treglia, Joseph. "A Classification of Agents and Entities Influencing Law Enforcement", Poster at *iConference 2010.* University of Illinois at Urbana-Champaign, Il, February 3-6, 2010.

Treglia, Joseph, Ramnarine-Rieks, Angela and McKnight, Lee. "Collaboration in a Wireless Grid Innovation Testbed by Virtual Consortium," *Networks for Grid Applications*, 2010, pp. 139-146.

Treglia, Joseph V. and Park, Joon S. "Towards trusted intelligence information sharing." In *Proceedings of ACM SIGKDD Workshop on Cyber Security and Intelligence Informatics (CSI-KDD), the 15th Conference on Knowledge Discovery and Data Mining*, Paris, France, June 28 - July 1, 2009.

Treglia, Joseph. "Motivating People to Adopt Information Security Practices in Organizations." Presentation *in Proceedings of 12th Annual 2009 NYS Cyber Security Conference*, Empire State Plaza Convention Center - Albany, NY, June 3 - 4, 2009.

Treglia, Joseph. "Two Cans on a String: Technical Social & Legal Barriers to Effective Information Sharing Among Federal, Tribal, State & Local Law Enforcement Agencies in the United States," Poster *in proceedings of iConference 2009 - iSociety: Research, Education, Engagement.* University of North Carolina at Chapel Hill, NC, February 8-11, 2009.

Ho, S. M. and Treglia, J.V. Roundtable Discussion - "Feasibility Discussion on Identifying Possibility for a National Behavioral Anomaly Detection Platform." *In proceedings of 4th Annual iConference on iSociety: Research, Education and Engagement, University of North Carolina*, Chapel Hill, NC, February, 8-11, 2009.

Treglia, Joseph. "Actionable factors affecting intelligence information sharing between federal, state and local law enforcement agencies in the United States." *Poster presentation at the AGEP Academic Excellence Symposium*, Syracuse University, June 11, 2008. Received award of Honorable Mention.

Treglia, Joseph. "Focus Group Findings on Early Wireless Grid Adopters." *Presented at 4th Wireless Grids Research Workshop: Research on the Wireless Grid Innovation Experience*. Syracuse University CASE Center, October 12, 2007.

Treglia, Joseph. "Advancing Integrated Recreational Opportunities in Central New York." *The 1st Statewide Conference on Health & Wellness for Adults with Disabilities: Empowerment through Healthier Lifestyles. Sponsored by Centers for Disease Control and Prevention, U59/CCU 203351 and the New York State Department of Health*, , Albany Marriott, Albany, NY. April 15-16, 2004

"Standard Practices Manual for Processing Finger printable Criminal Cases." Published by *New York State Division of Criminal Justice Services, Office of Justice Information Services*, Albany, NY, 2001.

Treglia, Joseph V., "Monitoring How Children Use the Internet," Post-Standard, The, Syracuse, NY. 1997, April 10 (67).

Grants and Projects: $7 million awarded in over more than 37 projects and proposals

Professional Certifications, Training, and Relevant Other Experience:

- Certificate in University Teaching (2011)
- General Topics Instructor, New York State Bureau of Municipal Police
- Crisis Negotiator Training by Federal Bureau of Investigation (FBI) I & II
- Youth Officer, State of New York Police Juvenile Officers Association
- Certified Corrections officer, New York State Department of Corrections
- Dale Carnegie Communication Training & Public Speaking
- Drug Abuse Resistance Education Instructor (DARE)
- John Reid Schools on Basic & Advanced Interviewing
- Interviewing Sexually Abused Children, University of Delaware
- Project Adventure - Team Building & Group Facilitation for Adults & Youth
- Office of Justice Programs (OJP) Reviewer, 2010