LOCAL COLLABORATION IN DAY-TO-DAY INCIDENT RESPONSE WITHIN THE HOMELAND SECURITY ENTERPRISE

DW Davis, PhD, Supervisor

PSAA: 675-700

November 2022

About the Capstone Project
The Bush School of Government and Public Service, Texas A&M University

About the Project

This report is the product of two academic semesters of work by a team of graduate students enrolled in the Executive Masters of Public Service and Administration program at the Bush School of Government and Public Service at Texas A&M University. This coursework and the corresponding project allowed students to tackle a real-world problem designed to test the knowledge and abilities developed through their prior courses and professional experiences. This project was completed with the support of Hexagon Safety, Infrastructure and Geospatial Division and overseen by Bush School faculty member Dr. Danny W. Davis.

Capstone Team

Chuck Bondurant

Stephanie Brown

David Dedo

Jared Harwell

Tiffany Huff

J.R. Jones

Chris Kelley

Marilynn Larson

Joe Mabry

Josey Mathews

Bart Priest

Stephanie Reyes

Paul Schecklman

TABLE OF CONTENTS

ACRONYMS

CISA	Cybersecurity & Infrastructure Security Agency
DHS	Department of Homeland Security
DOJ	Department of Justice
EMS	Emergency Medical Services
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FOUO	For Official Use Only
GETS	Government Emergency Telecommunications Service
HSPD-5	Homeland Security Presidential Directive - 5
IAP	Incident Action Plan
ICS	Incident Command System
IoT	Internet of Things
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
ISE	Information Sharing Environment
LES	Law Enforcement Sensitive
NGOs	Non-governmental Organizations
NIMS	National Incident Management System
NIST	National Institute of Standards & Technology
NRF	National Response Framework
OEC	Office of Emergency Communications
PPD-8	Presidential Policy Directive - 8
S&T	DHS Science & Technology Directorate
SCIP	Statewide Communication Interoperability Plan
SEOC	State Emergency Operations Center
SIEC	Statewide Interoperability Executive Subcommittee
SWIC	Statewide Communication Interoperability Coordinator
TXDSHS	Texas Department of State Health Services
UHF	Ultra High Frequency

USDA	United States Department of Agriculture
VHF	Very High Frequency
WPS	Wireless Priority Service

EXECUTIVE SUMMARY

The Bush School of Government and Public Service was engaged by Hexagon Safety, Infrastructure, and Geospatial division to complete a research project exploring daily information sharing and interagency interoperability. This project was conducted by thirteen graduate students enrolled in the Executive Masters of Public Service and Administration program at the Bush School under the guidance and supervision of Danny Davis, Ph.D., in fulfillment of their Graduate Capstone Research Project. The project began in June of 2022 and was completed by November 2022. To explore impediments to interagency interoperability in public safety daily functions, the group identified three primary areas of focus. First, policies and political barriers were examined. Second, technological solutions and shortcomings were identified. Lastly, organizational and professional cultures were explored. These areas were researched utilizing existing literature, case studies, and legislation and by conducting interviews with experienced practitioners. The focus of this project was primarily based on the American system of grassroots, bottom-up characteristics within emergency services.

Consistent, sustained information sharing is vital to emergency operations. Every day, routine calls for service may require multi-agency cooperation.

Specific incidents may quickly require a greater number of partners from state, local, and federal entities to work in a coordinated effort. The ease, or difficulty, with which information is shared can have various consequences or outcomes. Communication, coordination, connectivity, and collaboration are vital to both daily incident response and major disasters. Political, cultural, and technical barriers may exist that render an inefficient and ineffective information sharing and response. This project seeks to identify common barriers and make recommendations to remedy collaboration and information-sharing issues while identifying areas of necessary further research.

Throughout the research, a common barrier identified was that of cost. This issue was especially prominent for smaller-sized agencies. Technological improvements and system upgrades require substantial capital investments. With competitive local and state budgets, significant investment in these areas proves difficult. Conversely, talent acquisition, development, and retention are other shared impediments. Turnover due to pay discrepancies or organizational advancement can hinder an agency's ability to develop collaborative networks and seek creative improvements. The training required to operate certain technology systems is significant. To advance existing and future systems, agencies must rely on capable practitioners.

Technological advancements are welcomed mainly as a positive occurrence but can also present challenges. Systems may bring forth sizable learning curves and fragmented implementation. Systems may have capable information-sharing features but lack operative capabilities due to these training requirements and focused implementation. This challenge can create reluctance to utilize new systems or technological solutions. Throughout our interviews, practitioners cited the need to improve current technology efficiencies instead of simply replacing systems with more complexities. Technological solutions remain one piece of the overall issue. Leadership and relationships appear to play significant roles in an agency's ability or willingness to share data and work collaboratively. These collaborative networks hold the potential to become coalitions, offering vast solutions with shared funding agreements. Agencies need to place the right people in the same room to work together on forming mutually beneficial and trusted relationships. Often, agencies are concerned with safeguards and what may happen to their data once it leaves their own systems.

There is an array of solutions that can begin addressing information-sharing barriers and increase collaborative efforts. Agencies and stakeholders should develop solutions-based coalitions that reduce operating costs. Agreements can spur information-sharing expansion through financial incentives. Agencies

and vendors should also focus on expanding or refining current technology rather than creating entirely new systems. Mandating specific technology and information-sharing capabilities deserves further attention as well. Agencies within specific regions should hold real-time, multi-jurisdiction, and multi-discipline training that identifies deficiencies and areas where collaboration can provide significant solutions. Since most existing guidance and literature pertains to major disasters, more focus should be placed on collaborative networks or single entities to identify best practices and trends and further realize solutions for daily operations.

The issue of information sharing and interoperability is more complex than anticipated due to the diverse operating environments. Within our research, we identified agencies that are seemingly pushing the boundaries of existing technology and software due to strong leadership, creative talent, and competition. Conversely, even within the same region, other organizations simply lack the support or energy to make substantive or necessary changes. In these areas, many believe the only way to pursue change would be through legislation that mandates funding, collaboration, or operational capabilities. Overall, our team has found that there is likely no all-encompassing solution to these issues. Interested parties must recognize the areas in which they are operating and what

complexities exist. A more nuanced approach based on region, funding, and political support may be highly effective. Leaders and stakeholders must balance existing state and federal guidance with the specific realities of each jurisdiction. The grassroots, bottom-up environment of American emergency operations is clearly evident. To this end, decision-makers should remain current in laws, regulations, cultures, and assets of their specific country, state, or region. Improving information sharing and interagency collaboration will largely depend on both human and technological elements.

INTRODUCTION

Problem Statement

In day-to-day incident response, a single agency can generally overcome the challenges present at most incidents. However, specific local, state, and even national incidents may require a multi-agency response. During these types of incidents, interagency interoperability is critical. Political, cultural, technical, and operational barriers may exist within the homeland security enterprise that can contribute to an inefficient and ineffective response. Communication, coordination, connectivity, and collaboration are vital to daily incident response and disasters.

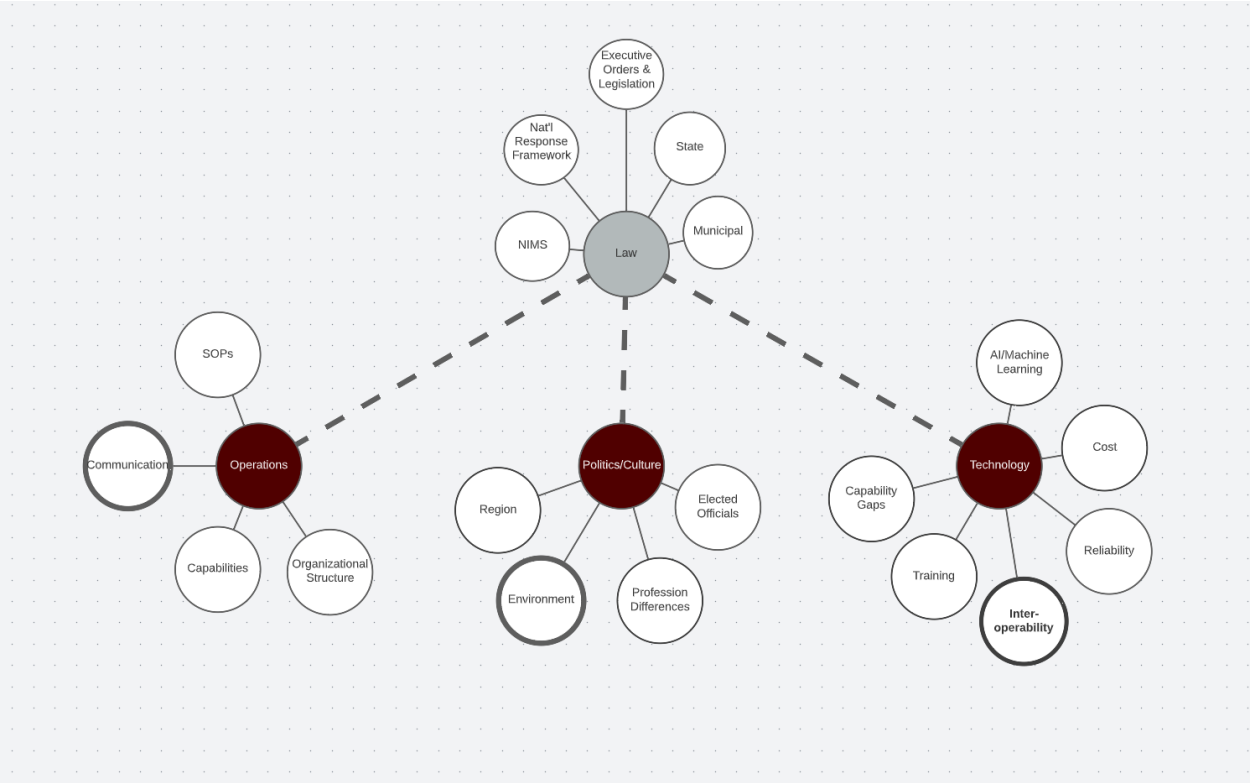
Research Design & Methodology

This research was conducted over two semesters as a requirement for graduation from the Executive Master of Public Service and Administration program at the Bush School of Government and Public Service. Thirteen individuals comprised the entire capstone team. However, based on its size, sub-groups were formed to tackle specific facets of the research problem and their related research questions. After reviewing the problem statement and completing a cursory review of the body of literature, the team developed figure 1 to demonstrate its understanding of the elements which impact interoperability and collaboration. This understanding assisted in developing the following research questions:

- What impact do politics and culture have on interagency interoperability in a day-to-day setting?
- What is the role of technology in interagency interoperability in a day-to-day setting?
- What is the impact of operations on interagency interoperability in a day-to-day setting?

Groups of three were formed and assigned to a specific research question. The remaining four individuals assisted in compiling a review of the relevant literature and supporting the teams' research—this larger group managed administrative tasks, presentation development, interviews, and editing.

Figure 1, Issues that Impact Interoperability



A significant element of this capstone project is its literature review. Through this process, teams were able to leverage a robust general body of research, as multi-agency interoperability is one of the long-standing questions within the public safety enterprise. Relevant case studies of federal, state, and local organizations and events were identified and studied to determine common characteristics related to interoperability. The geographical focus of this project is predominately centered around issues in the United States, although findings from the international community have been incorporated as deemed appropriate. The review of applicable statutes and policies centers on the federal level for a more overarching approach. Still, the research also includes state and local policies to demonstrate strengths and weaknesses in current legislation at all levels.

Semi-structured interviews were conducted with a representative from six different agencies across the United States, varying in size, operation and jurisdiction. The purpose of the interviews was to gather detailed information and understand any political, cultural, technological, and operational barriers that may exist within each respondent's agency and how they might impact interagency interoperability in a day-to-day setting. Before commencing these interviews, respondents were provided the complete list of interview questions, included below, and the problem statement developed for the project. Respondents also consented to the group's use of anonymized quotes and transcripts, as contained

in **Appendix A.** Maintaining confidentiality of information collected from respondents ensures that only the investigators can identify individual participants' responses. “The convention of confidentiality is upheld as a means to protect the privacy of all persons, to build trust and rapport with study participants, and to maintain ethical standards and the integrity of the research process” (Baez 2002). Therefore, respondents’ names and affiliated agencies shall remain anonymous.

Interviews were conducted virtually using the Zoom meeting platform and recorded with the respondent's consent for note-taking purposes. The average interview lasted for 45 minutes. Following the conclusion of the interviews, the team analyzed the transcripts to identify common themes and critical insights relevant to the problem statement and related research questions.

The research design and methodology were not immune from limitations. One such limitation is a lack of pertinent literature related to the day-to-day operations of public safety agencies and organizations; much of the current body of research focuses on the response to significant incidents or is more general in nature. Additionally, the team completed this project in partial fulfillment of the requirements for graduation. As such, the timeline for the project was compressed. Another limitation is the potential biases from the research group composition. The groups are made up of a large number of public servants and

the majority of the team is from Texas. These factors may impact research and findings.

Federal Doctrine/Legal Landscape

This section provides a historical context of emergency management and how it has evolved from a broad and all-encompassing definition to a focused guide for the homeland security enterprise in establishing, exercising, refining, and maintaining systems used for emergency response and recovery.

National Response Framework

The National Response Framework (NRF) serves as a manual on how the Nation should react during various times of emergency and disaster. It identifies scalable, flexible and adaptable coordinating structures to align key roles and responsibilities (Federal Emergency Management Agency 2021; hereafter FEMA). The management of situations ranging from significant but merely local, to massive terrorist attacks or devastating natural catastrophes, are covered in detail in this Framework (Department of Homeland Security 2019; hereafter DHS). This guidance also explains how response activities are combined across all stakeholders, including all levels of government, non-profit organizations (NGOs), and the private sector.

In order to address domestic incidents, the NRF develops a solitary, all-inclusive strategy. The purpose of the NRF is to provide a foundational framework that will mitigate the impacts of terrorist attacks, significant disasters, and other emergencies by directing users how to prepare for, react to, and recuperate from them (FEMA 2021). It gives a practical, national-level guidance framework and set of steps to follow (Malone and Hildebrand 2022). In reaction to a threat, in advance of a large event, or in the wake of an occurrence necessitating a concerted federal response, the NRF may be implemented as needed. A situation's specific operational and information-sharing needs may be met with the greatest degree of flexibility possible by selective adoption via the activation of the NRF components. This makes it possible for different federal, state, municipal, tribal, private-sector, and other nonprofit agencies to cooperate effectively.

National Incident Management System

The National Incident Management System (NIMS) is a framework that provides a systematic nationwide approach to the management of incidents. The scalability and flexibility of NIMS allows it to be applicable in all four phases of emergency management (United States Department of Agriculture 2004; hereafter USDA). The system provides guidance for federal, state, and local responders to coordinate a consistent response to an incident of any size or scope. NIMS has six

components that lay the foundation for the systematic approach, including: preparedness; supporting technologies; management and command; ongoing maintenance and management; communication and information management; and resource management.

NIMS ensures preparedness by training personnel and carrying out exercises. It ensures that personnel qualify for the tasks and meet certification standards. It provides a standardized approach to dispatch, describe, track, mobilize, and recover resources after an incident. It has an information system that enables resource tracking, data display, and record keeping. The Incident Command System has various features that allow effective management of incidents. They include accountability, common terminology, reliance on Incident Action Plan, position titles, and organizational resources like major equipment and personnel (USDA 2004).

Robert T. Stafford Disaster Relief and Emergency Assistance Act

The *Robert T. Stafford Disaster Relief and Emergency Assistance Act of 1988*, known as the Stafford Act, details how the United States responds to disasters. The Stafford Act amended the *Disaster Relief Act of 1974* and defined significant emergency and disaster declarations, thus giving the President power to assist in a disaster or emergency (Bazen 2005). This allows the President to have access to the disaster relief funds and assistance established by Congress.

After an emergency declaration is formalized, FEMA obtains the power to mobilize and coordinate relief funds and resources to help the states and local governments in need.

Title 44 - Emergency Management and Assistance

Chapter 1 of *Title 44 - Emergency Management and Assistance* outlines the procedures and policies to be followed by the Federal Emergency Management Agency (FEMA) in the adoption of rules. Under the Mitigation Directorate of FEMA, Title 44 outlines the processes of identifying and assessing the risks that are presented by natural or technological disasters (Kapucu, Augustin and Garayev 2009). Furthermore, FEMA establishes the policies for mitigations and program implementation strategies designed to alleviate or reduce loss of life and property from disasters. Title 44 outlines the procedures for sharing disaster risk information to other federal, state, and local agencies to promote a coordinated approach to hazards at all levels (Kapucu, Augustin and Garayev 2009). Title 44 improves interoperability by formalizing policies and procedures to be followed by federal, state, and local agencies in the arena of disaster recovery.

The Homeland Security Act of 2002

The *Homeland Security Act of 2002* was passed by the U.S. Congress in the wake of the September 11th terrorist attacks. The legislation created the

Department of Homeland Security (DHS), which consolidated twenty-two federal agencies and offices into a single organization. DHS is a cabinet-level agency responsible for protecting the U.S. homeland from terrorist attacks, natural disasters, and other incidents. As outlined within the legislation, the mission of DHS is to "prevent terrorist attacks, protect the nation's critical infrastructure, and respond to natural disasters."

Other law provisions include establishing an executive branch interagency coordinating council to help manage the response to emergencies and creating new grant programs to support emergency preparedness and response. The Act created numerous new agencies within the department, including FEMA, responsible for coordinating disaster relief efforts across all levels of government. Overall, the *Homeland Security Act of 2002* was successful legislation that created several new agencies and strengthened existing ones to protect the nation from terrorist attacks and other emergencies. It has increased security at U.S. borders, airports, and seaports and enhanced information sharing and coordination between federal, state, and local law enforcement agencies.

Presidential Directive 8 National Preparedness

Presidential Policy Directive–8: National Preparedness (PPD–8), outlines how U.S federal agencies should prepare for incidents. The directive requires that DHS coordinate with other Federal, State, Local, Tribal agencies and

governments to establish a National preparedness goal. The objective of PPD–8 is to ensure the coordination and implementation of all-hazard preparedness. This increases the Nation's preparedness in preventing, responding, and recovering from any range of disaster or emergency. The goal is achieved by providing effective, timely, and efficient delivery of federal preparedness assistance to the state and local governments. By promoting multiagency coordination at all levels of the government, the PPD–8 ensures that interoperability is accomplished in emergency and disaster incidents and that emergency responders can communicate and share information timely and effectively.

The purpose of the *Homeland Security Presidential Directive–5* (HSPD–5) was to improve the U.S ability to manage domestic incidents through a single and comprehensive national incident management system. The policy establishes that to effectively prepare, respond and recover from major disasters and terrorist attacks as well as other emergencies, the government should establish a single and comprehensive approach to the incidents. The objective of the HSPD-5 is to ensure that all government levels can effectively and efficiently work together on a national approach to incidents. Furthermore, the directive requires that the Federal government recognize the role of NGOs and the private sector in planning and responding to emergencies and major disasters.

As a result, the Secretary of State coordinates with all sectors to ensure that adequate and effective planning, training, equipment, and inter-agency partnerships are in place to address the incidents as they occur. By establishing a single comprehensive national approach to disasters, HSPD-5 ensures that every response agency and public safety organization has a single overarching policy and procedure to effectively and efficiently coordinate the various agencies (Noran and Bernus 2011). This helps to achieve interoperability through information sharing and comprehensive planning and management of disasters.

TECHNOLOGY

Technology is a critical component of any collaboration effort in day-to-day incident response. This section will provide an overview of the literature related to technological solutions and present the related scope and findings of the research.

Current Technological Capabilities and Trends

Alsamhi et al. (2021) propose technology providing real-time information concerning delivering emergency services leveraging the Internet of Things (IoT). Oracle (2022) defines IoT as "the network of physical objects—'things'—that are embedded with sensors, software, and other technologies to connect and exchange data with other devices and systems over the internet." IoT provides many capabilities, including advanced technology such as drone edge intelligence. The advantages include gathering and processing data, expanding wireless coverage, delivering medical emergency assistance, providing real-time incident information, and obtaining data from areas that are impossible for humans to reach. This type of technology in incident response is highly dependent on reliable network connectivity. Connectivity between IoT, including drones and wearable devices, such as a smartwatch, can aid in search-and-rescue operations and incident response in real-time.

Another area of relevant literature explores the use of social media as a tool in emergency management. Di Talia and Antonioni (2022) find that the prevalence of social media platforms creates an opportunity to integrate information posted by citizens with the emergency management process. Through their work, the authors explore the "Civil Protection Emergency System model" designed for the Italo-Croatian decision support system developed in the Interreg project E-CITIJENS" (577). This model includes key steps that allow the system to identify and analyze significant social media posts that can provide Civil Protection authorities with additional real-time data regarding potential or ongoing emergencies in a designated geographical area" (577).

Ongoing assessments of technology are essential to ensure systems align with current needs. Wang et al. (2020) find that many systems, such as high-definition maps and 3D technology used for live broadcasting, are no longer sufficient to address current needs. Instead, advanced technology, such as mission cognitive wireless emergency networks, can better facilitate urgent decision-making during an emergency. Interagency communication is reliant on robust, up-to-date infrastructure. Emergency communication infrastructures supporting rescue situations require reliable communication channels between victims, responders, and public safety command centers (Wang et al. 2020).

Technological Challenges

Buchanan et al. (2021) conducted a semi-structured survey of 63 rural first responders to explore the use and communications technology issues and needs of rural first responders across four disciplines: Communications Center and 911 Services, Emergency Medical Services, Fire Service, and Law Enforcement. Researchers sorted interview data into distinct categories relating to problems and needs using qualitative data analysis. The results reflected that the most significant issues for rural first responders were reliable coverage/connectivity, interoperability, implementation and information technology infrastructure, and physical ergonomics. Although this research reflects a need to address these current problems, the data also shows an interest "in new technology that leverages real-time technology and location tracking" (817). Buchanan et al. (2021) also consider implications for researchers and developers of public safety communication technology.

The Cybersecurity and Infrastructure Security Agency (CISA) was established to bring DHS into the next generation of cybersecurity and to monitor and study technology that could support functions within the Homeland Security enterprise. CISA has conducted many studies involving the successes and failures of communication before, during, and in response to major disasters and incidents. These studies show how out-

of-the-box thinking and flexibility could be the key to opening up new frontiers of technology for communication in public safety and how the public can play a role.

Further, a survey published by the National Institute of Standards and Technology (2022) concluded that technology might be a burden and that future technology must consist of more usable, functional, and cost-effective versions of current technology (National Institute of Standards and Technology 2022; hereafter NIST).

Evolution of Communication Technology

The events of September 11 proved to be a catalyst in the evolution of technology-supporting communication systems critical for coordinated emergency response. The attacks revealed fundamental problems stemming from varied communication methods used by responders from the many agencies that rushed to the scenes (FirstNet Authority n.d.). The radio systems that law enforcement, fire services, emergency medical services (EMS), and emergency management relied on could not efficiently operate across agencies, and high call volumes overwhelmed land and mobile phone lines (FirstNet Authority n.d.). In years since the attacks, many agencies and organizations from the public and private sectors have worked to develop and implement technology solutions that provide reliable interoperability to support unified emergency response.

When evaluating the use of technology in interoperability communications in the homeland security space, the most prominent source is the study of major disaster responses. The need for communication between different agencies is most prevalent when an incident is too large or destructive for a single agency or discipline to handle the response independently. Large emergencies such as natural disasters, terrorist attacks, and mass shootings require representation from several agencies and disciplines to make an effective response to mitigate. By assessing the performance and outcomes of the response following a major emergency, agencies can gather lessons learned and use them to enhance future response capabilities. Major emergency response can show how different agencies can use technology to communicate in an efficient manner. This includes assurance that the right assets are dispatched to the right location and important information is passed along to the necessary stakeholders.

The following timeline illustrates some of the significant milestones to identify and overcome technology barriers to interagency interoperability.

2001-2012:

The 9/11 Commission Report documents the challenges first responders faced in responding to the disaster (National Commission on Terrorist Attacks Upon the United States 2004). The Report identifies gaps in emergency communications leading up to and throughout the response and outlines recommendations for a nationwide network for public safety communications

(FirstNet Authority n.d.). In response to this report, public safety organizations and associations united to encourage Congress to pass legislation establishing a reliable, dedicated, nationwide high-speed network for first responders (FirstNet Authority n.d.).

Eleven years after September 11, the First Responder Network Authority, or FirstNet Authority, was created as part of the *Middle Class Tax Relief and Job Creation Act of 2012* and signed into law on Feb. 22, 2012 (FirstNet Authority n.d.). The law allocated 20 megahertz of spectrum and 7 billion dollars to establish a broadband network dedicated to the nation's first responders. It also charged the FirstNet Authority with the mandate to ensure the building, deployment, and operation of the network (FirstNet Authority n.d.). Congress also required that the network extend coverage in rural areas through buildout milestones (FirstNet Authority n.d.).

2015: Next Generation First Responder Apex Program

The DHS Science and Technology Directorate (S&T) First Responder Capabilities Program pursues the fulfillment of priority needs using existing and emerging technologies, knowledge products, and standards across focus areas that include public safety communications solutions to achieve efficiencies, interoperability, and compatibility for critical communications and information sharing (DHS 2021). In 2015, the S&T initiated the Next Generation First Responder Apex program to “develop and integrate next-generation technologies

to expand first responder mission effectiveness and safety" (U.S. Department of Homeland Security Science and Technology Directorate 2018; hereafter DHS S&T). The program aimed to develop and integrate technologies that were modular and scalable with the goal of defining open-source standards that enable commercially developed technologies to integrate with existing first responder technologies (DHS S&T 2018).

2016-2017:

Through a public-private partnership, the FirstNet Authority awarded an innovative 25-year contract to AT&T in March 2017 to build, deploy, operate, and maintain a network to ensure robust public safety coverage (FirstNet Authority n.d.).

2018-2019:

In 2019, the Cybersecurity and Infrastructure Security Agency (CISA) developed the National Emergency Communications Plan. The plan's objective was to "ensure communications and information sharing systems meet public safety's mission-critical needs" (Cybersecurity and Infrastructure Security Agency 2019, 34; hereafter CISA). The plan identified six specific activities required to implement next-generation 911 technology and infrastructure; these activities are as follows:

1) convert all addressing to geographic information system;

2) establish dedicated emergency services internet and next generation 911 core services;

3) install next generation 911-capable and standard-compliant 911 customer premises equipment as well as computer-aided-dispatch;

4) create a robust mechanism for integration of devices and applications through a technical review and acceptance process supported by commercial and public safety standards;

5) develop and rapidly adopt standards facilitating the interface between 911, computer-aided-dispatch, and FirstNet; and

6) develop and rapidly adopt technical models to manage the receipt, processing, and sharing of multimedia." (CISA 2019, 34)

FirstNet provides its subscribing public safety agencies access to 72 dedicated deployable network assets stationed across the country. This access includes the option to utilize Satellite Cell on Light Trucks, a mobile cell site that links to FirstNet via satellite and does not rely on commercial power availability (FirstNet Authority n.d.). FirstNet's footprint has grown with the deployment of Band 14 spectrum to further increase the coverage and capacity for first responders in both urban and rural areas – on both indoor and outdoor sites (FirstNet Authority n.d.).

Present Day:

Technology advancements in emergency communication systems solutions is a continual process. In recent years, innovative technologies such as Unmanned Aerial Vehicles and IoT have been deployed during response efforts (Carreras-Coch et al. 2022, 2).

Cybersecurity Considerations in Emergency Communication Technology

Issues in communication equipment/services are a common occurrence. When challenges manifest during emergency events, they can compound the effects of the emergency, thereby hampering the response efforts. It is important for data to flow in both directions, and an interruption or degradation of this information could hinder operational control of the emergency incident.

The significant cybersecurity implications to emergency response communications are on par with the level of criticality for interoperability. A 2021 audit performed by the inspector general's office identified issues related to oversight of the National Public Safety Broadband Network (Johnson 2021). The network, which encompasses FirstNet, is frequently targeted by malicious hackers (Johnson 2021). There is a vast amount of published work on the subject and related potential scenarios, including cybercriminals exploiting communication systems during emergency response efforts. CISA, the National Telecommunications and Information Administration, public safety organizations and nonprofits, and contractors such as AT&T (who manages FirstNet) must all contend with these types of cybersecurity incidents (Johnson 2021).

Major Emergency Response

The Department of Homeland Security (DHS) has created the Office of Emergency Communications (OEC) to assist local, state, and tribal partners in emergency communication preparedness. "OEC has developed a framework with public safety personnel and government officials to implement solutions that address operability, interoperability, and continuity of communications" (DHS 2015). In this framework, the OEC mandates that each state has a Statewide Communication Interoperability Plan (SCIP) and designates a single point of contact for each state that administers the SCIP called the Statewide Interoperability Coordinator (SWIC). OEC also provides "the Government Emergency Telecommunications Service (GETS), Wireless Priority Service (WPS), and Telecommunications Service Priority programs to state and local officials. These programs enhance call completion for select landline and wireless users by providing priority during abnormal call volume on the public switched telephone network" (DHS 2015).

The plans and technology that have been developed by the OEC have spawned entirely new offices and committees inside many states' governments such as the Louisiana Statewide Interoperability Executive Subcommittee (SIEC). "Operationally, the subcommittee has full authority to design, construct, administer and maintain a statewide interoperable communications system with capacity to transport voice, data and imagery in support of full response to any

emergency event, as well as general day-to-day operations" (Louisiana Governor's Office of Homeland Security and Emergency Preparedness 2022). This subcommittee is also responsible for implementing the SCIP along with coordination with the OEC to develop the procedural and technical requirements necessary.

Findings

Among the barriers to interoperability in day-to-day incident response, technology-related issues pose a significant challenge. In research, to determine the role of technology in interagency interoperability, findings align with three key areas: 1) Communication Interoperability Challenges, 2) Evolution of Communication Technology, and 3) Cybersecurity Considerations in Emergency Communication Technology.

Communication barriers to interoperability between emergency response agencies are often due to technical issues. Recent guidance asserts, "public safety agencies cannot communicate seamlessly for three primary reasons: incompatible frequencies, incompatible equipment, and lack of common language" (Department of Justice 2022a, 1; hereafter DOJ). The evolution of technology to improve communications highlights both the advancements and challenges to addressing these issues. Coupled with technical issues, cybersecurity threats pose significant ongoing concerns.

Examining Communication Interoperability Challenges

Two specific challenges to achieving interoperability include the use of different frequency bands by different agencies and incompatible radio equipment (DOJ 2022a). The Federal Communications Commission (FCC) has authorized multiple bands of the radio spectrum for use by public safety agencies, including the following four primary public safety bands:

1. Very High Frequency (VHF) Low or Low Band (30–40 megahertz);
2. VHF High (152–162 megahertz);
3. UHF (406–512 megahertz); and
4. 700 or 800 megahertz.

Because agencies do not all operate on the same band, their communications devices are not interoperable. For example, "a radio operating on a VHF Low radio system can communicate only with other radios in the same range with pre-programmed common frequencies" (1). However, even when using radio systems in the same frequency range, issues such as differences in equipment can still prevent interoperability. Agencies that have different equipment can use a bridging device or gateway to connect the different systems or purchase a cache of radios to use in emergencies. Using alternative radios for emergencies, however, requires first responders to carry and operate a second radio and requires agencies not only to pay for the additional radios but also to monitor whether the batteries are charged.

Lessons Learned from Case Studies

Tennessee Storms

In March 2012, Tennessee was hit by a major storm system that spawned eight tornadoes and required ten counties to be declared disaster areas. “The unrelenting onslaught of severe weather overwhelmed the capabilities and resources of emergency response and communications throughout the region” (DHS 2012, 1).

In Tennessee, amateur radio operators, known as Auxiliary Communicators, belong to the Middle Tennessee Emergency Amateur Radio System, which is a statewide system where Auxiliary Communicators can report significant weather observations and damage reports. “The system is monitored by Tennessee’s National Weather Service and by many of the local emergency operations centers, including the State Emergency Operations Center (SEOC) in Nashville” (DHS 2012, 1). During the storms, an Auxiliary Communicator reported a tornado was approaching the SEOC, which gave the staff inside the building time to relocate to a safer area. “As the storm passed through, cell phones became overloaded and useless, but reports and information sharing continued uninterrupted via the Auxiliary Communications circuits” (DHS 2012, 2).

By utilizing circuits that are not normally used by the public or emergency communications, the Auxiliary Communicators continued reporting uninterrupted while cellular, landline, and radio operations were overloaded. The technology used by amateur radio operators is considered extremely out of date. However, the

system works efficiently and is not susceptible to interruption by more modern systems.

The Boston Marathon Bombing

There were many lessons learned following the bombing of the Boston Marathon, as well as triumphs in planning that allowed great interoperability during the response and the ensuing manhunt for the suspects. During the planning stages of the marathon, Steve Staffier was designated as the SWIC and "worked with the Boston Athletic Association, Federal authorities, and the eight communities affected by the race to plan and coordinate communications among the various agencies that support the marathon" (DHS 2013). The OEC also made recommendations to "further integrate communications into the event's overall command and control functions" (DHS 2013). Staffier accomplished this by adding a "medical command and control radio network, enabling public safety supervisors and commanders to better circulate and share medical information" (DHS 2013). This addition became a critical piece when the two bombs were detonated near the finish line of the marathon.

Following the detonations, land and cellular phone communications became saturated with users and became virtually unavailable for 90 minutes. During that period, first responders could communicate using the established radio networks, which could keep pace with the demand. Responders also turned to GETS and WPS "to enhance call completion and support communications

continuity" (DHS 2013, 2). These technologies allowed responders to communicate using dedicated broadband networks separate from commercial lines that continued to be saturated with calls.

The aftermath of the marathon also highlighted several flaws in technology that could occur in an incident management scenario. One such issue "was the battery life of the portable radios carried by law enforcement and public safety during the long shifts and deployments the situation required" (DHS 2013, 3). Long-shift deployments are a common occurrence amongst all disciplines and agencies, and the issue of battery life could play a role in incident response if communications are hampered. Another issue arose when some agencies that responded to the bombing did not follow the established SCIP. As a result, agencies following the plan could immediately plug into the channels, while "a small number of agencies that came to assist did not have the interoperability channels programmed in and needed to be given a pre-programmed radio to use" (3). This is a policy issue present in some agencies where leadership fails to follow best practices laid out by the SCIP and could result in communication failures.

Russia's Invasion of Ukraine

The Russian invasion of Ukraine in February 2022 further highlights the need for secure communications. At the onset of the initial invasion, Germany experienced a loss of 11 gigawatts of electricity from some of its wind-generated

energy fleet (Willuhn 2022). Most of the generation loss was due to precautionary shutdowns of wind turbines due to an incident forcing "responders to switch off the remote data monitoring connections to the wind turbines for security reasons" (Arghire 2022). Some early speculation on this incident supports the theory that the wind turbines were not the intended target but rather satellite communications.

Russia was believed to have actively targeted satellite communications by jamming their signals to prevent the Ukrainian army from using them. In this case, the wind turbines also operated via satellite communication and had to be shut down. An article by PV magazine Germany states that "it would appear unlikely, however, Russian hackers directly targeted German wind turbines. Commenting on the incident to the *Handelsblatt* business newspaper, a spokesperson for the German Wind Energy Association said the disruption was due to the failure of the KA-Sat communication satellite belonging to Viasat" (Willuhn 2022).

Authors Channa and Ahmed (2010) explore emergency response communications and provide alternative means to establish communications when primary communication channels of landlines and cell services are compromised. In addition to providing these network communication alternatives, the authors also discuss security considerations to protect communications and data. This is an important inclusion, as secure communications are not usually a primary consideration during emergencies. The results of using unsecured

communications can be seen in the recent conflict in Ukraine. Although war is an extreme example of emergency operations, lessons can still be learned about the dangers of using unsecured communications. Tim Stickings (2022) shares a story of Russian troops discussing operation plans via unsecured networks allowing the Ukrainian forces to obtain this information and use it for counter-attacks, resulting in "the death of at least one Russian general." Again, war is an extreme case but one that can never-the-less offer relevant lessons. Ensuring secure communications is imperative in mitigating nefarious actors from adding an additional layer of uncertainty in an already chaotic situation.

Superstorm Sandy

Another relevant historical case study is Superstorm Sandy, a tremendous hurricane that struck in 2012. Although this disaster is a "gray sky" event, a review of preparation and response still offers relevant insight into what communications should be practiced during "blue sky" events. One such lesson is the poor planning in developing communication procedures for poorer communities during and after the storm. Rejina Manandhar and Laura K. Siebeneck (2018) use socio-demographic characteristics to examine and analyze challenges to communication within "vulnerable populations and poor and ethnic minorities" and also "Spanish-speaking populations" (123). Focusing on these particular groups before emergencies can identify challenges for first responders to

respond to events in these communities effectively. Communicating with utility companies, particularly electric companies, was also identified as a shortcoming during Hurricane Sandy (128–9). Despite inquiries and attempts at communicating with these entities, first responders could not get timely and accurate information, especially as the public flooded the electric utility with inquiries simultaneously. These lessons emphasize the critical importance of developing a direct source or liaison when coordinating response and recovery efforts.

Hurricane Harvey

In 2017, Texas Governor Greg Abbott commissioned an After-Action Report to identify ways to improve emergency response after Hurricane Harvey. Although this storm was another "gray sky" event, it also offers valuable insight into the strengths and weaknesses of communication and interoperability within the state at the time. The resulting report focuses on restructuring and realignment of agencies, but it also addresses communication and data challenges. Of note are references to the "Emergency Radio Infrastructure Account" established by the Texas Legislature in 2011 to facilitate the interoperability of radio infrastructure throughout the state, ways to better utilize social media, improve "relationships with private technology providers," and utilize "data analytics to improve disaster management" (Sharp 2018, 150).

CULTURE

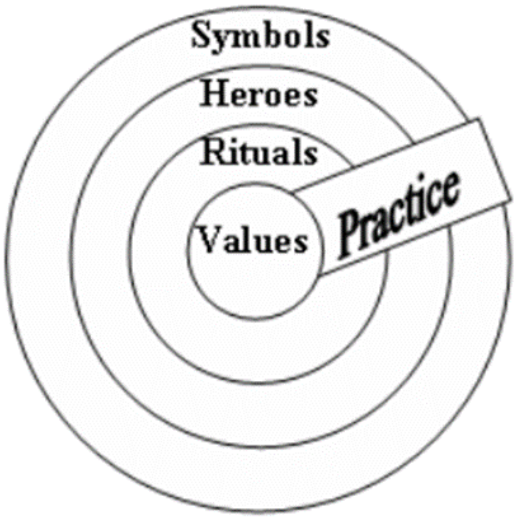
Culture is critical in an organization's ability and willingness to collaborate in day-to-day incident response. This section will explore the current understanding of the culture within and between organizations by reviewing the current body of literature. Next, this section will present the findings of the capstone team's research.

Defining Culture

The current body of research offers several definitions and models of culture. Schein and Schein (2017) define it as "learned patterns of beliefs, values, assumptions, and behavioral norms that manifest themselves at different levels of observability" (18). According to Schein (1984), "organizational culture is the pattern of basic assumptions that a given group has invented, discovered, or developed in learning to cope with its problems of external adaptation and internal integration, and that have worked well enough to be considered valid, and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems." Brough, Chataway, and Biggs (2016, 29) define organizational culture as "a set of basic taken-for-granted assumptions, shared perceptions of organizational work factors and a set of core values"

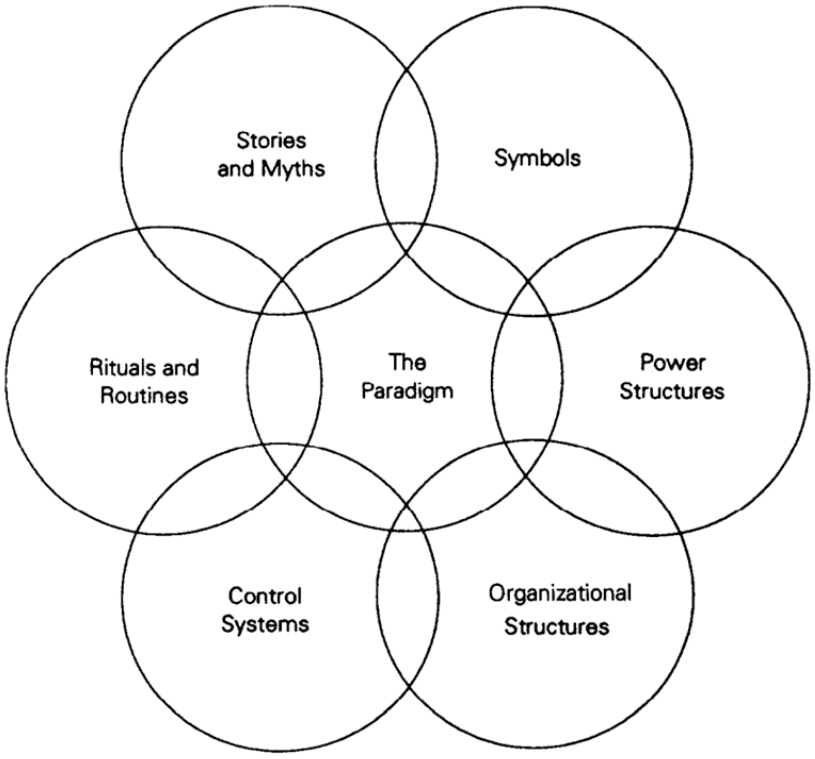
"The literature recognizes organizational culture as one of the primary factors influencing the extent of interagency collaboration, primarily because it shapes the organizational members' attitudes and actions toward that collaboration" (Cohen 2018). Culture is maintained at the group level, and through the practice and use of symbols, heroes, rituals, and values, culture acts to guide action at the individual level (Hofstede and Hofstede 2005, Bloor and Dawson 1994). The onion model of culture illustrated in figure 2 demonstrates this relationship. According to Hofstede and Hofstede (2005), through the practice of these elements, culture is learned and perpetuated. As elements of the model shift and are practiced within the organization, the culture of the organization may begin to shift dynamically.

Figure 2, The Onion Model of Culture (Hofstede and Hofstede 2005)



A related model is the cultural web developed by scholars Johnson and Scholes (1993). Below, figure 3 presents an early version of this model. Although there are some similarities between the cultural web model and the onion model of culture developed by Hofstede, the former incorporates the role of structure, control systems, and stories and myths in the development of culture (Johnson 1992, Johnson and Schole 1993). The overlapping areas that make up the paradigm "result in behaviors that serve as a guide to employees about what is considered appropriate or inappropriate behavior in an organization" (Sun 2008, 139).

Figure 3, The "Cultural Web" of an Organization (Johnson 1992)



These models illustrate the various elements that impact culture and, in turn, potential interagency collaboration. As Cohen (2018) points out, this is in part because organizational culture "shapes the organizational members' attitudes and actions toward that collaboration" (888). When members are part of a collaborative organization, they will be more prone to working with others; conversely, collaboration will suffer in organizations that focus on independence. It is also vital to understand that an organization's culture is defined over time and through practice (Schein and Schein 2017, Hofstede and Hofstede 2005).

When looking at collaboration amongst public safety agencies, it must be recognized that agencies are not homogenous. Different service providers must work together for the good of the public. These agencies include emergency services such as police, fire, and EMS. Each of the agencies or organizations that are attempting to work together are going to have their own culture, and that culture is going to define all aspects of how they interact internally and externally with other agencies and customers.

Findings

Now more than ever, collaboration amongst public safety agencies is critical, as "crime is rarely confined to defined jurisdictional boundaries" (Cohen 2018, 887). As one interviewer noted, neither fires nor criminals are not bound by the jurisdiction of one county or city and another; "the more [agencies] can work

collectively for the common good, the better it is for [all agencies]" (Appendix A, Respondent 5 2022). It is common for situations or circumstances affecting someone or something in one jurisdiction to cross jurisdictional boundaries. If agencies were willing to share information, then they may have a better chance of solving crimes or resolving situations. However, "there is often a hesitancy in agencies sharing law enforcement data. Reported reasons have to do with data owners wanting to retain strict control over 'their' data, as well as concerns about what might happen to the data and how they might be used if shared outside their own systems" (Hollywood and Winkelman 2015, 16). Additionally, public safety agencies "can experience legal conflict, confusion, and insecurity when addressing issues that cross state lines and implicate conflicting or inconsistent state laws" (Ladich 2018, 2).

A recent study of police officers and their use of body-worn cameras offers support for the idea that culture will make or break any strategy or implementation (Willis 2022). Through this research, Willis (2022) found that when the strategy "fit well with existing police values and beliefs, they were more likely to be accepted by line officers; when they were in tension or conflict, they were more likely to be modified or resisted" (726).

The Size and Complexity of the Homeland Security Enterprise

When looking at collaboration amongst public safety agencies, it must be recognized that agencies are not homogenous. According to the DOJ (2022b), as

of 2018, there were 17, 541 law enforcement agencies operated by state and local governments. This number includes 67% local police departments, 17% county sheriff's departments, and 15% other agencies, including state, tribal, and special jurisdictions such as constables and marshals. These agencies employed 1,214,000 full-time employees; of that figure, approximately 800,000 served as full-time sworn law enforcement officers (Gardner and Scott 2022). These officers are spread across all states and U.S. Territories. Table 1 below shows a breakdown of employees by law enforcement agency type.

Table 1, State and Local Law Enforcement Employees, by type of agency (DOJ 2022b)

State and local law enforcement employees, by type of agency, 2018

		Full-time employees			Part-time employees		
Type of agency	Agencies	Total	Sworn	Civilian*	Total	Sworn	Civilian*
All types	17,541	1,214,260	787,565	426,695	118,824	50,134	68,690
Local police	11,824	601,011	465,891	135,121	66,222	31,414	34,807
Sheriff's office	3,051	377,682	192,380	185,302	29,948	12,864	17,083
Primary state	49	92,756	60,451	32,305	690	139	551
Tribal police	217	5,652	3,789	1,863	174	107	67
Special jurisdiction	1,753	132,030	60,833	71,198	21,055	5,040	16,015
Constable/marshal	647	5,128	4,221	906	736	569	167

Note: Details may not sum to totals due to rounding. Excludes agencies that did not employ at least one full-time equivalent (FTE) sworn officer. FTE is the number of full-time sworn officers plus half the number of part-time sworn officers. See appendix table 2 for standard errors.

*Includes officers and deputies with limited or no arrest powers and nonsworn employees.

Source: Bureau of Justice Statistics, Census of State and Local Law Enforcement Agencies, 2018.

Another type of responder vital to public safety collaboration is EMS. The National Association of State EMS Officials 2020 National EMS Assessment reports that there are 1,052,842 licensed EMS providers within the 54 states that responded to their survey. In the State of Texas, the Texas Department of State Health Services (TXDSHS) has licensed 738 EMS Providers and 620 First

Responder Organizations with over 72,000 certifications (Texas Health and Human Services 2022).

The U.S. Fire Department Profile 2020, published by the National Fire Protection Association, shows approximately 1,041,200 firefighters in the United States in both paid and volunteer positions (Fahy, Evarts, and Stein 2022). According to this report, within Texas alone, there are approximately 800 fire department agencies with over 52,000 firefighters. Table 2 shows the number of career and volunteer fire departments across the nation and the percentage of the U.S. population they protect.

Table 2, Number of Departments and Percent of U.S. Population Protected by Type of Department (Fahy, Evarts, and Stein 2022)

Type of Department	Number	Percent	Percent of US Population Protected
All-career	2,785	9%	49%
Mostly-career	2,459	8%	21%
Mostly-volunteer	5,335	18%	14%
All-volunteer	18,873	64%	16%
Total	29,452	100%	100%

Each of these agencies has its own unique culture, which impacts how they interact with other agencies. The more than 70,000 agencies referenced above only include police, fire, and EMS. They do not include other agencies such as Federal agencies, private agencies, utilities, and other service providers that play a role in public safety.

Law enforcement agencies have a common goal of promoting public safety. Shared purpose is a driving force for collaboration, and this common goal should be conducive to working together (Nayar 2014). However, "one significant barrier to law enforcement collaboration is the fragmentation within the American law enforcement organizational culture" (Schnobrich-Davis and Terrill 2010). Agencies differ in size, location, type of service, structure, and leadership and rank structure, among other factors.

One factor that affects agencies' willingness to cooperate with each other is agency type. Agencies of the same type or in the same region showed more willingness to collaborate than with agencies of a different type. This finding is reflected in Cohen's (2018) research; study participants indicate that collaborations go more smoothly with neighboring agencies because "With [a neighboring agency] it is easier to collaborate. I understand their job and they understand mine…there is a bond because they know what we are doing" (Cohen 2018). This sentiment is not extended to other agencies whose jobs are viewed as different, and there is a lack of understanding between different levels about their jobs (Cohen 2018).

Additionally, agency size can pose a barrier to collaboration, mainly because agency size often determines capacity, resources, and capabilities. For example, when large agencies collaborate with smaller surrounding agencies, the smaller ones rely heavily on the largest agency for support and capacity, not the

other way around. Therefore, “when [large agency’s] facilities go down, they cannot ask their neighboring counties to take 1,000 calls per hour while [they] figure out what [they’re] doing” (Appendix A, Respondent 4 2022) The level of support is uneven and not always mutually beneficial. Additionally, coordination and collaboration can be burdensome for smaller agencies. Respondent 5 shared how “even though [they] are [in a leadership role], [they] are just part-time and work 20 hours a week. Just keeping the lights on - putting together board packets, answering trouble tickets, managing the vendors, etc. - takes up all [their] time… So [they] haven’t been able to invest in it” (Appendix A, Respondent 5 2022).

Rank Within Agencies

Cohen further proposes that collaboration differs by rank, with officers of similar rank more likely to collaborate, and officers of lower rank more often participating in informal collaboration. “This condition creates a barrier for meaningful collaboration as officers at the lower level do not have the authority and resources needed to manage effective, long-term collaborative relationships (Cohen 2018).” Formal collaboration is often established at higher levels; however, there are more political barriers to this type of collaboration because the relationship is formalized in agreements (Cohen 2018). “The public management literature agrees that collaborative leadership plays a prominent role in the development of collaboration culture in organizations (Cohen 2018, 890).” If leadership engages in collaboration, then lower levels are more likely to.

However, if chiefs and agency administrators are secretive or resistant to collaboration, then other members of their agencies have the same tendency (Cohen 2018). Yet, Respondent 3 noted a cultural shift occurring within their agency due to more private sector employees transitioning into the public sector, pushing for more collaboration and offering new ways to address concerns about security in sharing information. However, they often get shut down by upper management" (Appendix A, Respondent 3 2022)

Respondent 3 also noted the impediments to collaboration are caused by "a lack of memorandum of understanding (MOUs) between agencies… while the [agencies] talk about it and have meetings, it just dies because there's no follow-up" (Repondent 3, 2022). This is primarily attributed to an "old school mindset and culture of "this is the way we've always done it" instead of moving forward and looking into a broader vision and data sharing" (Appendix A, Respondent 3 2022).

Although culture can be a barrier to collaboration in law enforcement, it can also promote collaboration. If the agency leaders are collaborative in nature, then they can breed a collaborative culture that promotes coordination with other agencies rather than impeding it.

Case Study: Uvalde

We offer a recent example of when established policies and procedures were not practiced or followed to make conclusions on interoperability policy failures. For example, we reference the *Texas House Investigative Committee on the Robb Elementary Shooting, Texas House of Representatives Interim Report 2022*. These factual conclusions are based on the information developed through its investigation; the House Committee has drawn the following preliminary conclusions (Burrows 2022).

Pre-attack reports suggest that social-media users may have reported the attacker's threatening behavior to the relevant social media platforms. However, social media platforms seem to have not responded by restricting the attacker's access or reporting his conduct to law enforcement authorities (Burrows 2022). In addition, the services that the Uvalde Consolidated Independent School District used to check social media for threats did not deliver any alert of threatening behavior by the attacker (Burrows 2022).

No law enforcement officers were on the Robb Elementary property when the attacker scaled the fence and moved to the school. Citizens at the scene immediately alerted local law enforcement about a motor vehicle accident, a male with a gun, and multiple shots fired near the Robb Elementary campus. As initially recounted by Uvalde Police dispatch and as understood by most initial responders, the scene began off-campus as an incident that falls under the

jurisdiction of the Uvalde Police Department. As a result, Uvalde Police officers were among the first, if not the first, law enforcement officers on the scene as a man firing a gun went toward Robb Elementary School. As the situation progressed and responders received additional information, it became evident that the suspect went on to the school campus and within the authority of the Uvalde school district Police Department. Several law enforcement officers arrived at Robb Elementary within a few minutes of the attacker breaching the fence. Although an Uvalde Police Department officer noticed a person dressed in black and thought it might have been the attacker. That officer requested permission to shoot from over 100 yards. The subsequent evaluation suggested that the person in black was a school coach, and the officer did not have an opportunity to stop the actual attacker by shooting him before entering the west building. In a standout move, Robb Elementary School Coach Yvette Silva acted heroically and almost certainly saved lives by alerting the school to the attacker's advance. Most fourth-grade classes were successfully locked down because of her quick response. After entering through the opened west door, the attacker had about three minutes in the west building before first responders arrived, including nearly two and a half minutes. The attacker is assessed to have fired over 100 rounds. The initial officers to the west building heard gunfire and witnessed a hallway with a fog of drywall debris, empty rifle casings, and bullet holes. Officers converged on rooms 111 and 112, which they discovered as the attacker's

location. Officers acted appropriately by attempting to breach the classrooms and stop the attacker. However, the attacker instantly repelled them with a burst of rifle fire from inside the classrooms. The responders instantly began to assess options to breach the classroom. However, they lost crucial momentum by handling the scenario as a "barricaded subject" instead of with the greater urgency attached to an "active shooter" scenario (Burrows 2022).

It was an *active shooter* scenario because the attacker prevented critically injured victims from getting medical attention. An active shooter scenario varies from a barricaded-subject situation in that officers responding to an active shooter are trained to prioritize the protection of innocent victims over the safety of law enforcement officers. Initially, the first responders did not have *reliable evidence* about whether there were injured victims inside Rooms 111 and 112. However, circumstantial evidence strongly suggested that possibility, including the fact that the attacker had fired many rounds inside classrooms with students in attendance. The Advanced Law Enforcement Rapid Response Training standard of *reliable evidence* did not support the *reasonable officer* standard employed by Advanced Law Enforcement Rapid Response Training in its preliminary report (Blair 2022). The Uvalde school district's active shooter policy called for Uvalde district Police Chief Arredondo to be the incident commander in any active shooter response. Chief Arredondo was among the first responders to arrive at the west building. In

the initial reaction to the incident, Chief Arredondo was actively involved in the attempt to "stop the killing" up to the time the attacker was in Rooms 111 and 112, and the attacker fired on responding officers. By this time, dozens of officers were on the scene. However, a critical failure of Chief Arredondo in that he did not assume his preassigned responsibility of incident command, which would have required notifying other officers that he was in command and leaving the building to exercise command, beginning with launching an incident command post. Instead, the Chief remained in the hallway, where he lacked reliable communication with other law enforcement elements and could not effectively implement staging or command and control of the situation (Burrows 2022).

Over the next hour, hundreds of law enforcement officers arrived at the scene. The scene was chaotic, with no leadership directing the law enforcement response or anyone obviously in charge. To the extent any officers considered Chief Arredondo the overall incident commander, they also should have recognized that was inconsistent with his position inside the building. There was an overall apathetic approach by law enforcement at the scene. For many, they were provided and relied upon incorrect information. Others had enough information and knew better. Despite apparent deficiencies in command and control at the scene, which other law enforcement responders should have recognized, no one approached Chief Arredondo or any of the officers around him

or assistant to him to offer support with incident command. Instead, chief Arredondo and the officers at the south end of the building were focused on gaining access to the classrooms (through a key, breaching tool, or other means) along with officer protective equipment (rifle-rated ballistic shields, flashbangs, etc.).

Meanwhile, dozens of officers were assembling in the hallway on the north side of the building, stacking up for the assault on the classrooms and primarily awaiting further instructions pending the arrival of protective gear and breaching equipment. Although meanwhile, 911 received communications from victims inside Rooms 111 and 112, Chief Arredondo did not learn about it because he failed to establish a reliable method of receiving critical information from outside the building. Ultimately, Chief Arredondo understood there probably were casualties inside Rooms 111 and 112. However, even if he had received information about living injured victims in the classrooms, it is unclear whether he would have done anything differently to act "more urgently" (Burrows 2022).

U.S. Marshals provided a rifle-rated shield, which arrived at about 12:20 p.m., nearly 30 minutes before the classroom was finally breached. While officers acted on the belief that the doors to Rooms 111 and 112 were locked, as they were designed to be, not a single person tested that assumption. Evidence later revealed that Room 111's door probably was not effectively locked shut. Chief Arredondo

did not exercise tactical incident command over the Border Patrol Tactical (BORTAC) team, nor did the team seek instruction from Chief Arredondo. By the time the BORTAC team breached the classroom door, the tactical command inside the building had been de facto assumed by Border Patrol Tactical. Acting on the data available to Chief Arredondo, including an assumption of injured victims in the room, the Border Patrol Tactical commander on scene waited to arrange a rifle-rated shield and obtain the working master key before breaching the classrooms (Burrows 2022).

Failure to anticipate probable outcomes can be mitigated by training and policy. This is why communication is so vital. It is critical that organizations communicate before significant events to prepare for them and to address known problems, and develop a plan for previously unknown problems. Ensuring that everyone has the tools, training, and resources to do that is paramount in the business of saving lives.

POLICY BARRIERS

Political and institutional barriers within the homeland security enterprise can impede interoperability. This section provides an overview of the literature related to inconsistent standards for technology and equipment, how differing funding priorities and budget cycles contribute to limited funding for training, equipment, adequate staffing, and training, as well as the conflicting management, policies, and procedures that exist among jurisdictions.

Conflicting Policies, Laws and Regulations

Public Records and Information Classification

State and inhabited territory laws on public records ensure that governments are open and transparent. However, each state and inhabited territory establishes its own statutes, exemptions, and limitations regarding public records, which means "any form of shared information across boundary lines will be treated differently" (Ladich 2018). This affects interoperable communication because the public safety agency sending information does not know how the receiving organization will handle or use the information despite how it could apply to a day-to-day activity or a potential emergency incident.

Additionally, each state classifies information differently, which can also hamper interoperable communication among public safety agencies. Information is classified by a specific designation -"Law Enforcement Sensitive (LES), For

Official Use Only (FOUO), and Classified. These designations are utilized at the federal government level and serve as internal controls to easily identify sensitive information and quickly determine the permissible recipients" (Ladich 2018, 21). However, every state has a different set of laws and definitions, meaning a public safety agency cannot share information without violating the laws in their respective areas.

As a result, public safety agencies "can experience legal conflict, confusion, and insecurity when addressing issues that cross state lines and implicate conflicting or inconsistent state laws" (Ladich 2018, 2). Each state and territory "has the authority to create and enforce criminal and civil laws, determine its public policies, and manage its own affairs" (Ladich 2018, 2). Consequently, there are more than 50 different forms of state and territory laws that need to be navigated when there is any form of interoperable communication sharing as it applies to public law or an individual's personal information.

Financial Barriers

Limited funding as well as differing budget cycles, processes, and priorities are all barriers to interoperability. Local, county, state, and federal agencies are constrained by a budget that has to be justified and approved by representatives of that government, and oftentimes the allocation of funds is political in nature.

The Information Sharing Environment (ISE), which was established by Congress as part of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) focuses on intelligence reform and establishes a national-level information-sharing strategy. (Offices of Inspector General, 2017) However, in 2017, the Project Manager of the ISE "determined that its implementation across the information sharing environment has been uneven" and that at the local and state levels, public safety agencies seemed to be more "focused on sustaining operations rather than enhancing capabilities due to unpredictable federal support, including potential reductions in grant funding" (Offices of Inspector General 2017, 9).

Updating and Replacing Equipment

When a jurisdiction adopts its budget, it prioritizes and strategically invests in its immediate needs. Communication with other agencies is an afterthought. As a result, organizations with systems that currently function well would be hesitant to spend money on updating or replacing expensive radio communications equipment. Furthermore, "interfacing and connecting systems isn't a one-and-done job; when you make upgrades or changes, you must re-do the interfaces, which gets complicated and time/energy consuming" (Appendix A, Respondent 4, 2022) Therefore, it is often not cost-effective to join a consortium or collaborate what other agencies. "Particularly for smaller departments, the cost

of joining a consortium can be hard to swallow. Rather than incurring the cost, these small departments have chosen to take their chances on their own and continue with the status quo in their units" (Appendix A, Respondent 5 2022). Unfortunately, "smaller agencies don't always have the budget or the staff for redundancy" (Appendix A, Respondent 2 2022)

Staffing Shortages

Respondent 1 (2022) reported staffing shortages as one of the primary barriers to collaboration. "Many units are short-staffed, and as a result, many employees are overworked." Respondent 5 (2022) noted that "when attending regional and national meetings, they often hear that every agency has a dispatch center, has multiple consoles, multiple licensing, multiple infrastructure… and half of them are understaffed by 50%." Respondent 2 (2022) noted that "their help desk is understaffed and it is hard to find people, especially because it's competitive. They have roughly 350 mobile computers and about three help desk staff." Respondent 5 (2022) attributes the shortage in dispatchers to "some cities pay[ing] their dispatchers more than others."

According to Dalton et al. (2010), attrition can result from several sources: a budget crises might cause jurisdictions to reduce their number of officers; some characteristics of the local police organization might become unappealing to officers and they decide to pursue work elsewhere; a pending wave of baby-boom

generation retirements threatens to reduce experience levels of police departments; increasing numbers of call-ups are requiring more officers who are also reservists to spend longer periods on nation-building and other military duties; and younger generations of workers might be more likely to change careers to find the work they like best. “Talented and driven people are migrating to specific areas with a better working environment, and remote work is also driving some of this workforce shift” (Appendix A, Respondent 2 2022)

Inadequate Training

Training and knowledge are critical in improving interoperability. “A lot of times, planning and training don’t happen, and as a result, people do not use all of the tools in their tool chests” (Appendix A, Respondent 4 2022). Respondent 5 (2022) noted that “a lot of the people now in information technology (IT) specialist roles do not have formal training. According to Respondent 2 (2022), “the lead time for training an IT person is about a year.”

Even when there is political will to allocate funding to technology, equipment, staff, training, etc., bureaucracy often impedes approval and acquisition. Respondent 3 (2022) noted “when looking at a new system, by the time [they] get it, it is somewhat updated.” This is more problematic in larger agencies.

CONCLUSION AND RECOMMENDATIONS

Reduce Financial Barriers to Interoperability

Overwhelmingly, responses continue to reflect the importance of the guideline to lower product/service costs, which reflects the theme that technology costs are a major barrier to their use. Over and over again, first responders reiterate that technology must be developed at price points that they can afford. "They also note that cost does not only refer to the initial cost of purchasing the technology, but must also factor in costs such as maintenance, upgrades, IT support, training, and data plans" (Buchanan et al. 2021).

If the cost of technology is a barrier to information sharing between organizations, federal and state funding mechanisms should be more heavily pursued and leveraged. As Sharp (2018) identifies in the *Eye of the Storm* report, funding options are earmarked by the Texas Legislature. However, the investigation has revealed that appropriations from accounts designated for communication have not been appropriated for radio infrastructure (Sharp 2018). Although this finding is specific to Texas, other agencies and organizations seeking to address issues in information sharing and interoperability may find benefit in exploring similar appropriations at the state or region level. The *Funding Mechanisms Guide for Public Safety Communications* produced by

SAFECOM and the National Council of Statewide Interoperability Coordinators details funding sources for emergency communications projects.

Front Line User Recommendations

The overarching themes that are discussed in the conclusions section of this report map closely to six user-centered design guidelines that have emerged in the research of technology. These six guidelines are as follows:

- Improve current technology
- Reduce unintended consequences
- Recognize "one size does not fit all
- Minimize "technology for technology's sake"
- Lower product/service costs
- Require usable technology. (Buchanan et al. 2021)

Focus on Improving Current Technological Capabilities

The theme "technology of the future = current technology improved" maps closely to two of the guidelines discussed, "improve current technology" and "minimize technology for technology's sake." First responders have stated that it is not necessarily new technology that they want but it is more important to improve on the existing technology (Buchanan et al. 2021). The rates at which first responders experience problems with their current technology increases the likelihood of losing trust and lacking confidence in it. It is clear that "first responders need to trust that the technology they use for day-to-day incident

response will work well, work consistently, and be affordable" (Buchanan et al. 2021). First responders also do not necessarily believe that new technology is always better technology and more technology is not needed. New technology has shown to be fragile in its initial stages with a high learning curve for implementation. These characteristics make for simply improving current technology to be the better course of action.

The theme "technology can be both a benefit and a burden" follows closely with "reducing unintended consequences." Futuristic technology can come with many unintended consequences. Many personnel that work in dispatch or 911 call center positions worry that receiving pictures and/or video from accidents and crime scenes could create physical, cognitive, and emotional burdens that may put an undue strain on resources (Buchanan et al. 2021).

The guideline "require usable technology" shows the importance of many issues that first responders experience with a wide variety of technologies supporting the need for usable technology. "Technology, in general, should make it easy for the user to do the right thing, hard to do the wrong thing, and easy to recover when the wrong thing happens. First responders were not opposed to technology, but they want technology that makes sense to them and makes their work easier to accomplish" (Buchanan et al. 2021). Technology should be developed with and for first responders, driven by their user characteristics, needs, requirements, and contexts of use.

Despite the many similarities found across the four first responder disciplines, there is also evidence of important differences between public safety disciplines. “Survey data suggests that there are some disciplinary differences in the technology used for day-to-day incident response” (Buchanan et al. 2021). This highlights that the “recognize one size does not fit all” guideline permeates the data as well. “While technology standardization across disciplines is important for consistency, compatibility and quality, technology must be easily adaptable to a wide variety of public safety needs” (Buchanan et al. 2021).

Lastly, technology and infrastructure to effectively support interagency communication and coordination must be an ongoing effort. As CISA notes, “if regions expect emergency responders to use interoperable equipment daily, supporting documentation and the installed technology must be well-maintained with a long-term commitment to upgrades and the eventual replacement of equipment” (CISA 2021). Channa and Ahmed (2010) provide potential alternative means to establish communications when primary communication channels of landlines and cell service are compromised.

In addition to providing network communication alternatives, the authors also provide security considerations to protect communications and data, which will be discussed later in the recommendations section (Channa and Ahmed 2010).

Utilize Training and Simulation Exercises

Communication issues are an unfortunate reality in incident response for much of our nation. Challenges with communication equipment and services often manifest during emergencies, which is undoubtedly the worst time to discover these challenges. Training exercises during "blue sky days" are the opportune time to identify deficiencies in emergency operations plans or to find the limitations of current equipment.

Simulation exercises provide emergency responders and other relevant organizations with an opportunity to prepare resources, discover what works and what does not work well, develop plans to improve methods and equipment to eliminate mistakes, and observe where capabilities and limitations lie. Although these efforts can be time- and resource-consuming, the outcome of well-executed exercises is incredibly valuable; exercises can reveal limitations and potential areas for improvement while simultaneously providing a platform for relationship building and collaborative problem-solving. Respondent 2 (2022) described how [the] director is involved in many conferences, networks, and associations… never afraid to leverage [the] network to assist people in finding the answers that they need. This is also something that the respondent attributes to successful collaborations in their own

organization. “They make connections with others and lean on their network. Relationships matter” (Appendix A, Respondent 2 2022).

Models also suggest that these types of activities can spur changes in behavior, not only amongst individuals but also within organizations, as well (Van Haperen 2001). Training exercises during blue-sky days are the opportune time to identify deficiencies in emergency operations plans or to find the limitations of current equipment. It is also crucial to incorporate poorer communities into these training exercises.

Some of these exercise programs already exist. Through its National Exercise Program, FEMA operates a two-year cycle of exercises across the nation to examine and validate capabilities. This effort assists state, local, and tribal governments, as well as Non-Government Organizations and Non-Profit Organizations, in planning, developing, conducting, and evaluating aspects of exercises for their specific needs. Additionally, as directed by the Robert *T. Stafford Disaster Relief and Emergency Assistance Act*, the Homeland Security Exercise and Evaluation Program “provides a set of guidance that any organization can use to structure an effective exercise and evaluation program with a common approach to program management, design and development, conduct, evaluation, and improvement planning.”

Although technology solutions have improved communications between agencies during incidents and lessened the severity caused by barriers, challenges still remain. Continual interagency work must be done to ensure systems are reliable, implemented technology is maintained, and ongoing planning is performed to anticipate future needs to mitigate issues. This involves a number of factors for emergency response agencies, including ongoing planning, budgeting, acquisition, testing, and deployment. Collaboration can significantly deliver immediate services, emergency services, guiding search-and-rescue operations, and activities during a disaster in real-time (Alsamhi et al. 2021, 1).

Further Research

As additional research related to communications, technology, interoperability, and incident management is completed, outcomes and recommendations will reveal themselves to this study. A picture of the landscape of technology has been established, and the future of how it will evolve. This study forms a framework of existing problems, what works effectively, and how we can combine these into suitable responses to questions that plague the people and agencies that are affected daily.

However, short-term strategies to incrementally improve existing radio communication systems with limited resources need to be explored and

developed. Additionally, the current body of research indicates that information exchange is often inhibited by various reasons related to "data owners wanting to retain strict control over 'their' data, as well as concerns about what might happen to the data and how they might be used if shared outside their own systems" (Hollywood and Winkelman 2015, 16). Safeguards to address such restrictions also need to be further explored.

While several respondents acknowledged concerns over broadcasting the private medical information of patients or sharing location-sensitive information broadly, none of the project team's interview respondents indicated a reluctance to share information in their current organizations (Appendix A). In fact, several of the interview respondents described efforts to promote information sharing, including an initiative to develop a home-grown database that leverages information from various organizations and then disseminates it (Appendix A, Respondent 4 2022). Therefore, the dynamics of information sharing behavior among agencies must be further explored.

Additional research may also be beneficial if focused on specific regions. As discussed, states and local agencies may have agreements already in place. They may be experiencing similar challenges or shared progress. Broadening research and evaluation toward geographical regions may lend more specific

trends to be analyzed and compared with others. Existing federal and state guidance is well known but implementation and outcomes will vary greatly.

Lastly, most available research and case studies pertain to major events. Questions remain regarding overall, day-to-day information sharing, implementation, and outcomes. Targeted research and analysis on single entities or collaborative networks during routine operations could provide valuable insight into issues highlighted by our interview respondents.

Appendix A

TRANSCRIPTS AND NOTES FROM INTERVIEWS

TABLE OF CONTENTS

Prior to commencing these interviews, respondents were provided the full list of interview questions, included below, and the problem statement developed for the project. Interviews were conducted virtually using the Zoom meeting platform and recorded with the consent of the respondent for note-taking purposes. Respondents also consented to the group's use of anonymized quotes and transcripts. The average duration of the interviews was approximately 45 minutes. The sections included below are divided by respondent. In order to protect the identity of these individuals, a combination of quotes and notes are included. Notes are indicated by italic text.

Interview Questions

Collaboration & Information Sharing

1. As you probably guessed, a major focus of our project is interagency collaboration and information sharing. When a disaster overwhelms the Authority Having Jurisdiction, and they call for assistance, collaboration is of the utmost importance. How does an organization maintain control of an incident and utilize assisting agencies?
2. What impediments to collaboration and information sharing with other agencies in your same discipline do you experience?
    a. What about in other disciplines?
3. Switching gears, what makes collaboration and information sharing easier with other agencies?

Technology

4. Technology has advanced a lot over the last decade, particularly in the area of communications. There is a growing push towards shared networks and other

technological solutions that allow multiple agencies to interact. Does your agency currently employ a solution like this?

   a. If yes, could you tell me about your experience with this solution?
   b. If not, do you think your agency would be supportive of such a solution?

5. What current technology does your agency utilize in day-to-day operations?
   a. If they mention Hexagon, ask them to describe what services and equipment they use.
6. What concerns do you have with your current technology as far as interoperability, functionality, length of use and cost?
7. What future requirements would you need for your technology needs going forward?

Organizational Barriers

8. Are there budget issues that limit your agency's work and interoperability?

Political / Cultural Barriers

9. How operational are your agency's communication policies? Are there deficiencies?
   a. Do you feel there are limitations in communication policies that simply cannot be planned for?
10. Do agency leaders encourage their subordinates to withhold certain information from collaborating agencies during emergency incidents? If so, why?
11. Have decision-makers and stakeholders supported policies that enhance your operations?
   a. Do you believe these decision-makers and policymakers understand the scope of the issues your agency faces? Overall, do they support the work?
12. Given your experiences, what are the primary concerns and/or challenges facing your agency regarding interagency interoperability in a day-to-day setting?
13. What can be done to ensure that these problems do not add to the vulnerability of the public during emergencies?

Transcripts and Notes from Interview with Respondent 1

Interviewed Virtually by Authors in September 2 022

Respondent 1's organization is uniquely positioned as emergency management is in the dispatch center. This physical proximity is reflected in a close relationship between the two units, which allows for great collaboration, mainly because the employees know each other.

Respondent 1 reports staffing shortages as one of the primary barriers to collaboration. Many units are short-staffed, and as a result, many employees are overworked.

Respondent 1's organization primarily relies on radio systems, although they also have a community notification system, as well. These radios are "very bad" and are pretty old. Respondent 1 reported that they had been approved for a raise in sales tax to fund a whole new radio system for all of their agencies. Through this initiative,

Interviewer: What are the challenges with this technology?

Respondent 1: Our radios are very bad. They are very old. We have a radio RFP and a microwave RFP. We also got a sales tax approved to be able to get a whole new radio system.

They will get all new radios for all of their agencies. They have all kinds of radios currently, but they will all have the same moving forward. They are eliminating the variety. They will also potentially get two new radio towers.

Interviewer: Was there any resistance to your sales tax plan?

They did have some. They did video vignettes trying to get everyone to understand the need. It's about the safety of the systems. There is no sunset clause on it, which also created some pushback. But there is no sunset clause because it has an ongoing cost. There is no other funding outside of the sale tax.

Interviewer: Is there any technology that you think will be beneficial (smart city)?

Real-time information sharing would be beneficial. In the Level 1 snowstorm, they made phone calls. If there were a map, it would be helpful. They have their own GIS analyst. They do have all of their hydrants in their map in CAD. They can toggle them on and off in the system, which is nice because it gets cluttered.

Interviewer: Do you see any inconsistencies or challenges with policy and interoperability/collaboration?

There are always different opinions, but the respondent doesn't see any of this. They can work out their differences. An example, just this morning, they discussed an agreement signed in 2002 for waterborne incidents, but they said they don't need the agreement anymore… if there's a need, they will go. They work through the issues and work well together.

Interviewer: Is there anything that would enhance operations?

The respondent indicated that radios and connectivity would enhance operations. They have to daisy-chain currently. They do quarterly tests that are voluntary. But it would be nice to have something where they can get on the same radio if phone lines are down. If an event caused the phone lines to go down, this would be a need they cannot fulfill.

Interviewer: [Can you discuss how security impacts this work?]

There are concerns about the radio system getting taken over. Their technology department hired an additional position for a network system admin to help address security concerns.

Criminal Justice Information Services training – the vendors have questions about why. They are an accredited agency, so they have to do this. They don't want to fail any reviews or audits, and it's important to them to keep their accreditation.

Transcripts and Notes from Interview with Respondent 2

Interviewed Virtually by Authors in September 2022

This respondent works closely with the technical side of things and has experience as a CAD administrator and technician.

Interviewer: Has [your county] brought in a universal system for their public safety enterprise?

The respondent's county pretty much owns, manages, and maintains its radio systems. They are currently rebuilding it. They will own/lease their own system entirely – a total system ownership model. This allows them to get rid of impediments. They've seen it work well with mobile computers, so they are transitioning the radios to this model as well. Some agencies don't have their own, but for those, they go to their IT folks who work with their office. This has proven helpful because then the technical people are speaking to other agencies. From the respondent's perspective, agencies WANT to be connected. The pushback often comes from guidelines and best practices. Additionally, the county owns the network and has to maintain it – this creates a bit of a pushback.

They have 16 agencies using these systems. With the improved systems, the agencies will be able to communicate seamlessly. There are some concerns with the connectedness, particularly regarding viruses. A firefighter in one agency could get a virus and then send it to the others inadvertently if there aren't fences.

A flat network is not the best for the users. They are working on redesigning to put each agency in its own lane but still allow information sharing. This will help with information/cyber security.

Interviewer: Do you have sufficient resources (people)?

Their staffing approach is to create the need and then get the people. They are trying to reverse that with the radio system. They want the people first. Their helpdesk is understaffed. It is hard to find people, especially because it's competitive. The lead time for training an IT person is about a year. They have roughly 350 mobile computers and about three helpdesk staff, so the ratio is high. The helpdesk is staffed for about ten hours daily, but they have on-call available. They are trying to develop tools for dispatch staff to help troubleshoot/triage, too.

Interviewer: [Can you talk a bit about mobile technology?] Is it moving to the ability to see everything everyone is doing?

Respondent: All of them are set up to see any and all agencies that are hosted, but most don't use it. They can toggle them on and off. Some agencies want to see others, though. This is a feature that is used – a filter – that is often used for bigger events. Individuals can't choose whether to share their own location; they can just decide whether they want to see others or not.

There is a drug enforcement task force that doesn't share their location at all, but that's not really an issue. There has been some concern over their location sharing at the end of their shift, so they are allowed to turn it off for the last 5 minutes of their shift to avoid sharing the location of their homes. They have a lot of take-home cars. CPR in progress is also shielded. PulsePoint (for CPR) has been pretty seamless once the growing pains were managed. They only mess with it when they are doing upgrades or changing out servers.

Interviewer: What are the concerns with current technology?

Interoperability is something that they are constantly working on. They are developing a CAD-to-CAD interface with [a vendor] currently with another neighboring county. This county is a [uses the same vendor], which makes this easier. They haven't tried to mesh with [agencies or counties using other vendors' products]. The complication factor depends on how much you want to share and what functionality you want. The current meshing project is helpful because sometimes the closest station is in another county. It's a lot like a game of go-fish currently, with them trying to sort things out for dispatching. They are more open to border dropping once the technology can support it.

They are trying to meet standards, but they can also utilize grant funding by meeting standards. Their director has done an excellent job of working with the fire agencies to ensure that their wants and need align with the strategic plan.

This allows them to dedicate resources to the effort. Putting the planning stages in line has been very helpful. As far as the respondent knows, they are the only group in their area that has linked two separate CAD systems.

Interviewer: Did your county grow with COVID?

Respondent 2: Yes, we did. We saw people leaving [large metropolitan areas].

Interviewer: [As the population density shifts to these more rural areas,] a**re they built to grow and to expand? If you do keep having a continual kind of population growth, is it relatively set up?**

Respondent 2: We've been doing a good job on the new systems we bought in the last few years to really add in that growth. We bought a virtual server infrastructure three or four years ago now and have almost grown beyond it. But the new one we bought just last year is scalable. [This product] makes it so our virtual infrastructure is only limited by need and finance.

Interviewer: Do you do much with your area hospitals or other agencies? Could it spur up any kind of communication between them? Do you have any working relationship with them, or is it pretty guarded?

Respondent 2: We don't have a lot with those. There are some in fire rigs. [Some] have a device that transmits patient data as they drive down the road…We

don't have direct connectivity from our CAD system or other technology [that goes] to a hospital or anything like that.

Interviewer: Has that been discussed?

Respondent 2: Not that part of it. No.

Interviewer: Do you think there would be any benefit in sharing that information?

Respondent 2: We try not to put too much medical [information] in the calls other than what is needed. I think they are more interested [in information like the location of] the units, route, or how far [out] they are. [This information will allow the hospital to] have that crash cart ready for them as they come in the door.

Interviewer: What does [your county] have in place for mass casualty incidents? Are there large enough hospitals to handle a lot of that? Or are they going to be sent to other counties?

Respondent 2: We have a couple of very large medical complexes…If it's over a certain threshold, they just airlift right over. We have multiple airlift providers that we use for that. I know all the agencies have mass casualty CAD run cards. Operations chiefs frequently to get them, and drills to get them all playing on the same page.

Interviewer: How is the tech side with those air providers?

Respondent 2: I think they have a couple of web apps that they can see where the airlifted person is and when they are coming in. But we don't have direct again integration into our account system. That is something that came up at one of our training days, where we learned about their dispatch system and things like that. It's very different than ours, but maybe further down that line of different counties and agencies, we could do something to at least link to their dispatch system. It's not very high on our list, but it's something that is out there.

Interviewer: Do you think the people making decisions and policies for your group and beyond have a good understanding of the scope of needs and the resources necessary for that to happen internally?

Respondent 2: Yes, it definitely takes some more education when it gets up to the board level as each step gets removed. There's more education and more discussion that needs to be had internally. Our internal leadership knows what we need and where we need to get where we are going. Then at the strategic advisory board level, we need to bring them in a little bit and give them more information. Going up to the executive board level and then the full board, we need to really bring it to their level so they can understand what we're trying to do. They are supportive of a lot of efforts that we're trying to do when it comes to replacing a technical system or improving one.

Interviewer: So how does that work, or are you briefing management? Are they allowing subject matter experts to come in and provide that education?

Respondent 2: A little bit of both. I am the bridge. Our director briefs them on budgeting and some of those other high-profile topics. But routinely, I am at our executive and board meetings, giving them status updates on all of our technical initiatives [and] answering any questions they occasionally have. Like with the radio project, we hired a subject matter expert and he has been doing a fantastic job educating them on coverage and interoperability and where we're at with the process. But when it comes to the day-to-day project upgrades we are doing on our help desk system updates or we are doing on our CAD system, I can usually bridge that gap as well as our director. He and I kind of just trade-off.

Interviewer: Do you have any glaring concerns with just day-to-day operations and the ability to work between agencies and in and within agencies? Is there anything that jumps out as a challenge, weakness, or concern that you have right now?

Respondent 2: I think our biggest concern is the CAD system as a whole is a very complicated, complex system, and no one can really know all the ins and outs of it. But we found a number of show-stopping bugs that we have been working on with [our vendor].

The respondent indicated that their vendor's responsiveness to these issues has been challenging. They have had tickets open for an extended period of time that are related to important functions, like visibility which impacts situational awareness and safety. The respondent acknowledged that each CAD system has its own challenges, and all CAD systems have had different amounts of turnover. However, these issues have caused them to consider whether they want to pursue a solution or vendor that better fits their needs.

Interviewer: Do you see third-party contractors as more of a vulnerability than the internal work you're doing? Because it sounds like, internally, things are a pretty well-oiled machine compared to many places. You seem to have a lot of resources, support, and experience.

Respondent 2: Yes, I mean, look at what we've done with COVD: we pioneered remote 911 call-taking and dispatching. And again, it started with just a computer and a monitor and a phone, and it proved [itself] over time, and through that process, it has become something pretty amazing. Our limitations, right now, are not on our side…We exposed problems that were not an issue until we started using this stuff in a different way. And [we are] just trying to get that better and better because it's never going to be perfect. But it needs to be as robust as it can be given the subject matter we're working with.

Interviewer: [What do you think causes these issues with vendors?]

Respondent 2: From my talks with multiple vendors…it seems like it's a manpower priority issue. You know they need more and more well-trained staff to solve some of these problems. They need to fit it into their business plan because they already have [other projects and priorities]. They have to figure out how to [fit in the work when a bug comes up. They may have had turnover, and the] person that helped write that code isn't the person that's helping maintain it anymore. So, someone else has to go unravel it and figure out why this bug is happening and how to fix it.

Interviewer: Who do you think sets in the pace with these advancements? Is the industry keeping up with the needs of the business, or are they holding it back?

Respondent 2: At least from the vendors that we are working with, they are a step behind us in our needs… there are people okay across the country pioneering different ways to use the software. [Industry is] making the software, and then we're taking it and using it in a way that they never thought of. [Particularly for consolidated centers, it] is a challenge trying to find [a vendor] that's meeting the needs of two very different agencies with the same piece of software.

Interviewer: Do you think there would be a benefit if these providers and companies provided more of a collaborative working group setting? Would you be open to this type of collaboration?

The respondent acknowledged that this is already happening. With some of their vendors, they send multiple technicians to meetings and conferences to learn and also to share experiences and feedback with others. This is a valuable experience for attendees and also the vendor itself. They can absorb feedback and better understand the needs and challenges of their customers. It's a chance for attendees to air their challenges and hear from others users who may have experienced the same things. The respondent sees a lot of value in sending people from his unit to these conferences, even despite the cost associated with it.

Interviewer: [Your region seems to be at the forefront of innovation in this regard. Why do you think that is? Is it because of a competitive culture?]

The respondent acknowledged part of the reason for this is competitiveness but also pointed out that their advancements in this area can also be attributed to the politics of the region and a willingness to collaborate and help others in the area.

Respondent 2: We like being first. We also like helping the other person get their work done and be first, too, because it ultimately helps all of us.

Interviewer: How did you get there?

Respondent 2: I think it's our leadership, [specifically] our director…Also, the tone of [local conferences] is very open and very collaborative. [The approach is:] "here is what I have learned, let me help you learn it, and let me help you do it."

The respondent described how his director is involved in many conferences, networks, and associations. He is never afraid to leverage his network to assist

people in finding the answers that they need. This is also something that the respondent attributes to successful collaborations in their own organization. They make connections with others and lean on their network. Relationships matter.

The respondent also described how they had recruited people from other areas of the country where there were more roadblocks. He raised the possibility of the problem of collaboration and interoperability getting worse at the national level because talented and driven people are migrating to specific areas with a better working environment. Remote work is also driving some of this workforce shift.

Interviewer: As we have discussed the possibility of connectivity and interoperability, it is essential to ask, how much data is too much?

Respondent 2: I dread photos and video, [particularly] what to separate from our dispatch staff and how to deal with public disclosure.

The respondent sees this as a forgone conclusion but envisions that it will be a challenge to deal with analytics. At some point, there may be a need for a full-time data analytics role – someone whose job is solely to report dashboards.

Interviewer: How far does that circle need to go for data sharing?

The respondent described a recent exercise they did with another area. As part of this exercise, they took down their system offline and fed their calls into the respondent's system.

Respondent 2: Those smaller agencies don't always have the budget or the staff for redundancy, and we larger agencies can help them out with that. We can help them be more redundant and resilient. That way, if they have a fire [in their area,] we are not going to have a wildfire on our side…[In becoming] much more interoperable…you're really laying the groundwork for a disaster situation.

Transcripts and Notes Quotes from Interview with Respondent 3

Interviewed Virtually by Authors in September 2022

This respondent has worked in multiple agencies as a CAD administrator.

Interviewer: In your experience, what impedes collaboration?

Respondent 3: There's collaboration in our agency; there is [also collaboration] out in the field. Mostly [the impediments are caused by the] lack of memorandums of understanding (MOUs) between the agencies. Since I got here, we have been trying to get them to talk together because they actually work together, especially the county with all of the cities. They have different software - different things - and even though we can make it talk on the software level, on the political side, there's a lack of MOUs and agreement between the agencies.

Interviewer: Why do you think that is?

Respondent 3: There's discussion about it, but it never moves to the implementation stage. They talk about it, they have meetings, and they have reps from the different agencies… but at the end of the day, it just dies because there's no follow-up. Currently, the effort to collaborate is renewed and they are pursuing MOUs again. This is being pushed by a vendor for safety reasons because they need to share data.

Interviewer: Is your agency just law enforcement only?

Respondent 3: Yes, we have probation, jails, and adult probation.

Interviewer: You mentioned a [new] radio project. Tell me more about that. Are you implementing a new system?

Respondent 3: Sort of - we are upgrading and there is a VHF radio upgrade that basically adds more power. Then there's more real estate on the towers that are owned by the county. So, there's more equipment that needs to go on in-place because there's a safety aspect of it. In this field, the deputies have horses, boats, and all kinds of stuff, and in some places, they don't have any signal. They don't have a place to take a computer with them, but they have the radio and sometimes the radio doesn't have coverage. That's what we are trying to do. We are trying to get them coverage everywhere.

Interviewer: So, kind of officer safety?

Respondent 3: Yes, increase coverage.

Interviewer: So, regarding technology and sharing data, especially covering such a large agency, what does that look like for you?

Respondent 3: Yes, for us, it's a major aspect. We're going out for an RFP [a Records Management System (RMS)], like the computer-aided dispatch and report management systems. A part of that is the data-sharing abilities that we currently don't have in place. We will be new to the RMS area because we have somewhat of an in-house developed RMS and that needs to go away. They are looking into putting everything into one ecosystem. One of the things is data sharing amongst other agencies. We've been having meetings with other agencies, and they have MOUs in place to share data amongst themselves.

Interviewer: So you want a regional impact?

Respondent 3: Yeah, like some people commit a crime down [in another city], and they come down here.

Interviewer: What is the political perspective of that?

Respondent 3: On the political side of it, it's just getting the MOUs in place and getting the powers that be to agree. One can be seen and cannot be seen because on their side, there's the challenge on the technology side. And then there is a challenge on the political side. The political side is mostly about [the fact that] some people want to see that data; some agencies are more restricted than others. [For example,] I can tell you from my experience that I worked for another Public Safety agency here in [the region], which is more restrictive than everybody else. They don't want to share a whole lot of data, and if they do, they won't even give you something as simple as the address. They will actually give you the 100 block out of that address. But they won't share the actual address of whatever happened.

Interviewer: Would you say that is the leadership? Is that kind of the culture within those agencies, and it's trickling down and preventing the MOUs from being put in place?

Respondent 3: It's mostly the old-school mindset and culture of "this is the way we've always done it" instead of moving forward and looking into a broader vision and data sharing, which would actually improve deputy safety. That's a big aspect of it, and that's something that we encounter. Once you get when once you

get somebody new, there's a little bit of change. But even that person, being in that higher position, gets pushed back from the ones down [the line].

Interviewer: I think it's obvious that you're probably infrastructure limited, just with the large area. Do you feel that your technology is limited as well? Do you feel that the current technology just doesn't support your mission; are you past technology at this point?

Respondent 3: Based on the ride-alongs that I've been taking with deputies, they say on the technology, we are spot on, but we lack in other areas. So, we are trying to fix it, but the vision from our CIO here is "moving forward into technology." That's a plus that we don't see in other agencies. The technology in the county here is about the cloud, virtualization, etc.; we have all of the new toys.

Interviewer: Are there budget limitations to that?

Respondent 3: Yes, but we ask. We get a fair amount per year for technology, so we've been able to manage for that. If we require a new system, like the one that we're going to purchase [the RMS system], that's going to go out, it got approved by the Board of Supervisors. This just takes a long time to get a budget for things. Let's say that we're looking at this new system, and by the time we get it, that's somewhat outdated. That's the only challenge because of all the approvals and all this stuff.

Interviewer: Does your sheriff have to incorporate his budget into the county budget?

Respondent 3: He gets a chunk; we get a chunk out of the county budget. We get a fairly good amount.

Interviewer: What kind of system are you employing? What's the base of that technology? Is it radio-based? Is it cell-based?

Respondent 3: Well, it's all it's very chatty; it's a network, and what we have is a combination. We have interfaces with the radio for certain functionality. We have cells. Out in the field, they have cell technology through carriers. We have two carriers - we have a combination of Verizon and FirstNet (AT&T). It depends on the area that they are in. We've been able to get around with a dual network.

Interviewer: Is there a plan to go to a singular network, like FirstNet?

Respondent 3: Not at this point. We have the two carriers because we found limitations with just one. With FirstNet in certain areas, it defaults back. A deputy can be working today the lake, and tomorrow he'll be working all over all you know, across [another area].

Interviewer: We talked about budgets. We talked about technology. It seems like you guys have the financial support for equipment and technology. But would you agree that your partner agencies have the same? Or does that create a barrier that you guys are farther ahead or are more supported than the others?

Respondent 3: Hmm… well, it depends. Where I come from was a little faster to get things. This is because it's so large [in my current county]; it's a little harder to implement things with so many sites and people in training, and there are a lot of logistics that come into it. With [my prior] city, it was a smaller agency, but they did have the budget for all of the new infrastructure and stuff. [This area] - and all of the agencies that we've discussed - are on point with technology.

Interviewer: Is there a security concern? With data being put into the wrong hands and reflecting poorly on the agency in the media? Or is it more just that people are old school?

Respondent 3: A little bit of both. There's a security concern, and there is a culture change. As an example, I just gave some data to a third party, and one of the things that I was asked to remove was the unit information - the deputy information. They don't want anything linked to the deputy in the media. So, it's security, but that can be actually taken care of… if they don't want us [to share that it] can be blank. That value can be replaced with a generic value. We can get around that and but at the same time, there's the culture [of] no, we have always done it this way - we don't want that. That's slowly changing, and that's been a battle. It's moving slowly, but it's moving here because there has been kind of like a change here. The CIO came from the private sector, and I came in from the private sector. A bunch of people came in from that…so there's a little bit of a culture shift. We're trying to do things and kind of push for more instead of when

you say no. When we get shut down by upper management, we try again. We try again with, "let me provide you these things" or "what about this." Instead of just saying we tried, [we keep trying].

Interviewer: So it sounds like you've had the opportunity to do some ride-alongs. Can you share any insight into what the deputies want as far as information sharing? Do they feel like they have enough?

Respondent 3: Well, they want more, but they want it all automated. They would like the full picture. They want as much information as they can get.

Interviewer: So the efforts towards agreements are those more for big emergency incidents, or are they for day-to-day?

Respondent 3: They are for day-to-day. You can actually integrate it into a search when they're searching for a person.

Interviewer: So what kind of information are they looking to gather on those queries? Respondent 3: If that person has a warrant with another jurisdiction, or something happened within a jurisdiction…the special situations… if that person is anti-police, for example. They want to know for safety reasons.

Interviewer: When I contact someone and run their license or name/DOB, I can actually pull up every contact that any agency has had with them. Is that something that you're looking to do?

Respondent 3: We can do that in vehicles, but not any agency. What they're looking for is integration, like we have a bunch of subsystems that they can do

that and they don't use them. Because they just use the main thing and they are looking for integration. There's this thing called Coplink that was a big thing. It kind of grew, then it just died. Over here, nobody uses it; it just died.

Interviewer: Let's dive into that a little bit. Why don't they use it?

Respondent 3: I don't know. I heard it was fairly complicated to use. It's separate software, and if it's not integrated into what they use every day. That's a big thing. Everybody had their own thing and preferences with layouts and seeing the information. It wasn't customizable; it was - this is what you get. It died down and hasn't been used in the Valley for a while.

Interviewer: Do you know how many agencies that [your county] is looking to establish the MOUs with?

Respondent 3: At least the ones around the [area]. And they know that the others are talking to each other. They found out third-hand, and they want to jump in.

Interviewer: Okay, is that something that [your county] would end up being the champion of?

Respondent 3: We want to connect into it - that would be great. But I don't know about taking charge of it. Now we're not even on the same system. We'll have to look into an integration with whatever they have and kind of look into that. It will be a little limited for us right now.

Interviewer: So, does that mean everybody must go on the same system?

Respondent 3: Probably not, because you have integration through their systems. You have integrations through interfaces and stuff like that. So you can make it talk to each other regardless of who it is.

Transcripts and Notes Quotes from Interview with Respondent 4

Interviewed Virtually by Authors in September 2022

Respondent 4 works in technical services and has worked in public safety in a variety of roles for more than two decades.

Interviewer: What do you think impedes collaboration?

Respondent 4: Our county is probably fairly unique in that our agency is very collaborative. We share a common CAD system across the agency. What prevented it before was jurisdictional boundaries based on old models. You have a police department that has a call center, a fire department, and costs began to drive efficiencies. And then data sharing became important, especially on the law enforcement side. We have the RMS that has been shared for many years. But then you go up to [another region], and they don't [collaborate or share information]. They're very segmented by areas...I think a lot of times they want to [but don't know how.] There's always going to be a boundary…so, the [the question is] how far do those boundaries go [and do they stretch]? Like ours in our county…And do you have the interfaces to do it? I don't think it's about a desire…I think largely, it's not about [the fact] that technology can't do it, it's about how to get the right people in the room and the right folks from the vendor side to put things together to make it easy. It's hard. It's hard to make things easy…I think it all comes down to people and vision, and what are the cost benefits to do it. And I think there's a ton but sometimes it's making that case.

The respondent discussed how interfacing and connecting systems isn't a one-and-done job; when you make upgrades or changes, you must re-do the

interfaces, which gets complicated and time/energy consuming. The question becomes, how much is it really worth it to share? The respondent also discussed how important relationships and people are to collaboration.

The respondent shared that they have a lot of mutual aid agreements that are built into their CAD. Rather than asking a neighboring county for medics when they run out, they can run it. The respondent attributes this collaboration to all of the trust and relationship building that has been done through professional associations and fostering good relationships over time. Much of this interoperability effort begins with the leadership.

Interviewer: Where do you think the optimal stopping point is for the boundary or the circle of information sharing?

Respondent 4: I think that's an interesting question because, depending on size, sometimes such a large volume comes in and you kind of lose focus on the mission. It gets almost too busy. So, it's a hard question to answer because I feel like ours, like [my agency] is kind of on the edge of [having] too many eggs in one basket. If our facilities go down, we have a million people relying upon this agency. [Although we have] a backup facility, but where do the calls go? We can't ask [our neighboring counties to] take 1,000 calls per hour and just do it while we figure out what we're doing right. You might need to bifurcate a bit.

The respondent believes that counties with smaller communities are well positioned to take charge of dispatch, but in counties with bigger ones, it might be too much.

Interviewer: How much is too much information?

Respondent 4: There's a radius that makes sense; what's the mileage? Criminals move around the city; they don't know jurisdictional boundaries.

Depending on the area, you might need to see cross-state or county information, but in others, it might be irrelevant. The respondent described an analysis that was conducted with a joint terrorism task force grant. Through this story, the respondent highlighted that they often will find out about things from social media before getting it between call centers. He doesn't believe that they need to know about traffic stops, but shootings and other situations, like civil unrest, would be helpful to know about, just from an awareness point of view. In his area, the fusion center is working on aspects of this issue. Ultimately, the respondent believes that each agency has to determine its right-size for this; there isn't a magic formula.

Interviewer: How does it work with [your county] when you want to implement new technology?

Respondent 4: We're an independent agency, and we have a board of directors that are elected officials. We have an operations committee that kind of steers operations…sometimes [ideas] come from them. Other times, we come across

something that we see value in…It's not like one agency drives what we do. Agencies that do consolidations and still manage it have a harder time…when you can make the PSAP or ECC its own department, it is better…but not all states have that.

The respondent discussed the implications of changes and updates to their interfaces since they use them so heavily. Anything with APIs is helpful, according to the respondent. This is critical to any platform. Additionally, training and knowledge are critical. A lot of times, planning and training don't happen, and as a result, people do not use all of the tools in their tool chests.

Notes and Selected Quotes from Interview with Respondent 5

Interviewed Virtually by Authors in September 2022

The interviewee, Respondent 5, provided details about the evolution of the very formal Joint Powers Agreement comprised of agencies in his area. Through this effort, they have condensed to six public-safety answering points (PSAP) that are independently operated. However, each PSAP uses the same computer-aided dispatch (CAD) system. These all feed into a centrally managed system. As a result, "all of [their] public safety officials or responders are all, in essence, connected through technology."

Interviewer: How big do you think that circle can go? Does it just make sense in your area? Or does that circle eventually expand regionally or statewide?

Respondent 5: There is definitely room for growth. Ironically, some of our neighboring counties use Hexagon CAD, but we have no connection to them whatsoever.

Part of the struggle with expanding the connection to other areas and agencies stems from this type of technological challenge. This is something that was assessed a decade or two ago, and at the time, it was deemed too challenging. The idea was abandoned.

Through the consortium formed under the Joint Powers Agreement, one objective is to expand its reach. The idea is that one dispatch center can support any other dispatch center. So if one dispatch center goes down, another can step right in and fill that need.

Respondent 5: We have had major wildfires from 2017 - 2022, and the impacted agencies that were doing most of the work could actually call dispatchers from other police departments and have them show up. They could step into a terminal, and it was just like they were at their home agency. This allowed us to size them up quickly…I would love to connect our CAD systems also our records management systems with our neighboring counties who are on the same platform.

The respondent has started these conversations with neighboring counties, but, because some of these areas have undergone transition, it has been a challenge to find someone to spearhead this effort. Additionally, a lot of the people now in information technology (IT) specialist roles do not have formal training. Within the respondent's unit, they employ six IT professionals and they pay competitive wages.

Another challenge to expanding "the circle" is cost. Particularly for smaller departments, the cost of joining a consortium can be hard to swallow. Rather than incurring the cost, these small departments have chosen to take their chances on their own and continue with the status quo in their units.

Interviewer: Are there any impediments other than costs for these agencies not to join?

The respondent initially didn't think that there were many but then acknowledged that sometimes there may be governance issues. These may wax and wane depending on the perspectives and experiences of council members and other officials. From the respondent's perspective, governance issues are not a pressing issue in his unit. However, human bandwidth is a major issue.

Respondent 5: All of this [coordination and collaboration] takes time and energy. Even though I am [in a leadership role], I am just part-time and work 20 hours a week. Just keeping the lights on - putting together board packets, answering trouble tickets, managing the vendors, etc. - takes up all my time. So building out a much larger reach is just kind of a time suck that I haven't been able to invest in. But it can be done.

Interviewer: Can you speak to the benefits of the consortium?

The respondent discussed their approach to cost allocation within the consortium. This allocation is currently under review, and the respondent is hopeful that there will be changes to how it is handled. There are small agencies in their county that are interested in joining the consortium, but the way that cost allocation is handled at present makes it too expensive.

Respondent 5: Fires aren't contained within the jurisdiction of a city or a county, and I can certainly guarantee criminals are not confined within the confines of the

jurisdictional boundaries; the more we can work collectively for the common good, the better it is for all of us.

Interviewer: What has your experience working with state and even federal jurisdiction been like? Is information sharing done manually, or is it built into your systems?

Within the respondent's county, an individual within the sheriff's office has taken the initiative to develop a homegrown database. This system pulls in CAD data, records management data, state parole data, pawn shop records, etc. and rolls it into a huge database that serves as a one-stop-shop. This data is then scrubbed and shared with their local fusion center, which in turn shares it with their accounts and uploads to relevant other centers and data exchanges. The purpose of this system is to get the data into the hand of people who might use it.

Interviewer: Are you getting real-time hits on contact with vehicles or persons?

The system does not always provide real-time hits.

Interviewer: Using a kidnapping case as an example, walk me through the process and impact of the consortium. With a kidnapping, you're at the mercy of the responding officer to ensure that you have a "good" kidnapping. Then you have to wait on the supervisor to approve the bulletin going to dispatch and then wait for them to send it out to the communication

system. You must also wait for the dispatchers to send that out, then for the State's approval, and finally for the broadcast. This can be a pretty extensive timeline. How does the consortium impact this?

Respondent 5: We can message every dispatch center instantaneously. We can set flags on certain types of calls that will alert the neighboring dispatches and centers immediately about kidnapping homicides, vehicle pursuits, officer-involved shootings, etc.

Interviewer: And as soon as you've got a solid 28, the record, and you'll start getting hits on that?

Respondent 5: Even before then. You would know if our neighboring jurisdiction all of a sudden is working on a kidnapping…but you know they're working on something immediately. [There has been a big impact to the amount of time required to get relevant information into the hands of the people who need it.] The challenge that we haven't talked about yet, which is the big elephant in the room, is disparate radio communication systems. Not only is it just different channels - which, of course, we have to split the channels up a little bit - but because there's too much traffic. We have completely different platforms. We're a rural county, and so is the sheriff's office, which also means its contract cities are all working on low bands still. All the newer cities are all wanting to go to 800 megahertz because it's the newest and greatest, but the county refuses to do it because they

feel that it doesn't have the proper wavelength to kind of get through hills and valleys, and through trees, and so on, and so forth. So that can be overcome by adding more radio towers, but the cost of that is tremendous.

A county near the respondent passed a huge tax measure to fund a new program. However, they essentially handed all control of the system over to the vendor.

Interviewer: Do you have any options through the state to allow it to take over and maintain your tower sites if the county bears the upfront cost?

Respondent 5: I haven't heard of anything like that. When you think about radio communications, except CAD, we don't need our records management system during a disaster. We don't need to have great mobile data computers during disasters. But you need a radio for sure. And so the radio towers become so important. There is a technology [available for this] because they asked me to look at it. There's a technology that you can literally marry those 2 platforms together right there, switches and routers and access points, and so on, and so forth - much like you do with your cell phone. So as you move within your county, it just picks up the closest radio tower, and it figures out what radius system you're on and flips it to that switch. It can be done, but it requires coordination.

Interviewer: Have there been any incidents in your area that would push your county or state to pursue this more aggressively?

Respondent 5: We've had disasters. There's a 100-year flood that comes every 10 years in the river. They've always been prepared for the earthquake, which means that you sit through the class… but we were taught our lesson when the 2017 fire hit and burnt through our county in about 12 hours, and we lost almost 6,000 homes. It went through multiple jurisdictions. The chaos of that event created enough stress for us to at least look at it but not move on it. Part of it was trying to move more at the state level because we had immediately lost communication since we have two primary cell vendors out here. We lost a ton of [one of the vendor's] towers immediately. It was a mess. There were towers [owned by another vendor] that were good, but they wouldn't allow them to share bandwidth.

Interviewer: Are the policymakers generally supportive of this work, or do you feel like it's on the back burner until it becomes a problem again?

Respondent 5: It's on the backburner again…Public safety is a secondary thing.

Interviewer: Do you feel like your technology limits you?

Respondent 5: Oh, yeah, the challenge that I'm having with technology is vendors perpetually over-promising and under-delivering, and everything takes forever to get fixed. That has been my biggest frustration. My analogy to them is it is like we're married to them, and they're married to a bunch of people. They're sharing their time with all their spouses, and we only have one. So, we are just

begging for some attention, and it just it's a frustrating experience. They're in a tough spot because what happens in Texas, Wisconsin, Minnesota, or Tennessee may not be what happens for us. They're trying to find solutions that fit everybody. I know it's a challenge for them, and it's not easy. But I would certainly like to be able to have a smoother operation when it comes to implementing new technology or managing technology.

Interviewer: When you upgrade or change with your vendors, and you have troubleshooting problems, do you always go through the same person - for example, the same tech writer? Or do you notice a high level of turnover with them or even just deal with different people? We've heard from other counties that it's very competitive and difficult to find these tech workers right now.

The respondent indicated that one of their vendors has been fairly stable in their support and points of contact so far. Another vendor they use recently underwent a large-scale merger that has caused significant delays. This vendor has also gone through massive turnover, which puts many of the respondent's projects behind schedule.

Interviewer: As far as the consortium, when you switch vendors or implement new technology or projects, are you always working within your

annual budget? Or are you having to go to the participating agencies for more buy-in? Can you explain how that works?

Respondent 5: The way that we used to do it was – let's just say an average upgrade would cost half a million dollars, and we [upgrade] every five years. The annual maintenance agreement is $100,000 every year, so we would charge our members $200,000 per year. $100K would go to maintenance, and $100K would go into the savings account for the future. So at the end of 5 years, we always had a bucket of money to either upgrade or even change vendors. Granted, a change of vendors would cost more, so we would have to assess our members more or find that savings somewhere else in our budget.

The challenge I see going forward is a brilliant move on be part of the vendors. Now we're all subscription model, so instead of costing a $100,000 a year, it costs 150,000 dollars a year. But your upgrades are included. What happens is at the end of 5 years is that we don't have enough money to leave [the current vendor]. This presents an interesting challenge that [we have to tackle]. Do we want to continue to start assessing ourselves additional costs so we have this money? If we stay with our [current] vendor, it's just a kind of a waste of taxpayer money just sitting in the same account, right? But it also puts us in this really weird position where we are kind of beholden to the vendor because we have no cash.

I think in the past we've had issues with our small agencies during economic downturns. The bigger agencies oftentimes just kind of subsidize them for a year or two until they get back on their feet, thinking that together it is better to use that phrase. But you have to get through the hump so to speak.

Interviewer: Does centralized IT support all the agencies?

Respondent 5: Kind of. Our centralized IT support are actually county employees. They manage the databases and the applications. Every agency is supposed to have their own IT staff who kind of manages their end of it. We don't do desktop support for them. We don't do NDC support for them. We do all the kind of the back end which isn't great. There's not really a better model right now.

Interviewer: Is the county just a regular member [of the consortium]?

Respondent 5: Yes, the county has one vote. The county is the largest agency in the consortium and they have one vote. The consolidated dispatch center has one vote, and our smallest agency, with a tiny budget, has one vote. Granted, the bigger agencies kind of set policy, and they kind of drive everything because they do the majority of the work. The idea is, every application has a lead from one of the agencies. We have our RMS lead, a CAD lead, a mobile lead, etc. The big agencies are the ones who have always taken that responsibility because they have the bandwidth to do it.

Interviewer: How are members appointed?

Respondent 5: Per our agreement. We identify the positions that can be on the board, so for instance, at the city level, the city manager is the appointed board representative, but they can delegate to one person, which is their police chief. So most of them have delegated to the police chief. [However, I see value in not delegating.] I want two or three city managers on my board, because they bring a very unique perspective about budgeting and forecasting. I want to keep some city managers. It's up to them to decide but [the appointee should] be someone who can make policy for them.

Interviewer: Are you a taxing entity, or allowed to be? Are you strictly subscription based on the members subscription base?

Respondent 5: Subscription based. The idea is that every agency that is a member of the consortium takes a little portion of their own budget to pay for the consortium cost.

Interviewer: [Going back to the radios you mentioned,] do you have that within your county, as well? Between police, fire, and EMS? Or are they all on that low band system?

Respondent 5: The Sheriff's department is the only group I know of that actually has a telecommunications division. They provide radio support to the county to the sheriff's department, their contract cities, to probation, which is a county entity…all of the fire and EMS agencies are all on the county network, and then

two of the smaller cities are the other ones. All have their own independent radio systems.

Running your own radio systems is a beast. There has got to be a smarter way of putting radio systems together. Our [large city] just got a new 800-megahertz radio system, and the baseline system can handle like 40,000 radios…So, the county is anticipating that if we ever want to go to the 800- or 700-megahertz systems, they are going to have to double their size. [This will require] 30 plus radio towers, so we have been [discussing that there must be a] way to partner with vendors, like ATT and Verizon. They have towers built: [what if] they can throw their equipment on our towers, and we can put our equipment on their towers. It seems like it's a win-win but it just takes someone to champion that cause and drive it forward. Everybody's overworked and the political will doesn't appear to be there…

The fact that we've got decentralized law enforcement dispatch centers is way behind the bell curve. Consolidated is the way to go. [When you go to regional and national meetings] you hear that every agency has a dispatch center, has multiple consoles, multiple licensing, multiple infrastructure… and half of them are understaffed by 50%. We can consolidate them into one spot. No one would lose their job because there are enough vacancies already. We could actually build probably two dispatch centers - one to back up the other and even

share radio traffic. But again, we've looked at it a couple of times but never had the political will when it gets down to the nuts and bolts. Some cities pay their dispatchers more than others, so [there is the issue of] fair wages. You can't have people who are doing the same job being paid so differently. Do you create an independent joint powers agreement? That's just the dispatching centers, and that's a big political animal. There is a lack of political will to make that happen.

This type of change requires visionary county leaders who see the importance of public communication.

Interviewer: [How do you think that can be accomplished?]

Respondent 5: In this particular case, the only way I think we're going to get it done is if it's legislated. If the Legislature comes down and says we are going to consolidate dispatch centers, then everybody has an excuse. Everybody has the political cover.

We have looked at it a couple of times, and it seems to make sense on paper. We have never [enlisted the help of] a consultant; we have never gotten an outside vendor. We just have people jump on the subcommittee and work on what it looks like to be consolidated dispatching. It looks fine until you've hammered out the nuts and bolts. Then all of a sudden, the dispatcher realizes [that they are] the senior dispatch person for [their] agency. [As such, they] have days and weekends off, but [if they] consolidate, [that senior dispatch person becomes] like fifteenth

in line. So, all of a sudden, [that person is] losing nights and going to nights and weekends. [This] put[s] a lot of pressure on [the] chief who then gets soft because he doesn't want to upset his staff. So, then he then begins to back out and the political will falls apart.

The only way to do it is to have a legislative requirement as a cost, savings measure and an interoperability opportunity…In this case it's only I can think I can think of being done.

Notes from Interview with Respondent 6

Interviewed Virtually by Authors in October 2022

- *The respondent described the obstacles their agency faces. The biggest of these is related to the fact that the agency covers two separate states. These challenges include:*
    - *Each state does things completely differently;*
    - *There isn't a flow of training or information across state lines;*
    - *One of these states has a great program for hiring, history, and eligibility which greatly helps in preventing bad hires. There are also training standards and enforcement mechanisms. The other state has none of these programs or requirements;*
    - *There is currently a major labor and talent shortage; and*
    - *Within the profession, there is also a substantial disconnect with public service.*
- *The agency has great benefits, so their recruiting is better than others in the area. However, they still struggle.*
- *The respondent believes solid political will and support to move things forward is required. It is important to educate the decision-makers. When they learned more about the job, they became more supportive.*
- *Funding has not been a struggle because of the agency's size and location, but it has been a major issue for smaller localities.*
- *It is important to make sure technology adapts to personal technology.*

- *Grants are too specialized for small jurisdictions. Now, a lot do not even apply.*
- *Collaboration is issue dependent. All CAD and technology are the same in the area because of county oversight. Aside from systems and technology, agencies work well together.*
- *Neighboring counties: a lot of neighboring jurisdictions. There is a very rural, poor agricultural county. According to the respondent, the agencies have focused on addressing these areas and dropping borders. The technology works well together, with no issues sharing information.*
- *There are some political issues though but most ignore the red tape.*

Appendix B

REFERENCES

Alsamhi, Saeed Hamood, Faris A. Almalki, Hatem AL-Dois, Alexey V. Shvetsov, Mohammad Samar Ansari, Ammar Hawbani, Sachin Kumar Gupta, and Brian Lee. 2021. "Multi-Drone Edge Intelligence and SAR Smart Wearable Devices for Emergency Communication." *Wireless Communications and Mobile Computing*. doi: 10.1155/2021/6710074.

Arghire, Ionut. 2022. "German Wind Turbine Firm Hit by 'Targeted, Professional Cyberattack'." *Security Week*, April 26. https://www.securityweek.com/german-wind-turbine-firm-discloses-targeted-professional-cyberattack (October 18, 2022).

Baez, Benjamin. 2002. "Confidentiality in Qualitative Research: Reflections on Secrets, Power and Agency." *Qualitative Research* 2 (1). 10.1177/1468794102002001638.

Blair, Pete. 2022. *Texas State University; Advanced Law Enforcement Rapid Response Training ALERRT.* January 3. Accessed October 10, 2022. https://www.alerrt.org/ (November 12, 2022).

Bloor, Geoffrey and Patrick Dawson. 1994. "Understanding Professional Culture in Organizational Context." *Organization Studies* 15 (2). doi: 10.1177/017084069401500205. Waretown, NJ: Apple Academic Press.

Brough, Paula, Shannyn Chataway, and Amanda Biggs. 2016. "'You Don't Want People Knowing You're a Copper!' A Contemporary Assessment of Police Organisational Culture." *Police Science and Management* 18 (1). doi: 10.1177/1461355716638361.

Buchanan, Kerrianne, Yee-Yin Choong, Shanee Dawkins, and Sandra Spickard. Prettyman. 2021. "Communication Technology Problems and Needs of Rural First Responders." Paper presented at the 18th International Conference on Information Systems for Crisis Response and Management, Blacksburg, VA. https://www.nist.gov/publications/communication-technology-problems-and-needs-rural-first-responders (November 9, 2022).

Burrows, Dustin Moody, Joe Guzman, Eva. 2022. *House Investigative Committee on the Robb Elementary Shooting.* Interim report, Uvalde: Texas House of Representatives. https://house.texas.gov/_media/pdf/committees/reports/87interim/Robb-Elementary-Investigative-Committee-Report.pdf (November 12, 2022).

Carreras-Coch, Anna, Joan Navarro, Carles Sans, and Agustín Zaballos. 2022. "Communication Technologies in Emergency Situations." *Electronics* 11 (7): 1155. doi: 10.3390/electronics11071155.

Channa, Muhammad and Kazi Ahmed. 2010. "Emergency Response Communications and Associated Security Challenges." *International*

Journal of Network Security and Its Applications 2 (4). doi: 10.5121/ijnsa.2010.2412.

Cohen, Galia. 2018. "Cultural Fragmentation as a Barrier to Interagency Collaboration: A Qualitative Examination of Texas Law Enforcement Officers' Perceptions." *American Review of Public Administration* 48 (8). doi: 10.1177/0275074017744659.

Bazen, Elizabeth. 2005. *Robert T. Stafford Disaster Relief and Emergency Assistance Act: Legal Requirements for Federal and State Roles in Declarations of an Emergency or a Major Disaster*. RL33090. https://www.hsdl.org/c/abstract/?docid=456375 (November 11, 2022).

Cybersecurity and Infrastructure Security Agency. 2019. *National Emergency Communications Plan*, September. https://www.cisa.gov/sites/default/files/publications/19_0924_CISA_ECD-NECP-2019_1_0.pdf (November 9, 2022).

Cybersecurity and Infrastructure Security Agency. 2021. "Interoperability Continuum: A tool for improving emergency response communications and interoperability." https://www.cisa.gov/sites/default/files/publications/21_0615_cisa_safecom_interoperability_continuum_brochure_final.pdf (November 12, 2022).

Di Talia, V. and G. Antonioni. 2022. "The Integration of Social Media Data in Emergency Management: An Innovative Decision Support System." *Chemical Engineering Transactions* 91: 577–82. doi: 10.3303/CET2291097.

Disaster Relief Act of 1974, Pub. L. No. 93-288, 88 Stat. 143 (1974).

Fahy, Rita, Ben Evarts, and Gary P. Stein. 2022. *U.S. Fire Department Profile 2020: Supporting Tables*. National Fire Protection Association. https://www.nfpa.org/-/media/Files/News-and-Research/Fire-statistics-and-reports/Emergency-responders/osFDProfileTables.pdf (November 9, 2022).

Federal Emergency Management Agency. 2021. "National Response Framework." *Federal Emergency Management Agency*. https://www.fema.gov/emergency-managers/national-preparedness/frameworks/response (November 10, 2022).

FirstNet Authority. n.d. "FirstNet: The History of Our Nation's Public Safety Network." *FirstNet Authority*. https://www.firstnet.gov/about/history (November 9, 2022).

Gardner, Andrea M. and Kevin M. Scott. 2022. *Census of State and Local Law Enforcement Agencies, 2018 – Statistical Tables*. U.S. Department of Justice, October 2022. NCJ 302187.

https://bjs.ojp.gov/sites/g/files/xyckuh236/files/media/document/csllea18st.pdf (November 9, 2022).

Hofstede, Geert and Gerst J. Hofstede. 2005. *Culture and Organizations—Software of the Mind: Intercultural Cooperation and Its Importance for Survival*, 2nd Edition. New York: McGraw Hill.

Hollywood, John S. and Zev Winkelman. 2015. *Improving Information-Sharing Across Law Enforcement: Why Can't We Know?* Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/research_reports/RR645.html (October 19, 2022).

Homeland Security Act of 2002, Pub. L. No. 107–296, 116 Stat. 2135 (2012).

Homeland Security Presidential Directive–5: Management of Domestic Incidents, (2003). https://www.govinfo.gov/content/pkg/PPP-2003-book1/pdf/PPP-2003-book1-doc-pg229.pdf (November 12, 2022).

Johnson, Derek B. 2021. "CISA warns malware could be injected into emergency comms." *SC Media*, November 2. https://www.scmagazine.com/analysis/wireless-security/cisa-warns-15-states-that-malware-could-be-injected-into-their-emergency-comms (October 19, 2022).

Johnson, Gerry. 1992. “Managing Strategic Change—Strategy, Culture and Action.” *Long Range Planning* 25 (1): 28-36.

Johnson, Gerry and Kevan Scholes. 1993. *Exploring Corporate Strategy*, 3rd edition. New York: Prentice Hall.

Kapucu, N., Maria-Elena Augustin and Vener Garayev. 2009. “Interstate Partnerships in Emergency Management: Emergency Management Assistance Compact in Response to Catastrophic Disasters.” *Public Administration Review*, *69* (2), 297-313. https://www.jstor.org/stable/27697865/ (November 11, 2022).

Kapur, Girish Bobby, Sarah Bezek, and Jonathan Dyal. 2016. *Effective Communication During Disasters: Making Use of Technology, Media, and Human Resources*. Palm Bay, FL: Apple Academic Press.

Ladich, Samantha. 2018. “Asserting Collective State Sovereignty to Strengthen the National Network of Fusion Center.” Master’s Thesis, Naval Postgraduate School. https://calhoun.nps.edu/handle/10945/58326 (October 19, 2022).

Louisiana Governor's Office of Homeland Security and Emergency Preparedness. 2022. *Statewide Interoperability Executive Subcommittee*.

https://gohsep.la.gov/ABOUT/UNIFIED-COMMAND-GROUP/Interoperability-Subcommittee/SIEC (October 18, 2022).

Malone, Matthew A. and Sean Hildebrand. 2022. "Is There Coercion In Local Emergency Management Policy Implementation?" *Natural Hazards*, 113 (3): 1663–74. doi: 10.1007/s11069-022-05362-3.

Manandhar, Rejina and Laura K. Siebeneck. 2018. "Return-Entry Risk Communication Challenges: Experiences of Local Emergency Management Organizations following Superstorm Sandy." *International Journal of Mass Emergencies and Disasters* 36 (2): 120–48. http://ijmed.org/articles/743/ (July 22, 2022).

Middle Class Tax Relief and Job Creation Act of 2012, Pub. L. No. 112–06, 126 Stat. 156 (2012).

National Commission on Terrorist Attacks Upon the United States. 2004. *The 9/11 Commission Report*. https://www.govinfo.gov/content/pkg/GPO-911REPORT/pdf/GPO-911REPORT.pdf (November 11, 2022).

National Institute of Standards and Technology. 2022. *Digital Dispatch*. Public Safety Communications Research: Washington, D.C.

https://www.nist.gov/system/files/documents/2022/04/01/PSCR%20Digital%20Dispatch%202022%20Q1.pdf (November 9, 2022).

National Association of State EMS Officials. 2020. *2020 National Emergency Medical Services Assessment*. https://nasemso.org/wp-content/uploads/2020-National-EMS-Assessment_Reduced-File-Size.pdf (November 11, 2022).

Nayar, Vineet. 2014. "A Shared Purpose Drives Collaboration." *Harvard Business Review*, April 2. https://hbr.org/2014/04/a-shared-purpose-drives-collaboration (November 13, 2022).

Noran, O., & Bernus, P. (2011, October). Effective disaster management: an interoperability perspective. In *OTM Confederated International Conferences" On the Move to Meaningful Internet Systems"* (pp. 112-121). Springer, Berlin, Heidelberg.

Oracle. 2022. "What is IoT?" *Oracle.* https://www.oracle.com/internet-of-things/what-is-iot/ (November 9, 2022).

Presidential Policy Directive–8: National Preparedness, (2011). https://www.dhs.gov/presidential-policy-directive-8-national-preparedness (November 11, 2022).

Respondent 2. 2022. Interviewed by Authors. College Station, Texas.

Respondent 3. 2022. Interviewed by Authors. College Station, Texas.

Respondent 4. 2022. Interviewed by Authors. College Station, Texas.

Respondent 5. 2022. Interviewed by Authors. College Station, Texas.

Robert T. Stafford Disaster Relief and Emergency Assistance Act, Pub. L. No. 93-288, 88 Stat. 143. (1974).

Schein, Edgar H. 1984. "Coming to A New Awareness of Organizational Culture." *MIT Sloan Management Review*, January 15. https://sloanreview.mit.edu/article/coming-to-a-new-awareness-of-organizational-culture/ (November 8, 2022).

Schein, Edgar H. and Peter Schein. 2017. *Organizational Culture and Leadership*, 5th edition. Hoboken, NJ: Wiley.

Schnobrich-Davis, Julie and William Terrill. 2010. "Interagency Collaboration: An Administrative and Operational Assessment of the Metro-LEC Approach." Policing: An International Journal of Police Strategies & Management 33 (3): 506-30. doi: 10.1108/13639511011066881.

Sharp, John. 2018. *Report of the Governor's Commission to Rebuild Texas: Eye of The Storm. Rebuild Texas: The Governor's Commission to Rebuild Texas*. https://www.rebuildtexas.today/wp-

content/uploads/sites/52/2018/12/12-11-18-EYE-OF-THE-STORM-digital.pdf (July 21, 2022).

Stickings. Tim. 2022. “Russia’s Unsecured Communications Chatter Reveals Military Secrets in Ukraine.” *The National News*, March 28. https://www.thenationalnews.com/world/europe/2022/03/28/russias-unsecured-radio-chatter-reveals-military-secrets-in-ukraine/ (November 9, 2022).

Sun, Shili. 2008. "Organizational Culture and its Themes." *International Journal of Business and Management* 3 (12). doi: 10.5539/ijbm.v3n12p137.

Texas Health and Human Services. 2022. “EMS Certification and Provider Licensing Statistics.” *Texas Health and Human Services, Texas Depratment of State Health Services.* https://www.govinfo.gov/content/pkg/CFR-2002-title44-vol1/pdf/CFR-2002-title44 (November 12, 2022).

Title 44–Emergency Management and Assistance, 44 C.F.R.

U.S. Department of Agriculture. 2004. *Summary of Lesson Content: The National Incident Management System (NIMS)*. https://www.usda.gov/sites/default/files/documents/NIMLesson.pdf (September 20, 2022).

U.S. Department of Homeland Security. 2012. "Amateur Operators Aid Emergency Communications During Violent Storms in Tennessee." *U.S. Department of Homeland Security, Office of Emergency Communications*. https://www.cisa.gov/sites/default/files/publications/Case%20Study_Tennessee%20Violent%20Storms_0.pdf (November 12, 2022).

U.S. Department of Homeland Security. 2013. *Emergency Communications During the Response to the Boston Marathon Bombing.* https://www.cisa.gov/sites/default/files/publications/oec-case%20study-support%20for%20response%20to%20boston%20marathon%20bombing-2013.pdf (November 9, 2022).

U.S. Department of Homeland Security. 2015. *State, Local, and Tribal Coordination: Working with State, Local, and Tribal Public Safety Partners to Strengthen Emergency Communications*, July. https://www.cisa.gov/sites/default/files/publications/State%20and%20Local%20Coordination_Fact%20Sheet_July%202015%20FINAL%20508.pdf (November 9, 2022).

U.S. Department of Homeland Security Science and Technology Directorate. 2018. *Next Generation First Responder Integration Handbook*, Version 3. https://www.dhs.gov/sites/default/files/publications/997_NGFR-

Integration-Handbook_Version-3.0_Part01_180621-508_0.pdf (November 9, 2022)

U.S. Department of Homeland Security. 2019. *National Response Framework*, 4th edition. https://www.fema.gov/sites/default/files/2020-04/NRF_FINALApproved_2011028.pdf (November 9, 2022).

U.S. Department of Homeland Security. 2021. "DHS S&T Funds Critical Interoperable Messaging Capability for First Responders." *U.S. Department of Homeland Security*. https://www.dhs.gov/science-and-technology/news/2021/11/05/news-release-st-funds-interoperable-messaging-capability (November 9, 2022).

U.S. Department of Homeland Security, Federal Emergency Management Agency. 2017. *National Incident Management System*, 3rd edition. https://www.fema.gov/sites/default/files/2020-07/fema_nims_doctrine-2017.pdf (November 9, 2022).

U. S. Department of Justice, Office of Justice Programs. 2022a. *Public Safety Communications and Interoperability.* U.S. Department of Justice. NCJ 214331. https://www.ojp.gov/pdffiles1/nij/214331.pdf (November 9, 2022).

U.S. Department of Justice, Office of Justice Programs. 2022b. *Census of State and Local Law Enforcement Agencies, 2019–Statistical Tables*.

https://bjs.ojp.gov/sites/g/files/xyckuh236/files/media/document/csllea18st.pdf (November 12, 2022).

Wang, Li, Jun Zhang, Jianbin Chuan, Ruqiu Ma, and Aiguo Fei. 2020. "Edge Intelligence for Mission Cognitive Wireless Emergency Networks." *IEEE Wireless Communications* 27 (4): 103–9. doi: 10.1109/MWC.001.1900418.

Willis, James J. 2022. "'Culture Eat Strategy for Breakfast': An In-Depth Examination of Police Officer Perceptions of Body-Worn Camera Implementation and Their Relationship to Policy, Supervision, and Training." *Criminology and Public Policy* 21 (3): 713–37. doi: 10.1111/1745-9133.12591.

Willuhn, Marian. 2022. "Satellite Cyber Attack Paralyzes 11GW of German Wind Turbines." *PV Magazine*, March 1. https://www.pv-magazine.com/2022/03/01/satellite-cyber-attack-paralyzes-11gw-of-german-wind-turbines/ (November 9, 2022).

Appendix C

ANNOTATED BIBLIOGRAPHY

Akerkar, Rajendra. 2020. *Big Data in Emergency Management: Exploitation Techniques for Social and Mobile Data*. Cham, Switzerland: Springer.

Akerkar's book provides an in-depth look into how data can be useful in emergency management. Useful data can come from several sources, including first responders, traffic signals, and private and public owners of critical infrastructure. Of note is the chapter focused on the integration of social media and Emergency Management. Understanding the benefits of this relationship can assist in synchronizing Hexagon's communication efforts when identifying relevant technological solutions.

Allen, Craig and Edward Parkinson. 2021. "Communications from 9/11 to COVID-19: Lessons Learned That Have Shaped and Modernized Law Enforcement Communications." *Police Chief Online.* https://www.policechiefmagazine.org/communications-from-9-11-to-covid-19/ (July 21, 2021).

The events of 9/11 ushered in a new era of communications in law enforcement and emergency management. These changes continue today with the changes implemented during the COVID-19 pandemic response. These changes brought about the creation of FirstNet, a universal communication system that allows police, fire, EMS, and emergency managers to communicate using a dedicated broadband network system. This article outlines the lessons learned in communications that began following the 9/11 attacks and how it has changed in both emergency situations as well as everyday incident management.

Alsamhi, Saeed Hamood, Faris A. Almalki, Hatem AL-Dois, Alexey V. Shvetsov, Mohammad Samar Ansari, Ammar Hawbani, Sachin Kumar Gupta, and Brian Lee. 2021. "Multi-Drone Edge Intelligence and SAR Smart Wearable Devices for Emergency Communication." *Wireless Communications and Mobile Computing*. doi: 10.1155/2021/6710074.

Disaster management demands real-time information for providing and delivering emergency services to save people's lives. Recently, the advanced technology of the Internet of Things (IoT) enabled the collection of real-time data from different sources. Smart wearable devices (i.e., IoT devices) include sensors, actuators, and cameras, for smart environments. Thus, drones are equipped with onboard IoT devices connected to IoT devices to perform complex tasks effectively and efficiently. In case of a

disaster, drone technology is equipped with IoT devices to capture a map or high-resolution image and sense its surroundings.

Andrew, Simon A., and Christopher V. Hawkins. 2013. "Regional Cooperation and Multilateral Agreements in the Provision of Public Safety." *American Review of Public Administration* 43 (4). doi: 10.1177/0275074012447676.

Interlocal agreements are commonplace in public service. However, multilateral agreements are not as prevalent. This article examines why they are not common and where they would be appropriate.

Army Publishing Directorate. 2015. *ATP 5-0.1 Army Design Methodology*. Department of the Army. https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/atp5_0x1.pdf (July 21, 2022).

This manual outlines the use of Design Methodology in the United States Army. This method is used because the historical use of quantitative, qualitative, or mixed methods is not always ideal in solving or researching a social issue or problem. Given the complex issues that the military must contend with on a daily basis, this methodology allows for new and innovative problem-solving. Given the unique parameters of this research project, the design methodology should prove more useful in collecting and analyzing the data.

Beg, Abdurrahman, Abdul Rahman Qureshi, Tarek Sheltami, and Ansar Yasar. 2020. "UAV-Enabled Intelligent Traffic Policing and Emergency Response Handling System for the Smart City." *Personal and Ubiquitous Computing* 25 (1): 33–50. doi: 10.1007/s00779-019-01297-y.

This paper proposes the deployment of unmanned autonomous vehicles (UAV) within the smart city environment to supplement the use of current traffic policing infrastructure. The authors envision that this solution could compel drivers to reduce speed because of the potential to change the position of the UAV monitoring device continuously. Additionally, UAVs allow for real-time tracking and pursuit of violators, particularly for "flagged offenses such as a stolen vehicle or a previously issued and pending arrest warrant," and provide responders with a means to "investigate scenarios of possible accidents or causes for congestion" (35). This solution is also expected to operate largely autonomously, thereby reducing the need for large numbers of highway patrol personnel and

vehicles. Last, the authors offer that the proposed solution will "round-the-clock monitoring" and effective route prioritization.

Bexar County and City of San Antonio. 2002. *Plan for City-County Cooperation.* https://www.bexar.org/DocumentCenter/View/3662/Overarching-Agreement-Final (June 29, 2022).

In 2002, Bexar County and the City of San Antonio entered into an overarching agreement to integrate City and County services. This overarching agreement is the foundation for which these municipalities operate, coordinate, and communicate today. The overarching agreement includes general principles, strategies, and a work program to guide their effort and achieve their vision. A key element of the work program includes improved collaboration with the City, County, and the incorporated cities within the County to achieve a singular, coordinated emergency management operation. Additionally, a coordinated dispatch system for the Sheriff's Department and the City Police and Fire Departments is prioritized in the work program. More specifically, it emphasizes the need for a dispatch system with redundancy, the ability to communicate between agencies, and integration with the County's 911 network.

Bezek, Sarah, Jonathan Dyal, and Girish Bobby Kapur. 2017. *Effective Communication During Disasters: Making Use of Technology, Media, and Human Resources*. Apple Academic Press.

This book provides an in-depth look at communication challenges during and post-emergency events. The first section overviews "Communication Challenges and Best Practice Analyses." The second section focuses on the use of the internet and social media. The third section discusses the use of mobile phones and other technology. The final section provides case studies to highlight the challenges in effective communication.

Buchanan, Kerrianne, Shanee Dawkins, and Sandra Spickard Prettyman. 2021. *Voices of First Responders - Nationwide Public Safety Communication Survey Findings: Day-to-Day Technology*. National Institute of Standards and Technology: Washington, D.C. https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8400.pdf (July 22, 2022).

The Nationwide Public Safety Broadband Network (NPSBN) is being developed to provide a dedicated network for first responders' use. A

wave of new communication technologies compatible with the NPSBN is on the horizon, as major research and development efforts for these technologies are ongoing. The aim of the NIST PSCR Usability Team is to better understand the usability of communication technology for first responders by investigating the contexts in which they work, their experiences with incident response, and their problems with and needs for communication technology. To this end, NIST's PSCR Usability Team conducted an exploratory, sequential, mixed-methods study to gather insights into the experiences and needs of first responders.

Buchanan, Kerrianne, Yee-Yin Choong, Shanee Dawkins, and Sandra Spickard. Prettyman. 2021. "Communication Technology Problems and Needs of Rural First Responders." Paper presented at the 18th International Conference on Information Systems for Crisis Response and Management, Blacksburg, VA. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=931454 (July 21, 2022).

This paper explores the use and communication technology problems and needs of rural first responders. The authors conducted semi-structured interviews with 63 rural first responders across four disciplines: Communications (Comm) Center & 9-1-1 Services, Emergency Medical Services, Fire Service, and Law Enforcement. Researchers sorted interview data into problems and needs categories through qualitative data analysis. Rural first responders' most significant issues were reliable coverage/connectivity, interoperability, implementation/information technology (IT) infrastructure, and physical ergonomics. Rural first responders' greatest need for new technology was to address their current problems, but they were interested in new technology that leverages real-time technology and location tracking. This article also discusses the implications for researchers and developers of public safety communication technology.

Bullock, J., George Haddow, and Damon P. Coppola. 2015. *Introduction to Homeland Security Principles of All-Hazards Risk Management*. 5th edition. Amsterdam: Butterworth-Heinemann.

This source outlines the way that emergency response is conducted in the United States. By reviewing this source, the reader has a working idea of how all agencies interact during day-to-day operations and in times of crisis. This source also shows the operational tiers which identify where cultural and financial obstacles would lie for the interoperational

communication issues. This source can act as a road map in the emergency management realm and the parameters of this research project.

Carreras-Coch, Anna, Joan Navarro, Carles Sans, and Agustín Zaballos. 2022. "Communication Technologies in Emergency Situations" *Electronics* 11 (7): 1155. doi: 10.3390/electronics11071155.

The purpose of this paper is (1) to review emergency communications challenges, (2) to analyze existing surveys on technologies for emergency situations, (3) to conduct a more updated, extensive, and systematic review of the emergency communications technologies, and (4) to propose a heterogeneous communication architecture able to communicate between moving agents in harsh conditions. The proposed approach is conceived to link the relocating agents that constitute a Ubiquitous Sensor Network spanning a large-scale area (i.e., hundreds of square kilometers) by combining Near Vertical Incidence Skywave technologies with Drone-Based Wireless Mesh Networks.

Choong, Yee-Yin et al. 2021. "What Futuristic Technology Means for First Responders: Voices from the Field." *In Human-Computer Interaction Design and User Experience Case Studies: HCII 2021. Lecture Notes in Computer Science* 12764, eds. M. Kurosu, 271–291. doi: 10.1007/978-3-030-78468-3_19.

NIST's PSCR Usability Team conducted a multi-phase, mixed methods research project in order to provide a greater understanding of first responders, their experiences, and their communication technology problems and needs.

City of San Antonio, Committee on Emergency Preparedness. 2021. *Community Emergency Preparedness Committee Report*. San Antonio, TX: City of San Antonio. https://www.sanantonio.gov/Portals/5/files/CEP%20Report%20Final.pdf (July 22, 2022).

This report was generated by the City of San Antonio and its municipally owned utilities as a result of their inability to adequately respond, provide timely information, and quickly mobilize resources during extreme winter weather that came with the arrival of Winter Storm Uri in February 2021. The report was established to better understand what happened during the winter storm with respect to the emergency communications and service delivery effort. The report provides valuable information about the gaps in communication leading up to and during the incident, insufficient software

and communication tools available for providing real-time messages across agencies and to the public, and the lack of routine disaster scenarios, response simulations, tabletop exercises, and in-person field exercises. Some of the recommendations include: developing systems and protocols to have one coordinated messaging channel between agencies; creating a dashboard that reflects real-time outages, infrastructure failures, water pressure issues, etc., with the ability to filter by Council District; and creating an annual emergency response tabletop exercise that includes elected officials, executive leadership for the City, County, and Utilities.

U.S. Department of Justice. Federal Bureau of Investigation. 2020. *Criminal Justice Information Services Policy.* Washington, D.C.: Department of Justice. Version 5.9 06/01/2020. https://www.fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf/view (July 21, 2022).

The National Crime Information Center is a repository for computerized criminal justice records or criminal justice information (CJI). It is maintained by the Criminal Justice Information Services (CJIS) Division of the FBI in conjunction with CJIS System Agencies. The CJIS security policy governs accessing, maintaining, disseminating, and destroying criminal justice information.

Cohen, Galia. 2018. "Cultural Fragmentation as a Barrier to Interagency Collaboration: A Qualitative Examination of Texas Law Enforcement Officers' Perceptions." *American Review of Public Administration* 48 (8). doi: 10.1177/0275074017744659.

This study looks at barriers to collaboration in public safety agencies. Specifically, Cohen addresses the question, “to what extent does variation in agency type, rank segmentation, and leadership style hinder the collaborative process in American public safety agencies (Cohen 2018)?” Cohen’s study is limited to Texas law enforcement agencies. The study included 45 law enforcement officers at varying levels (local, state, and federal) and various ranks throughout the agencies. Cohen examined whether agency structure and leadership type affected collaboration.

Conradie, Peter and Sunil Choenni. 2014. "On the Barriers for Local Government Releasing Open Data." *Government Information Quarterly* 31: S10–S17. doi: 10.1016/j.giq.2014.01.003.

This paper examines the internal processes within local government that influence data release and the barriers that exist. The barriers presented include limited understanding of how data is collected and how requests

should be handled, decentralized data ownership, and employees' limited expertise and understanding of privacy regulations and laws. Additionally, the complex organizational structure of a municipality itself presents challenges since each department within the municipality deals with data in different ways. The paper also presents a fear of false conclusions being drawn from the released data or the data being misinterpreted or misconstrued by external parties. Lastly, open data is not necessarily a priority within the organization because data release is not part of the regular duties for many city employees.

Cresswell, A., S. Dawes, and T. Pardo. 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). doi: 10.1111/j.1540-6210.2009.01987_2.x.

Emergencies and routine calls exist and in between them is a tangled middle ground of information that needs sorted out and prioritized.

Crowther. K. 2014. "Understanding and Overcoming Information Sharing Failures." *Homeland Security and Emergency Management* 11 (1): 131–54. doi: 10.1515/jhsem-2013-0055.

Despite improved data interoperability, common digital architectures, and massive connected digital networks, the same failures of information sharing occur again and again

Cybersecurity and Infrastructure Security Agency. 2021. *Approach for Developing an Interoperable Information Sharing Framework*, Version 1.7.
https://www.cisa.gov/sites/default/files/publications/21_0929_cisa_approachfordeveloping_isf_v3_508.pdf (June 20, 2022).

To support the development of a framework for information sharing, the Information Sharing Framework Task Force was established and tasked with developing an information sharing framework to expand "beyond a single organization focus" (12). This document acknowledges the importance of "near real-time situational awareness" that can only be facilitated through successful information sharing, and it outlines a high-level information sharing framework to be utilized to share information within and across agencies during emergencies (23). This publication also recognizes the shortcomings of many industry-developed solutions to this issue, highlighting that "[t]he solutions [developed by industry] often attempt to position their product as the predominant central technology

without due consideration to the long-term impact to the end users' mission environments and their ongoing interoperability requirements" (2).

Cybersecurity and Infrastructure Security Agency. 2021. *Interoperability Continuum: A Tool for Improving Emergency Response Communications and Interoperability.* https://www.hsdl.org/?view&did=856580 (July 22, 2022).

This literature addresses the need for emergency responders—public safety and, as necessary public services and Non-Governmental Organizations—to share vital data and voice information across disciplines and jurisdictions to respond to day-to-day incidents and large-scale emergencies successfully. Developed with practitioner input from the Cybersecurity and Infrastructure Security Agency's SAFECOM program, the SAFECOM Interoperability Continuum is designed to assist emergency response agencies and policymakers in planning and implementing interoperability solutions for data and voice communications. This tool identifies five critical success elements that must be addressed to achieve a sophisticated interoperability solution: governance, standard operating procedures/standard operating guidelines, and field operations guides, technology, training and exercises, and usage of interoperable communications (CISA 2021).

Dawkins, Shanee, Kristen Greene, Michelle Steves, Mary Theofanos, Yee-Yin Choong, Susanne Furman, and Sandra Spickard Prettyman. 2018. "Public Safety Communication User Needs: Voices of First Responders." *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 62 (1): 92–6. doi: 10.1177/1541931218621021.

This study provided user input into what 133 firefighters, law enforcement operators, EMS workers, and communications personnel sought in reference to communications technology. It provides unique input into what they sought, including effectiveness, efficiency, and satisfaction.

Di Talia, V. and G. Antonioni. 2022. "The Integration of Social Media Data in Emergency Management: An Innovative Decision Support System." *Chemical Engineering Transactions* 91: 577–82. doi: 10.3303/CET2291097.

The upsurge of social media platforms has opened the prospect of integrating the information provided by citizens through these channels into the traditional emergency management process. This paper presents

the Civil Protection Emergency System model designed for the Italo-Croatian decision support system developed in the Interreg project E-CITIJENS. Seismic, flood, and forest fire are the risk typologies addressed. The model specifies the key steps that allow the system, a semantically enriched web-enabled platform, to identify and analyze significant social media posts that can provide Civil Protection authorities with additional real-time data regarding potential or ongoing emergencies in a designated geographical area.

Djahel, S., N. Smith, S. Wang, and J. Murphy. 2015. "Reducing Emergency Services Response Time in Smart Cities: An Advanced Adaptive and Fuzzy Approach." Paper presented at the 2015 IEEE First International Smart Cities Conference, Guadalajara, Mexico. doi:10.1109/isc2.2015.7366151.

This study explores the role that Information and Communication Technologies and the Internet of Things can play in Traffic Management Systems to reduce emergency response times. Delays in responses due to congestion, lane closures, construction, and more. Some of the solutions explored include real-time adjustments to traffic light changes, speed limit changes, lane clearances, utilizing reserved lanes, and rerouting travelers or emergency vehicles. The study discussed the loss of life and loss of property due to accidents, fires, medical events, and terrorist attacks.

Dufty, N. 2020. *Disaster Education, Communication and Engagement*. Newark: John Wiley & Sons, Incorporated.

Communication networks among responders are critical to effective coordination and information transfer across emergency agencies and other organizations in active disasters. As the complexity of the event increases, information about the disaster, its effects, associated response needs, jurisdictional responsibilities, available
resources, and engaged organizations and personnel are distributed among an array
of responders (Militello et al. 2007). As stated by Kapucu (2006), "if responders are not in contact with each other…and if information (whether a report or instruction) does not flow properly, it is hard to envision a successful disaster response" (218). Research has suggested that prior plans do not appear to be good predictors of actual communication interaction between agencies (Choi and Brower 2006). On the other hand, embedding communication relations and institutions apparently improves the efficacy of disaster network interactions (Nowell and Steelman 2015).

Egli, Virginia L. 2011. *Impact of Organizational Culture on Information Sharing.* https://apps.dtic.mil/sti/pdfs/ADA546535.pdf (July 22, 2022).

This report analyzes how the organizational culture of the Federal Bureau of Investigation and the Department of Homeland Security impact collaboration and the sharing of information.

El Paso County 911 District. 2020. *El Paso County 911 District: Strategic Document 2020*. https://www.elpaso911.org/strategic-plan (June 15, 2022).

This strategic plan outlines the mission, vision, values, and strategic goals for the El Paso County 911 District. Of particular note is the 911 district's emphasis on people-focused communication and its goal to provide "innovative, reliable and secure technology" (El Paso County 911 District 2020, 4).

Federal Bureau of Investigation. 2022. *Law Enforcement Enterprise Portal (LEEP)*. https://www.fbi.gov/services/cjis/leep (July 21, 2022).

The Law Enforcement Enterprise Portal (LEEP) is a secure information-sharing platform for all law enforcement agencies, criminal justice entities, and the intelligence community. The website discusses information sharing during law enforcement incidents such as active shooters, abductions, natural disasters, terrorism, and others. This information could be explored for adaptation to day-to-day operations throughout public safety.

Federal Emergency Management Agency. 2017. *National Incident Management System.* https://www.fema.gov/sites/default/files/2020-07/fema_nims_doctrine-2017.pdf (July 22, 2022).

The National Incident Management System guides all levels of government, nongovernmental organizations (NGO), and the private sector to work together to prevent, protect against, mitigate, respond to, and recover from incidents (FEMA 2017, 1). NIMS represents doctrine relevant to the need for solutions relating to collaborative incident management. NIMS provides references to laws applicable to the Hexigon project, including the Homeland Security Act, PETS Act, PKEMRA, Robert T. Stafford Disaster Relief and Emergency Assistance Act, Sandy Recovery Improvement Act of 2013.

Felgueiras, Sónia M. A. Morgado, and Lúcia G. Pais. 2019. ""Interoperability: Diagnosing A Novel Assessment Model."" *European Law Enforcement Research Bulletin*: 255–60. https://www.researchgate.net/profile/Sergio-Felgueiras/publication/358592279_Interoperability_Diagnosing_a_novel_assessment_model/links/620a8b96cf7c2349ca137b2c/Interoperability-Diagnosing-a-novel-assessment-model.pdf (July 22, 2022).

The promotion of better cooperation amongst first responders should be based on a multilevel interoperability model to solve potential and real coordination problems during rescue operations. It is clear that an interoperable system will respond in a better and integrated way to save lives. Preparedness is the key element. The authors assert, "there are some traditional barriers for the interoperability implementation, such as technological, cultural, organizational and individual." The presentation of a general reflection about the critical aspects of interoperability governance (plan, decision-making, and training) tackles key issues such as innovation, harmonization of safety and security culture, articulation of top-down and bottom-up approaches, operational procedures, technological support, and general training.

Finley, Melisa, Brooke Durkop, Poonam Wiles, James Carvell, and Gerald Ullman. 2001. *Practices, Technologies, and Usage of Incident Management and Traveler Information Exchange and Sharing in Texas.* https://static.tti.tamu.edu/tti.tamu.edu/documents/4951-1.pdf (June 15, 2022).

Addresses day-to-day issues relevant to our problem statement and includes a technology-related solution. "Agencies such as city and county traffic departments, police, fire departments, transit, information service providers, and media continuously use the information provided by TxDOT to improve their daily operations" (Finley et al. 2001)

Gallagher, J. C. 2018. *Federal Grants and Loans for State and Local Emergency Communications Projects: Frequently Asked Questions*. Congressional Research Service. https://crsreports.congress.gov/product/pdf/R/R45213/5 (July 21, 2022).

This source shows how all agencies can receive funding for their communications needs. Understanding this information will allow the reader to see the failings of financial access to necessary funds. This source also identifies the timeframes, windows, and hurdles required for

the obtainment of funds. This source shows why it is difficult to overcome financial obstacles in the emergency management realm.

Gallagher, J. C. 2018. *The First Responder Network (FirstNet) and Next-Generation Communications for Public Safety: Issues for Congress. Congressional Research Service.* https://crsreports.congress.gov/product/pdf/R/R45179 (July 21, 2022).

This source covers the Congress-driven nationwide communication system known as FirstNet. This system will allow all agencies from the local, state, and federal level to communicate during day-to-day operations and during a crisis. This system was built entirely with the emergency management realm in mind to streamline their communications. This source highlights the capabilities and functions of the FirstNet system.

Gallagher, J. C. 2019. E*mergency Communications: Homeland Security Issues in the 116th Congress*. Congressional Research Service. https://crsreports.congress.gov/product/pdf/IN/IN11028 (July 21, 2022).

This source was significant because it highlighted the still lingering issues of communication interoperability. These issues were identified as the Congress-driven system was being established. This source still identifies some other issues that acted as obstacles and the need to focus on solutions. The need for communication interoperability is a concern for Congress, and the need for a solution to this issue remains prevalent.

Gamage, Pandula. 2016. "New Development: Leveraging 'Big Data' Analytics in The Public Sector." *Public Money and Management* 36 (5): 385–90. doi: 10.1080/09540962.2016.1194087.

In this paper, the author highlights government entities that have embraced big data applications to improve operations, such as increasing public safety, tightening financial oversight, detecting fraud, and delivering services effectively. However, much of the paper is focused on the barriers that exist to investing in such applications, including privacy, access, and quality of data. Data compatibility and quality are most challenging, given that effectively analyzing data for decision-making requires the data to be accurate. Therefore, the author argues that the benefits of big data will only be realized if policymakers invest in research, create incentives for private and public sector entities to share data, and create employee training programs to develop the appropriate skills.

Goldstein, M. 2017. *Emergency Communications: Overlap and Views on the Effectiveness of Organizations Promoting the Interoperability of Equipment.* Gao.Gov. https://www.gao.gov/assets/gao-18-173r.pdf (June 27, 2022).

> Communication systems utilized by local, state, and federal agencies for various emergencies lacked interoperability that was not highlighted until events like Hurricane Katrina and September 11th. Even as recently as the Navy Yard attacks in 2013, issues remained. This research by GAO explored federally supported agencies that focus on interoperability related to communications. The report focused on SAFECOM, ECPC, NCSWIC, and PSAC. Each group has a specific role and complementary functions, ideally not duplicative. The study found that membership in these groups had positive effects.

Gordon, J. IV, B. Wallace, D. Tremblay, and J. Hollywood. 2012. *Keeping Law Enforcement Connected: Information Technology Needs from State and Local Agencies*. Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/technical_reports/TR1165.html (July 22, 2022).

> In contrast, few agencies reported significant awareness of the activities of the National Law Enforcement and Corrections Technology Center, whose primary mission is to assist with addressing the technology needs and challenges of state, local, tribal, and federal law enforcement outfits, as well as those of corrections and criminal justice agencies.

Griffin, T., D. Miller, J. Williams, and J. Woolredge. 2014. "Does AMBER Alert 'save lives'? An empirical analysis and critical implications." *Journal of Crime and Justice*. doi: 10.1080/0735648X.2014.1003577

> We reached conclusions consistent with the scant available prior research on AMBER Alert: although over 25% of the Alerts facilitated the recovery of abducted child(ren) and are thus arguably "successful" by that standard alone, there was little evidence AMBER Alerts "save lives." In fact, AMBER Alert success cases are in almost every measurable way identical to AMBER Alert cases in which the child(ren) were returned unharmed, but the Alert had no direct role in that outcome.

Herovic, Emina, Timothy L. Sellnow, Deanna D. Sellnow. 2020. "Challenges and Opportunities for Pre-Crisis Emergency Risk Communication: Lessons Learned from the Earthquake Community." *Journal of Risk Research* 23 (3): 349-364. doi: 10.1080/13669877.2019.1569097.

This journal submission evaluates crisis emergency communications. It primarily assesses the value of crisis emergency communications through earthquake emergency management responses. The researchers utilize the "Crisis Emergency Risk Communication (CERC) Model developed by US Centers for Disease Control and Prevention (CDC)." This is a model that can be adapted and used for any crisis event as it was designed to be utilized in all stages of a crisis with a heavy emphasis on the pre-crisis stage.

Hersman, R., R. Younis, B. Farabaugh, A. Reddie, and B. Goldblum. 2020. *Understanding Situational Awareness Technologies and the Emerging Situational Awareness Ecosystem.* Cloudinary.com. https://res.cloudinary.com/csisideaslab/image/upload/v1586648315/on-the-radar/OnTheRadar_Chapter_2_a3kirt.pdf (July 22, 2022).

This study was done primarily through the lens of military operations and national security but discussed the growing use of technology to improve situational awareness in real-time. Technological advances have brought capabilities and benefits that were previously not available, inaccessible, or highly costly. As with many advancements, the military can provide critical experiences and funding that can benefit the public good.

Hocevar, Susan, Erik Jansen, and Gail Thomas. 2011. "Inter-Organizational Collaboration: Addressing the Challenge." *Homeland Security Affairs* 7, The 9/11 Essays. https://calhoun.nps.edu/handle/10945/37884 (July 22, 2022).

This report looks at organization theory in regards to collaboration. It addresses that most research is about the need for collaboration but does not address how to collaborate. The report looks at how collaboration occurs.

Hogan, Greg and Stephanie Foster. 2022. The Next-Generation Incident Command System (NICS). *In Enhancing Capabilities for Crisis Management and Disaster Response*, eds. F. Hostiuc and E.K. Turmus: 23–32. Dordrecht: Springer Netherlands. doi: 10.1007/978-94-024-2142-2_3.

When disaster strikes, multiple agencies and jurisdictions take the call and respond. Organizing, coordinating, and commanding large-scale events present significant challenges to participating responders. To overcome these challenges, effective collaboration, shared situational awareness, and decision support requires the timely distribution of information across disparate systems and platforms. With guidance from these operational partners, MIT Lincoln Laboratory designed and implemented a prototype

system that enabled shared situational awareness and collaboration during response operations. The Next-generation Incident Command System (NICS) architecture is based on a net-centric and service-oriented paradigm and combines sensors, communications and visualization, and collaboration technologies with all components being linked in (near) real-time.

Hollywood, John and Zev Winkelman. 2015. *Improving Information-Sharing Across Law Enforcement: Why Can't We Know?* RAND Corporation. https://www.ojp.gov/pdffiles1/nij/grants/249187.pdf (June 19, 2022).

There are also increasing demands to share information with regional, state, and federal repositories of criminal justice information. While substantial progress has been made in improving the information-sharing ability and affordability of key law enforcement systems, many barriers remain.

Homeland Security Act of 2002, Pub. L. No. 107–296, 116 Stat. 2135 (2002).

This source shows the first attempt on a federal level to have communication interoperability among first responders. This act tried to overcome the communication deficiencies, which made the response to the terrorist attacks on September 11, 2001, such a quagmire. Even though this act stated that it wanted to achieve communication interoperability, it did not lay out a framework. Trying to implement the directives in this act showed the obstacles that stood in the communication interoperability at all levels.

Hu, Qian and Naim Kapucu. 2016. "Information Communication Technology Utilization for Effective Emergency Management Networks." *Public Management Review* 18 (3): 323–48. doi: 10.1080/14719037.2014.969762.

This article studies how information communication technologies are perceived by external organizations. "Furthermore, it investigates whether the centrality of organizations in emergency management networks relates to ICT utilization." The authors make a case for why communication challenges exist between organizations. After identifying some of the challenges, they provide a case as to the benefits of overcoming these roadblocks and achieving organizational, and mission success.

International Association of Law Enforcement Directors. 2021. *Data Driven Approaches to Crime and Traffic Safety.*

https://www.iadlest.org/Portals/0/Files/Documents/DDACTS/Docs/DDACTS_20_OpGuidelines_06_06_21.pdf (July 22, 2022).

Data Driven Approaches to Crime and Traffic Safety advocates for the collection and analysis of data relating to both traffic incidents such as collisions, officer activity, and calls for service and utilizes this data for better deployment of resources.

Jones, J. C. 1992. *Design Methods*. Germany: Wiley.

This source covers design methodology in the civilian world. The authors also identified that the traditional methods to gather data and solve problems did not always align or work for the issue at hand. This source shows different ways to gather data and conduct analysis for problem-solving issues outside of normal research parameters. This source should work for the research project given its outside-the-box thinking concepts.

Kadadi, A., R. Agrawal, C. Nyamful, and R. Atiq. 2014. "Challenges of Data Integration and Interoperability in Big Data." Paper presented at 2014 IEEE International Conference on Big Data, Washington, DC. doi: 10.1109/BigData.2014.7004486.

This study discusses existing infrastructure limitations and the complexities of collecting, storing, and synthesizing massive amounts of data. Additionally, the report explores the issues of combining different data types compared to heterogeneous data types. Data interoperability is only achieved through successful integration, a challenge of its own. An example the group used was noting a new food product borne disease due to animal, weather, temperature, and cattle food, among others. Obtaining real-time data from these various factors is manageable so long as the data is seamlessly integrated.

Kapucu, Naim. 2006. "Interagency Communication Networks During Emergencies." *The American Review of Public Administration* 36 (2): 207–25. doi: 10.1177/0275074005280605.

The article analyzes individual boundary-spanner networks in emergency response operations. Boundary-spanner networks refer to individuals within a system who have, or adopt, the role of linking the organization's internal networks with external sources of information. To foster inter-organizational communication and the trust that enables accelerating inter-organizational network coordination in emergency management response operations, the author suggests that individual public emergency

managers, nonprofit managers, and business sector managers should provide before-the-fact incentives and information to promote inter-organizational networks. The article also emphasizes how dynamic networks are underpinned by reciprocity and mutual trust, which allow members to share information, risks, and opportunities with greater ease. These links are vital because they not only connect organizations to one another but also give organizations access to the larger world outside their circle through a chain of affiliations. Willingness to share, proper training, trust, education, human relations, and willingness to create public value, experience, common interest, and communication skills are considered important skills, values, and attitudes that managers and staff must have to be successful in building communication networks in emergencies.

Lachacz, Tomasz and Przemyslaw Wrzosek. 2021. "Faster Technologies to Ensure the Safety of First Responders." Paper presented at SafeGreece 8th International Conference on Civil Protection & New Technologies, Online. https://www.faster-project.eu/wp-content/uploads/2022/01/SAFE-GREECE-WSPOL.pdf (July 22, 2022).

Complex emergency operations require the use of data, communications, unit positioning, mapping and scene imaging technologies. The aim of the paper is to present a set of modern technologies and tools developed by an international consortium within the FASTER project - First responders Advanced Technologies for Safe and EfficienT Emergency Response. The developed solutions are addressed to first responders who undertake high-risk rescue operations in hazardous environments. The use of FASTER technologies and tools (e.g., smart textiles, AR tools, drones) in emergency situations is expected to provide greater safety for responders and increase the effectiveness of actions taken.

Lea, R. 2017. *Smart Cities: An Overview of the Technology Trends Driving Smart Cities.* https://www.ieee.org/content/dam/ieee-org/ieee/web/org/about/corporate/ieee-industry-advisory-board/ieee-smart-cities-trend-paper-2017.pdf (July 22, 2022).

Advancements in technology are at a point where we can integrate things that we never thought possible. Information and communication technologies can be used to improve the quality of life by enhancing the abilities of transportation, energy, water infrastructure, and public safety. This paper discusses the whole of government approach and public-private partnerships.

Littlefield, R., K. Rowan, and S. Veil. 2009. "Dissemination as Success: Local Emergency Communication Practices." *Public Relations Review* 35 (4): 449–51. doi: 10.1016/j.pubrev.2009.06.004.

This study demonstrates that success is determined by the number of people the message reaches, rather than if people are persuaded to do what the message requested. The International Association of Emergency Managers (IAEM) recognizes "outstanding public awareness programs or public education products related to emergency management, homeland security, and/or disaster preparedness."

Liu, Brooke Fisher, Anita Atwell Seate, Irina Iles, and Emina Herovic. 2020. "Tornado Warning: Understanding the National Weather Service's Communication Strategies." *Public Relations Review* 46 (2). doi: 10.1016/j.pubrev.2019.101879.

The National Weather Service field offices do not employ public information officers. Instead, forecasters predict the weather, craft messages, and build relationships with the public. This study called for public relations research that examines messages, including how crisis communication can help the public cope. The authors argue that all organizations need public relations, even if they do not employ formal public relations personnel.

Louisiana Governor's Office of Homeland Security and Emergency Preparedness. 2022. *Statewide Interoperability Executive Subcommittee*. https://gohsep.la.gov/ABOUT/UNIFIED-COMMAND-GROUP/Interoperability-Subcommittee/SIEC (July 6, 2022).

The State of Louisiana has many incidents that could either bolster or expose the inadequacies of emergency communications. The state has enacted an Office of Homeland Security and Emergency Preparedness under the Governor's Office. Inside this office is the Statewide Interoperability Executive Subcommittee (SIEC). This group is focused on identifying ways that emergency services, including police, fire, EMS, federal agencies, and the military, can better respond and communicate in the planning, aftermath, and recovery of disasters within Louisiana.

M, Sathiyakeerthi. 2021. "Eye in the 5G Sky for Smart Cities." *IEEE Smart Cities.* https://smartcities.ieee.org/newsletter/september-2021/eye-in-the-5g-sky-for-smart-cities (July 14, 2022).

This article highlights the transforming capabilities of drones, particularly in smart cities. The author highlights a number of police departments abroad that use drones for tracking criminals, as well as drones used in gathering geographical data and other uses. The article offers a visual representation of the workings of a disaster management drone working in a 5G network in a smart city and describes the steps and features of its use. This includes real-time streaming of areas, the use of a complex base station to manage radio communication with multiple devices simultaneously, and the use of video analytics. This information is then provided to the Integrated Command Control Center, which directs the drone further to allow officials to act efficiently. This mapping is useful in understanding the ways that drones can enable communication. Additionally, the article highlights key performance indicators necessary for this type of drone application.

Manandhar, Rejina and Laura K. Siebeneck. 2018. “Return-Entry Risk Communication Challenges: Experiences of Local Emergency Management Organizations following Superstorm Sandy.” *International Journal of Mass Emergencies and Disasters* 36 (2): 120–48. http://ijmed.org/articles/743/ (July 22, 2022).

Although this article is a review of a “black sky” event, it offers insight into what communications should be practiced during “blue sky” events to help enable success during emergency situations. Socio-demographic characteristics are examined to analyze challenges to communication in “vulnerable populations and poor and ethnic minorities” and also “Spanish-speaking populations.” Focusing on these particular groups prior to emergency events can identify challenges for first responders to effectively respond to events in these communities. Communicating with electric utilities was also identified as a shortcoming during hurricane Sandy. Developing a direct source or liaison (LNO) is a critical need in coordinating recovery efforts.

Manoj, B.S. and Alexandra Hubenko Baker. 2007. "Communication Challenges in Emergency Response." *Communications of the ACM* 50 (30): 51–3. doi: 10.1145/1226736.1226765.

This article examines communication challenges in the form of technological, sociological, and operational barriers. Inter-personal and inter-agency cultural differences can impact communication, which can exacerbate the many challenges already present at an emergency event. Technological advancements allow communications to be established and

maintained in austere environments, yet sociological differences, coupled with organizational differences, can lead to misunderstandings and missed opportunities to bring resolution to the incident. Human activity and communication behavior models highlight the study of these issues.

Matheus, Ricardo, Marijn Janssen, and Devender Maheshwari. 2020. "Data Science Empowering the Public: Data-Driven Dashboards for Transparent and Accountable Decision-Making in Smart Cities." *Government Information Quarterly* 37 (3). doi: 10.1016/j.giq.2018.01.006.

In this paper, the authors present two case studies on the benefits, risks, and principles of designing dashboards in the public sector. One of the examples presents a dashboard that shows, in real-time, 24 hours per day, seven days per week, where traffic jams and accidents are in the city. The case demonstrated how dashboards help improve operational decision-making and reduce traffic problems. The authors present "information asymmetry," which is the situation where one party has more information than another party. By sharing data, dashboards can help to reduce information asymmetry by providing more insight into a certain situation. However, the benefits can only be gained if dashboards are properly designed, and the use of dashboards may involve many risks and challenges. One of the main risks is the misunderstanding of information, which could lead to incorrect conclusions about the data. Data is often context-specific, so interpretation will likely be wrong without in-depth knowledge of the context in which the data is collected.

Mayer-Schönberger, V. 2002. "Emergency Communications: The Quest for Interoperability in the United States and Europe." BCSIA Discussion Paper 2002-7, ESDP Discussion Paper ESDP-2002-03, John F. Kennedy School of Government. https://www.belfercenter.org/sites/default/files/legacy/files/emergency_communications_-_the_quest_for_interoperability_in_the_united_states_and_europe.pdf (June 19, 2022).

If anything, first responders, some of whom had taken part in Federal Emergency Management Agency (FEMA) training, were quite willing to work with each other. The real challenge was simpler—and much more serious. Responders from the various agencies had no communications system that would permit them to communicate with each other.

McNeely, Connie L. and Jong-on Hahm. 2014. "The Big (Data) Bang: Policy, Prospects, and Challenges." *Review of Policy Research* 31 (4): 304–10. doi: 10.1111/ropr.12082.

The authors examine the cultural, organizational, and technological capacities of the public sector and its primary concerns regarding big data applications. The authors present various challenges, including the collection, management, validation, integrity, and security of big data sets. Additionally, the authors present the costs and benefits of using big data in decision-making and analysis, as well as the problems of privacy, security, and ethics.

Mitchell, Robert L. 2013. "It's Criminal: Why Data Sharing Lags Among Law Enforcement Agencies." *Computerworld*, October 24. https://www.computerworld.com/article/2486359/it-s-criminal--why-data-sharing-lags-among-law-enforcement-agencies.html (Jul 18, 2022).

This article examines the FBI NDEX system and some of the barriers to its adoption and utilization by agencies. Although many of the barriers outlined are technological or financial, it does also address some cultural barriers.

Moloney, P. F. 2022. *The Federal Communications Commission: Structure, Operations, and Budget*. Congressional Research Service. https://crsreports.congress.gov/product/pdf/R/R45699 (July 22, 2022).

This source shows how the Federal Communication Commission (FCC) is structured and operates. This source also shows which element is responsible for the emergency response guidelines and regulations. This source will give the reader insight into any policy or technological issues which would act as roadblocks to communication interoperability. This source also shows how the emergency management communications realm is monitored for day-to-day operations and crises.

Moninger, W. R., R. Mamrosh, and P. Pauley. 2003. *Automated Meteorological Reports from Commercial Aircraft*. Noaa.Gov. https://amdar.noaa.gov/docs/bams/ (July 22, 2022).

This study was sent from our client, Mr. Fisher. Given that it piqued his interest, it may be relevant for our group to ensure a common operating picture of the project. The study is in reference to the NOAA and NWS receiving real-time data from commercial airline jets. Commercial air travel has become routine and so has their work with the Numerical

Weather Prediction models. This data is now available to government weather forecasters and researchers on a shared website.

Motorola, Inc. 2008. *Interoperability Planning for Public Safety*. http://uclapsns.weebly.com /uploads/6/7/4/8/6748113/interoperability_planning_for_public_safety_joint_emergency_comms_wp_031811a.pdf (July 22, 2022).

Motorola Solutions put out a white paper in 2008 that focused on interoperability planning for public safety agencies. This paper focuses on the communication and technology aspects of interoperability. While it is geared towards Motorola products, there is information about the steps to creating and implementing the interoperability plan. It also discusses some of the funding options for public safety agencies.

National Commission on Terrorist Attacks. 2004. T*he 9/11 Commission Report (Authorized Edition)*. New York: W.W. Norton.

This source identifies issues with communication interoperability among first responders. The authors highlight what went wrong with 9/11 and offer suggestions to fix them for the future. These suggestions were the groundwork for future Congressional Acts and Directives. This source was probably the first widespread publication highlighting the communication interoperability issues in the emergency management realm.

National Institute of Standards and Technology. 2022. *Digital Dispatch*. Public Safety Communications Research: Washington, D.C. https://www.nist.gov/system/files/documents/2022/04/01/PSCR%20Digital%20Dispatch%202022%20Q1.pdf (July 22, 2022).

The Public Safety Communications Research (PSCR) Digital Dispatch is a curated list of communications technology tools for public safety and the research community to interact with right now. PSCR also intends for the Digital Dispatch to facilitate partnerships and/or collaboration between stakeholders and the researchers behind the resources. The tools listed in this document are publicly available at no cost to use or reference and have been developed by research and development (R&D), both internal and external to PSCR. While this document serves as a shortcut to a handful of downloadable, actionable resources that are available for public safety to use Right now.

National Public Safety Telecommunications Council. 2019. *Public Safety Internet of Things (IoT) Use Case Report and Assessment Attributes*. https://www.npstc.org/IoT.jsp (June 20, 2022).

This report reviews a number of public safety internet of Things (IoT) cases, including non "high risk" traffic stops and generic use cases. These case studies allow for a better understanding of the needs of the public safety sectors, particularly with regard to IoT devices and technologies. Each study explores issues of ownership of the IoT solution, the number of users and devices, interoperability, overall benefit, and challenges created by the use of IoT solutions.

Nguyen, Phuoc Dai Huu and Dinh Dung Nguyen. 2021. "Drone Application in Smart Cities: The General Overview of Security Vulnerabilities and Countermeasures for Data Communication." In Development and Future of Internet of Drones (IoD): *Insights, Trends and Road Ahead.* doi: 10.1007/978-3-030-63339-4_7.

This text explores the cybersecurity vulnerabilities of the use of drones in smart cities. While the authors recognize the increasing use and demand for use of drones, particularly in smart cities, they also highlight the vulnerabilities created by sensors, communication links, and imaging. Several countermeasures are discussed in this text, including detection and defense methods, and the authors provide recommendations to improve the security of drone use in this context.

Nicolai Pogrebnyakov and Edgar Maldonado. 2018. "Didn't Roger That: Social Media Message Complexity and Situational Awareness of Emergency Responders." *International Journal of Information Management* 40: 166–74 doi: 10.1016/j.ijinfomgt.2018.02.004.

This is relevant literature regarding the interest and use of social media in emergency response. The authors assert, "social media have been acknowledged to play a role at different stages of emergency response, from disaster response to emergency preparedness, and in emergencies of different scale, from large-scale disasters such as earthquakes to smaller-scale emergency events, e.g. wildfires. In turn, the public increasingly expects emergency responders to communicate through social media."

Ockershausen, Joseph. 2008. *Special Report: The After-Action Critique: Training Through Lessons Learned.* Federal Emergency Management Agency.

https://www.usfa.fema.gov/downloads/pdf/publications/tr_159.pdf (June 23, 2022).

Office of the Director of National Intelligence. 2022. *Law Enforcement Information Sharing*. Dni.Gov. https://www.dni.gov/index.php/who-we-are/organizations/ise/ise-archive/ise-additional-resources/2142-law-enforcement-information-sharing (July 4, 2022).

A common, although not universal, implementation approach features distributed sharing methods, which allow each organization to retain its own information and, at the same time, make it available for others to search and retrieve. Since this information may be maintained in different formats by each organization, the Law Enforcement Information Sharing Program Exchange Specification (LEXS)—a subset of the National Information Exchange Model (NIEM)—was developed to translate information shared among different law enforcement systems into a common format, enabling participants on one system to receive and use information from multiple sources.

Painter, W. L., S.A. Lister, M. E. DeVine, D. Morgan, B. Elias, P. W. Parfomak, K. Finklea et al. 2019. *Selected Homeland Security Issues in the 116th Congress*. Congressional Research Servic*e.* https://crsreports.congress.gov/product/pdf/R/R45701 (July 21, 2022).

This source shows that Congress was still dealing with the communication interoperability issues in 2019. This source sheds light on the issues that were affecting the emergency management realm after the passing of the acts following 9/11. This source shows the effort and progress of the FirstNet system as it was being established. This source shows what attempts to fix communication interoperability and what was not successful between congressional sessions.

Pijpers, G. 2010. *Information Overload: A System for Better Managing Everyday Data*. Hoboken, New Jersey: John Wiley & Sons, Inc.

Many words express the idea of information: Consider data, knowledge, being, writing, sign, and symbol, to name just a few. But objects such as a name, a song, a picture, or an idea also contain a shared quality called information. Some information is considered more valuable than other information, typically because a person puts a higher value on it.

Police Executive Research Forum. 2017. "The Revolution in Emergency Communications." *Critical Issues in Policing*, November.

https://www.policeforum.org/assets/EmergencyCommunications.pdf (July 22, 2022).

Emergency communications are undergoing dramatic changes due to technology and other challenges. Technological advances include NexGen911, First Net, and updates to radio systems.

Reese, S. 2006. *State and Local Homeland Security: Unresolved Issues for the 109th Congress*. Congressional Research Service. https://crsreports.congress.gov/product/pdf/RL/RL32941/6 (July 21, 2022).

This source shows the progress and failings that occurred shortly after the passage of the Homeland Security Act. This source shows how Congress dealt with unknown or unforeseen complications to get communication interoperability at all levels of first responders. This source shows how things were being accomplished and what was working and what was not for first responders. This source also shows the first portion of progress on the congressionally directed FirstNet system for all levels of first responders across the nation.

Rosa, Carla, C. I. Gomez, C. Lumbreras, F. Nobre, and S. Walsh. 2021. *Data Analytics in Public Safety*. European Emergency Number Association. https://eena.org/knowledge-hub/documents/data-analytics-in-public-safety/ (July 21, 2022).

This piece of literature discusses data analytics in public safety in Europe. The piece discusses existing programs of use and the ability to forecast emergencies, plan accordingly, and respond as needed utilizing vast data sets. It includes examples from the London Fire Brigade. This agency employs a team of data professionals who have systems in place, analyze data, collaborate with stakeholders, and publish their work.

Saafi, Salwa, Jiri Hosek, and Aneta Kolackova. 2021. "Enabling Next-Generation Public Safety Operations with Mission-Critical Networks and Wearable Applications." *Sensors* (Basel) 21 (17): 5790. doi: 10.3390/s21175790.

Public safety agencies have been working on the modernization of their communication networks and the enhancement of their mission-critical capabilities with novel technologies and applications. In this paper, [the authors] provide an overview of cellular technologies ratified by the 3rd Generation Partnership Project to enable next-generation public safety

networks. On top of using wireless communication technologies, emergency first responders need to be equipped with advanced devices to develop situational awareness. Therefore, [the authors] introduce the concept of the Internet of Life-Saving Things and focus on the role of wearable devices—more precisely, cellular-enabled wearables, in creating new solutions for enhanced public safety operations.

SAFECOM. 2006. *Enhancing Communications and Interoperability: Perspectives and Key Considerations for Improving Local and State Coordination*. Dem.Nv.Gov. https://dem.nv.gov/uploadedFiles/demnvgov/content/NCSC/LocalAndStateAlignment.pdf (July 22, 2022).

This report explores a Regional Communications Interoperability Pilot program evaluating local and state coordination. The National Task Force on Interoperability guided this program evaluation to identify areas that emergency agencies need to focus on for improved interoperability and communication. The report identified five areas of focus that hinder interoperability that include incompatible and aging equipment, fragmented budget cycles or inconsistent funding, fragmented planning and coordination, limited radio spectrum, and lack of equipment standardization.

Davis, Julie, and William Terrill. 2010. "Interagency Collaboration: An Administrative and Operational Assessment of the Metro-LEC Approach." Policing: An International Journal of Police Strategies & Management 33 (3): 506–30. doi: 10.1108/13639511011066881.

Fragmentation in policing contributes to issues in fragmentation. There are multiple types of collaboration in law enforcement. Common types include task forces, law enforcement councils, and partnerships.

Schroeder, Jill M., David O. Manz, Jodi P. Amaya, Andrea H. McMakin, and Ryan M. Bays. 2018. "Understanding past, current and future communication and situational awareness technologies for first responders." https://dl.acm.org/doi/epdf/10.1145/3212687.3212861 (June 30, 2022).

This study builds a foundation for improving research for first responder communication and situational awareness technology in the future. In an online survey, we elicited the opinions of 250 U.S. first responders about the effectiveness, security, and reliability of past, current, and future Internet of Things technology. The most desired features respondents

identified were connectivity, reliability, interoperability, and affordability. The top barriers to technology adoption and use included restricted budgets/costs, interoperability, insufficient training resources, and insufficient interagency collaboration and communication. First responders in all job types indicated that technology has made first responder equipment more useful, and technology that supports situational awareness is particularly valued.

Segal, E. 2022. "Public Safety Personnel Face Challenges Responding to Crisis Situations: Report." *Forbes*, January 18. https://www.forbes.com/sites/edwardsegal/2022/01/18/public-safety-personnel-face-challenges-responding-to-crisis-situations-report/ (July 22, 2022).

This article discusses some of the challenges first responders faced during the pandemic with information sharing, especially real-time data. One of the primary reasons we are looking to address real-time data sharing during normal operations is to enhance efficiency, functionality, and safety during active incidents. This article addresses these concerns.

Severson, K. 2019. "Interoperability in Incident Command." *Journal of Business Continuity and Emergency Planning* 12 (4): 342–53. https://pubmed.ncbi.nlm.nih.gov/31200797/ (June 27, 2022).

This article explores the development and success of a recent program in Calgary (Canada) which was designed to bring together four agencies to improve interoperability. This program was designed to encompass all-hazards incident command and incident management. A key component of this effort was the development of tactic-specific standard operating procedures, equipment, and communications. Policy developed as part of this program was designed so that each agency could adopt and augment it as needed. Similarly, common communication practices were not only enacted but utilized by the agencies involved in the program.

Shahrah, Abobakr Y., Majed A. Al-Mashari, and M. Anwar Hossain. 2017. "Developing and Implementing Next-Generation Computer-Aided Dispatch: Challenges and Opportunities" *Journal of Homeland Security & Emergency Management* 14 (4). doi: 10.1515/jhsem-2016-0080.

This paper discusses the challenges and trends impacting the development and implementation of next-generation computer-aided dispatch technology. The authors highlight some of the impediments to this next generation, which include the continued use of legacy and conventional

CAD systems, as well as the "many complicated technological, operational, funding, and governing issues" (11). Additionally, the authors explore other potential hurdles, including information overload, cybersecurity, and interoperability.

Sharp, John. 2018. *Report of the Governor's Commission to Rebuild Texas: Eye of The Storm. Rebuild Texas: The Governor's Commission to Rebuild Texas.* https://www.rebuildtexas.today/wp-content/uploads/sites/52/2018/12/12-11-18-EYE-OF-THE-STORM-digital.pdf (July 21, 2022).

The "Eye of The Storm" report commissioned by the Texas governor's office takes an in-depth look into the emergency response to Hurricane Harvey. Although the majority of the report focuses on restructuring and realignment of agencies, it also addresses communication and data challenges as well. Chapter 5 discusses funding opportunities to improve the radio infrastructure. Chapter 8 looks at ways to better utilize social media, improve "relationships with private technology providers," and utilizing "data analytics to improve disaster management."

Smith, Kimberly A. 2014. "How ComEd Automatically Manages Blue-sky and Dark-sky Utility Crews." *Electric Light & Power*, 92 (6): 32–4.

This article explores the Commonwealth Edison Company's (ComEd) approach to the deployment of an automated system for the management of blue-sky and dark-sky utility crews. Although this article is centered on the utility provider, there are lessons that can be learned through the struggles and deployment of the system itself. This roll-out included a deviation from spreadsheets to a centralized database and automated crew management and call-out.

State of Connecticut Office of Policy and Management. 2020. *Legal Issues in Interagency Data Sharing.* Hartford, CT: State of Connecticut. https://portal.ct.gov/-/media/CT-Data/Legal-Issues-in-Interagency-Data-Sharing-Report-11521_merged.pdf (July 22, 2022).

This report presents Connecticut's State Data Plan, which identifies the legal obstacles to sharing high-value data of executive branch agencies, as well as provides recommendations to facilitate the sharing of data across government agencies. The recommendations include: establishing a coordinated statewide governance structure for cross-agency data sharing; and using flexible, durable data sharing agreements to protect clients' information and reduce the effort needed to share data. These

recommendations address the fragmented approaches to sharing data on high-priority issues, which reduce the ability of the state to mobilize a response.

Stephan, K. 2007. “We’ve Got to Talk: Emergency Communications and Engineering Ethics.” *IEEE Technology and Society Magazine*, Technology and Society Magazine 26 (3): 42–8. doi: 10.1109/MTS.2007.906675.

Emergency communications systems in the U.S. are owned and operated by thousands of individual municipalities, regions, and states. Emergency Communications technologies follow paths of governmental authority. As a result, while a system may provide reliable communications within the locale of who purchased it, they may not be able to talk to others nearby.

Sujata, J., S. Saksham, and S. Tanvi Godbole. 2016. "Developing Smart Cities: An Integrated Framework." *Procedia Computer Science* 93: 902–9. doi: 10.1016/j.procs.2016.07.258.

This paper explores the application of modern technology, like smartphones, to broader projects such as entire cities. The goal is to make the city more efficient and optimize resource allocations by analyzing real-time data from critical infrastructure, first responder agencies, healthcare facilities, and other stakeholders.

Texas Department of Public Safety. 2021. *Fiscal Year 2021 Report on Interoperable Communications*. https://www.dps.texas.gov/section/service/interoperability-report-pdf (July 22, 2022).

The Texas Department of Public Safety is required by Texas Government Code 421.098 and 421.096 to provide a report on interoperable communications to the Texas Legislature. This report highlights the planning, effectiveness, funding, accomplishments, and challenges of the statewide interoperable communications network. This report is Texas-specific but details the year’s activities towards interoperability for the entire State. The report grades counties on a scale of one to five, depending on their capabilities.

Tuite, D. 2008. "Radio Interoperability—It's Harder Than It Looks." *Electronic Design* 56 (8): 30–7 Penton Publishing, INC. https://www.electronicdesign.com/technologies/communications/article/21770393/radio-interoperabilityits-harder-than-it-looks (July 22, 2022).

This article explores the challenges many first responders are faced with when encountering emergency situations with differing equipment. Some of the technical challenges can be as simple as a single channel versus the use of multiple channels. The authors discuss how "trunking" and the use of "repeaters" can be a solution if done properly or additional confusion if not. Hardware solutions with built-in security are also identified in this article.

U.S. Department of Homeland Security. 2010. *NECP Capabilities Assessment Guide*. Cisa.Gov. https://www.cisa.gov/sites/default/files/publications/3aNECPCapabilitiesAssessmentGuide_07072010_FINAL_1.pdf (July 21, 2022).

Interoperability continuum, assessment guides, decision trees, and interagency coordination.

U.S. Government Accountability Office. 2012. *Information Sharing: DHS Has Demonstrated Leadership and Progress, but Additional Actions Could Help Sustain and Strengthen Efforts.* GAO-12-809. https://www.gao.gov/assets/gao-12-809.pdf (July 4, 2022).

GAO recommends that DHS revise its policies and guidance to include processes for identifying information-sharing gaps, analyzing root causes of those gaps, and identifying, assessing, and mitigating risks of removing incomplete initiatives from its list.

U.S. Department of Homeland Security. 2012. *Amateur Operators Aid Emergency Communications During Violent Storms in Tennessee*. CISA.Gov. https://www.cisa.gov/sites/default/files/publications/Case%20Study_Tennessee%20Violent%20Storms_0.pdf (July 22, 2022).

This case study outlines how amateur radio operators, or HAM radio operators, were able to assist emergency operations during violent storms that occurred in Tennessee. Since amateur radio operators do not operate on normal communication networks such as cell or internet, there are no interruptions that could be caused by an emergency. Although This case study is based on an emergency situation it does show how other modes of communication could be utilized in normal operations.

U.S. Department of Homeland Security. 2013. *Emergency Communications During the Response to the Boston Marathon Bombing*. CISA.Gov. https://www.cisa.gov/sites/default/files/publications/oec-

case%20study-support%20for%20response%20to%20boston%20marathon%20bombing-2013.pdf (July 22, 2022).

Although this is a case study involving communication between agencies in response to an emergency and not "blue sky day" operations, it offers great insight into how inter-agency communication can be effective and efficient. Local, state and federal agencies responded in unison to the actual bombing as well as the ensuing manhunt for the suspects. The successful execution of communication was due to precise and meticulous planning prior to the event utilizing a common system that all agencies could utilize in case of just such an emergency.

U.S. Department of Homeland Security. 2013. *Tribal Communications Partnerships - The Missing Piece in the Emergency Communications Landscape*. CISA.Gov. https://www.cisa.gov/sites/default/files/publications/oec-case%20study-tribal%20communications%20partnerships-2013.pdf (July 22, 2022).

This case study details the efforts made by the Office of Emergency Communications in assessing how local tribal communities communicate with neighboring counties and cities during an emergency. The establishment of an Emergency Operations Center Inside the tribal Government center incorporated the tribe into statewide communications plans.

U.S. Department of Homeland Security. 2015. *State, Local, and Tribal Coordination - Working with State, Local, and Tribal Public Safety Partners to Strengthen Emergency Communications.* CISA.Gov. https://www.cisa.gov/sites/default/files/publications/State%20and%20Local%20Coordination_Fact%20Sheet_July%202015%20FINAL%20508.pdf (July 22, 2022).

This document outlines the Office of Emergency Communications' mission to assist local, state, and tribal agencies in coordinating emergency communications. This document establishes the need for a regional coordination branch in each state that would be headed by a Statewide Interoperability Coordinator (SWIC). The SWIC would also implement a Statewide Communications Interoperability Plan (SCIP).

U.S. Department of Homeland Security. 2018. *Interoperability Continuum: A Tool for Improving Emergency Response Communications*

and Interoperability. https://www.hsdl.org/?view&did5769874 (June 30, 2022).

This tool was designed to assist agencies and policymakers in the planning and implementation of interoperability solutions. It identifies five elements that need to be addressed in order to achieve success in these efforts: governance, standard operating procedures, technology, training/exercises, and the use of interoperable communications. The authors of this document have created a useful visual tool for understanding the interoperability continuum, which illustrates that daily use of interoperable technologies can only be achieved when users are routinely working collaboratively with one another and familiar with the system(s). This type of use is also only sustainable when the system(s) are well-maintained and not viewed as a one-time investment but instead a long-term commitment/investment.

Verizon. 2022. "From Reactive to Proactive: Transforming Public Safety with Safe Cities Technologies." Verizon White Paper. https://www.verizon.com/business/content/dam/resources/whitepapers/transforming-public-safety-with-safe-cities-technologies.pdf (July 22, 2022).

This is a white paper from Verizon that discusses the benefits of utilizing safe city technologies to enhance public safety. This is a technology-driven piece that highlights evolving abilities in data collection and sharing. The paper discusses several factors and attributes of modern technology that collaborate to create a real-time response system.

Voss, Britta. 2019. Obstacles to Data Sharing in Public Safety Applications Require More than Technical Solutions Alone. *National Institute of Standards and Technology*. doi: 10.6028/NIST.SP.1243.

This report presents key non-technical challenges facing public safety use of emerging data sharing technologies. The author emphasizes that while more user-friendly or efficient devices and programs may increase the value of emerging communication technologies, they are unlikely to make technologies more accessible to agencies without adequate inter-agency governance structures or technically trained staff. Addressing these kinds of challenges requires a re-evaluation of institutional structures, policies, and funding processes.

Voss, Britta and Eric Anderson. 2019. *Interoperability of Real-Time Public Safety Data: Challenges and Possible Future States.* National

Institute of Standards and Technology. https://www.nist.gov/document/nistir8255pdf (July 22, 2022).

The Voss and Anderson report explores some of the challenges that agencies face in their mission to achieve the goal of interoperability with real-time data. This report is focused on the technical aspects of interoperability, specifically the public safety broadband network. It also incorporates some of the economic and legal challenges that agencies face in the implementation of these types of programs.

Wang, Li, Jun Zhang, Jianbin Chuan, Ruqiu Ma, and Aiguo Fei. 2020. "Edge Intelligence for Mission Cognitive Wireless Emergency Networks." *IEEE Wireless Communications* 27 (4): 103–9. doi: 10.1109/MWC.001.1900418.

Emergency communication infrastructures are of critical importance in disaster rescue scenarios, responsible for providing reliable connection services among victims, rescuers, and public safety command centers. Moreover, many rescue missions demand effective perception and real-time decision making, which highly rely on effective data collection and processing, and the availability of low-latency computation platforms. Wang et al. (2020) propose an edge intelligence-based MCWEN to address these challenges by leveraging edge-based technologies, including edge caching, edge computing, and edge learning.

Watson, B. 2016. "Is Twitter an Alternative Medium? Comparing Gulf Coast Twitter and Newspaper Coverage of the 2010 BP Oil Spill." *Communication Research* 43 (5): 647–71. doi: 10.1177/0093650214565896.

An alternative medium is best defined in contrast to a mainstream medium. Social media pushes may be a valid way to move important information in real-time.

Welch, Eric, Mary K. Feeney, and Chul Hyun Park. 2016. "Determinants of Data Sharing in U.S. City Governments." *Government Information Quarterly* 33 (3): 393–403. doi: 10.1016/j.giq.2016.07.002.

In this paper, the authors explore the mechanisms that facilitate and hinder data sharing in government. Some of the barriers that exist include a lack of trust and confidence that data will be used appropriately, a lack of technical standards and capacity, and contextual fas actors such as a limited understanding of data use and privacy laws. Municipalities are often reluctant to share too much data, given the risk of such information

being misinterpreted by the media or others. This often occurs in cases related to emergency response, where municipalities are under pressure to improve coordination and maintain public safety.