A Model Approach for Effective Emergency Telecommunication Architecture for Texas Border Cities

by

Juan Pablo Gutíerrez

An Applied Research Project
(Political Science 5397)
Submitted to the Department of Political Science
Texas State University
In Partial Fulfillment for the Requirements for the Degree of
Masters of Public Administration
Spring 2006

Faculty Approval:

_____
Dr. Hassan Tajalli

_____
Mr. Mario Molina

ABSTRACT

PURPOSE: The Texas-Mexico border region is considered to be one of the most important borders in the world because of the land area it covers, the large amount of international trade that occurs as a result of NAFTA, and the high rates of legal and illegal immigration that can be observed at any given time. Because of these reasons, the Texas-Mexico border is vulnerable to man-made or natural disasters. And because disasters can occur anywhere and at anytime, communities along the Texas-Mexico border must be prepared to effectively respond to a cross-border man-made or natural disaster. Therefore, it is important to assess and enhance current emergency telecommunications for cities along the Texas-Mexico border in the event of a cross-border catastrophe.

METHOD: The research examines and utilizes existing literature on the subject of emergency telecommunications to develop criteria for assessing and developing emergency telecommunication architecture for cross-border emergency response. The assessment focuses on public sector employees in cities along the Texas-Mexico border and their opinions concerning current cross-border emergency telecommunication infrastructure. Additionally, current local emergency management plans for cities along the Texas-Mexico border are examined as part of the assessment.

FINDINGS: The research findings suggest that effective emergency telecommunication infrastructure for cross-border emergency response is lacking along the Texas-Mexico border. The findings specifically address deficiencies in the areas of interoperability, survivability, security, and international connectivity, which are essential for effective cross-border emergency response and emergency response efforts in general.

Table of Contents

Figures

List of Tables

CHAPTER 1: INTRODUCTION

Research Purpose

The advent of telecommunication can be described as one of the greatest technological achievements in history. Telecommunications have bridged the smallest to largest of distances in the information gap, but telecommunications have also created a society dependent on constant and reliable communication. From the teenager who spends countless hours chatting on the phone or Internet, to the parent who orders takeout after a tough day at work, to the businessman who conducts transnational business, to the politician who conferences with world leaders to settle critical disputes, to the first responder who utilizes radio to respond to an emergency, telecommunications play an important role in the lives of every individual.

During emergencies, telecommunications are employed for coordination and response efforts between command and control centers and field emergency personnel. Without telecommunications, a breakdown in communication occurs between the command and control center and emergency response personnel. Communication breakdowns may result in uncoordinated, inefficient, and ineffective emergency response efforts. But more importantly, communication breakdowns may result in loss of life.

Yet despite the obvious reliability and resiliency of modern technology, telecommunication failures continue to occur. Existing literature on telecommunication is fraught with information and examples indicating that the United States' public telecommunication infrastructure is not keeping pace with technological advances. For emergency response, this failure can prove to be catastrophic. The Columbine High School shooting, the World Trade Center attacks, and the failed Hurricane Katrina evacuations underscore the impact and loss of life attributed to ineffective emergency telecommunication

infrastructure (Mayer-Schönberger 2002/2003, 2; Grubesic and Murray 2005, 802; Cannon et al 2005).

While the impact of telecommunication failures as a result of man-made or natural disasters have already demonstrated the inability for city's and states to effectively respond to their own emergencies, the public sector has yet to address the impact that telecommunication breakdowns could have on the ability for U.S. border cities to respond to cross-border emergencies with Canada and Mexico. This begs the question; can the same telecommunication breakdowns observed in the World Trade Center attacks and Hurricane Katrina evacuation efforts affect cross-border emergency response?

Because of the limited literature devoted to the subject of cross-border emergency the most likely response is yes. Olson et al. (2005, 75) state that "communications is arguably the most cited barrier to reaching and maintaining a high level of preparedness." Additionally, the recurring myth about infrastructure protection that only the United States is vulnerable solidifies Americas continued inability to effectively respond to emergencies attributed to telecommunication failures (Mickel-Kerjan 2003, 138).

The topic of cross-border emergency response is an important and timely topic because the possibility of man-made or natural disasters occurring along American borders is plausible. Consider the fact that America is at war and that its porous borders can be used by enemies to gain access into the United States to inflict economic harm against America. Also, consider the possibility of having to gear up for cross-border emergency response because of a major hurricane or tsunami possibly impacting the South Texas Gulf Coast, which is shared with Mexico. Because of these two possible scenarios and because Canada and Mexico are important allies and economic partners of the United States, it behooves American interests to implement

emergency response contingencies along the Canadian and Mexican borders in the event of a man-made or natural disaster.

To allow local and regional communities to determine their own emergency preparedness needs, the federal government has delegated emergency response activities to local governments. As a result, community officials and urban planners along the U.S.-Mexico and U.S.-Canadian border must shift their attention to address and mitigate any potential impact that any man-made or natural disaster may wreak on their borders. Key in addressing and mitigating any potential impact to American borders includes conducting pre-event planning, and enhancing emergency telecommunication infrastructure, which is critical to emergency response efforts. Olson et al. (2005, 76) explain that "Pre-event planning requires ongoing communication between sectors and agencies that usually interact on an as-needed basis."

Because a national assessment of emergency telecommunication infrastructure requires a lengthier time to conduct, this research focuses on assessing emergency telecommunication infrastructure along the Texas-Mexico border. The purpose of this research is threefold. First, to identify the ideal elements for effective cross-border emergency telecommunication architecture based on a review of the literature. The second purpose is to conduct a survey and assess emergency telecommunications in six Texas border cities using the ideal elements. And the final purpose is to make recommendations to Texas border cities for developing effective emergency telecommunication architecture for cross-border emergency response.

Benefits of Research

This research will help Texas border cities in developing effective emergency telecommunication architecture for cross-border emergency response that can later be duplicated by other border regions in the United States. First, the research assesses emergency

telecommunications for six Texas border cities to determine the current level of emergency planning and preparedness undertaken by each border city for cross-border emergency response. Second, the research provides a model framework for effective emergency telecommunication architecture to assist border cities in achieving a high level of preparedness for cross-border emergencies.

Chapter Summaries

To achieve the research purpose, this study is divided into six chapters. Chapter 2 provides background material explaining the global dependence on telecommunications and a discussion of what makes the Texas-Mexico border region an important area of interest. Chapter 3 reviews the current literature surrounding emergency telecommunication infrastructure, which allows for the development of the conceptual framework and model emergency telecommunication architecture designed for cross-border emergency response. Chapter 4 provides an overview of the applied research methods, which includes a discussion of the survey development, unit of analysis, target population, sample, and statistical methods used. Chapter 5 discusses the detailed results of the survey and document analysis. And Chapter 6 presents the findings of the research in relation to the overall research purpose, provides recommendations to Texas border cities for developing effective emergency telecommunication architecture for cross-border emergency response, and includes recommendations for future research.

CHAPTER 2: SETTINGS

The purpose of this chapter is twofold—to expand on the topic of telecommunication reliance and to examine characteristics unique to the Texas-Mexico border region, which underscore the need for effective emergency telecommunication architecture along the border.

Telecommunications

The global reliance on telecommunications is impalpable and can be illustrated in the amount of information transmitted over telecommunication networks. Grubesic and Murray (2005, 802) illustrate telecommunications reliance by examining the Internet telecommunications sector.

> To provide some additional insight into the massive information flows across telecommunication networks and their global importance, Internet traffic counts can be examined. Coffman and Odlyzko (2002) note that between 20,000 and 35,000 terabytes per month are transmitted over US backbone networks. To put this in perspective, an average e-mail with no attachments consists of approximately 60 kilobytes (Hachman, 2003). Therefore, if US Internet backbones were used to exclusively transport email, 20,000 terabytes of data would equal 357,913,941,333 email messages per month. At 35,000 terabytes, this figure nearly doubles, to 626,349,397,333 messages per month. Further, in terms of all information transmitted over telecommunication links, these figures do not include the 53,000 terabytes of US phone traffic per month-or the 6,000-11,000 terabytes of information transferred on private lines (Coffman & Odlyzko, 2002). Given these statistics, and the sheer amount of traffic on North American backbones, there is little doubt that the US and much of the developed world are heavily reliant on telecommunication networks for both commerce and communication.

While global reliance on telecommunications is underscored by the amount and instantaneous flow of information, the reliance on telecommunications by other infrastructure e.g. water supply, energy, transportation, banking and finance, can result in cascading effects. Krock (2004, 14) illustrates the cascading effects of telecommunications on other dependent infrastructure when he explains that “the primary goal following a service disruption is restoration of service as quickly as possible. This is especially true when a disaster disrupts

telecommunications services for an extended period of time. The longer the outage lasts, the greater economic impact the community will feel, the greater the vulnerability to terrorism will be, and the greater the likelihood that someone impacted by the disruption will have need of emergency services."

Telecommunication innovation is another contributing factor influencing the reliance on telecommunications. The deployment of different modes of communication such as radio, wireless, Internet, video, satellite, and voice over IP[1] communications has provided choices to consumers and greatly increased the consumer's ability to communicate instantly across vast distances. The dependence on these different modes of communication is self-evident because of their extensive availability and usage by the population at large.

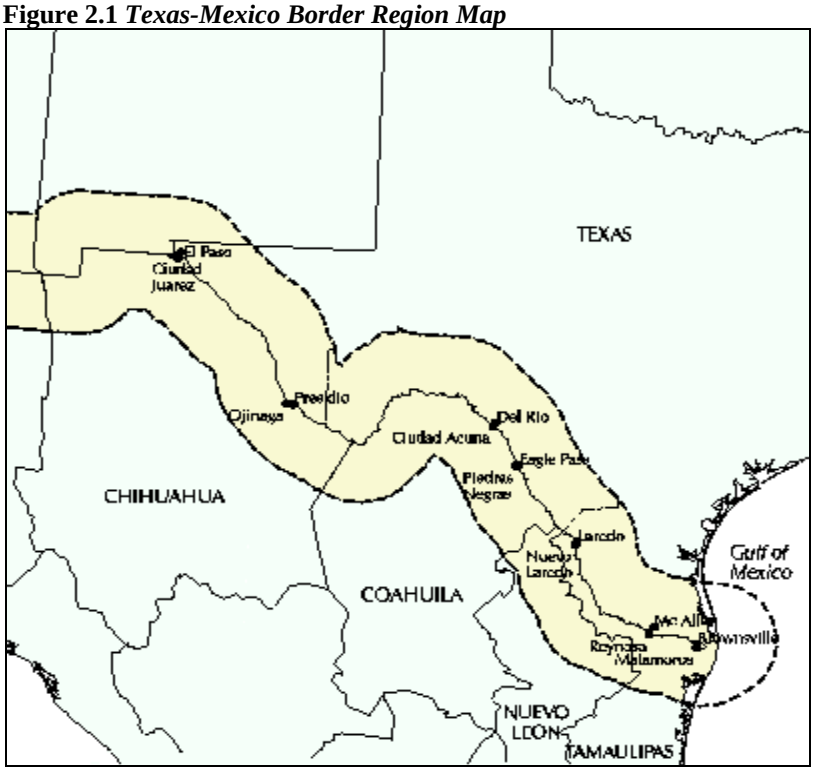
At the federal level, the public sector's dependency on telecommunications has prompted the United States Department of Homeland Security to classify telecommunications as one of thirteen critical infrastructures requiring protection from disasters. The thirteen national critical infrastructures include: agriculture and food, public health, emergency services, government, defense industries, banking and finance, chemical and hazardous material plants, postal and shipping services, transportation, water, *telecommunications*, and energy (Goodno 2005, 10).

Texas-Mexico Border Region

The Texas border with Mexico spans 1,240 miles and two-thirds of the U.S.-Mexico border is situated within the state jurisdictional lines of Texas (Governor Perry 2005). Because of their geopolitical location, Texas border cities are becoming epicenters of important national and international economic activities for the United States and Mexico. Figure 2.1 illustrates the jurisdictional lines of the Texas-Mexico border.

[1] Voice over Internet Protocol is the routing of voice conversations over the Internet or any other Internet Protocol based network. Voice over Internet Protocol is also referred to as VoIP, IP Telephony, Internet Telephony, and Broadband Phone. Current carries include Vonage, Time Warner Cable, etc.

Figure 2.1 ***Texas-Mexico Border Region Map***



Source: Texas Commissioner on Environmental Quality

The impetus of the Texas border region onto the global economic and political stage came with the ratification of the 1994 North American Free Trade Agreement (NAFTA). The purpose of NAFTA "was to bring Mexico into the free-trade zone that already linked the United States and Canada in order to create the world's largest market—a $6.5 trillion market with nearly 370 million people" (Kegley and Witkopf 1995, 246-247).

NAFTA has transformed quiet border towns into cities that continue to attract large numbers of businesses. Additionally, NAFTA has inadvertently increased legal and illegal immigration and transformed border cities into immigration hubs for illegal immigrants, terrorists, and drug cartels along the Texas-Mexico border region. However, because of the World Trade Center attacks, border security along the U.S.-Texas-Mexico border captured the national attention that it had previously lacked. Federal officials quickly began discussing the possibility of closing the U.S.-Texas-Mexico border for increased protection against terrorists.

But closure of the borders has never materialized due to the large amount of travel and commerce that NAFTA generates between the U.S., Texas, and Mexico, which is vital to all three economies, and in particular border economies. Instead, of closing the U.S-Texas-Mexico border the federal government has increased surveillance along the border. But emergency preparedness efforts require more than just surveillance.

In October 2005, in an attempt to address border security in a much broader context than surveillance, Texas Governor Rick Perry unveiled his "Border Security Plan for Texas," which addresses cross-border emergency response.

> Texas will seek partnerships with Mexican communities to minimize loss of life and damage to property if a catastrophic event occurs in the border region. Just as terrorism and crime affect both sides of the border, disasters and other emergencies do not respect national boundaries. Response and recovery are critical homeland security functions that will be tailored to the bi-national needs of the border. Bilateral emergency response plans and exercises will foster information channels between first responders in Texas and Mexico. These communication channels will also enhance other aspects of homeland security (Perry 2005, Border Security Plans).

While Texas Governor Rick Perry tackles border security and cross-border cooperation, his plan still requires cooperation from Mexico to effectively ameliorate security and cross-border issues. The plan provides an opportunity for both Texas and Mexico to cooperate and dialogue on cross-border issues affecting both sides i.e. crime, illegal immigration, and security threats.

Chapter Summary

This chapter provides background on two issues key to understanding the overall research purpose. The discussion centers on telecommunication reliance and the Texas-Mexico border region. The discussion of these two issues provides the ultimate justification for requiring effective emergency telecommunication architecture along the Texas-Mexico border.

CHAPTER 3: LITERATURE REVIEW

This chapter examines current scholarly literature on emergency telecommunications and specifically focuses on identifying critical elements for effective emergency telecommunication architecture for cross-border emergency response. The information used to develop the ideal elements also serves as criteria for assessing the effectiveness of current emergency telecommunications for Texas border cities.

There is extensive literature on the subject of emergency telecommunications, but the majority of it centers on the different emergency telecommunication devices and networks e.g. radio, wireless, Internet, video, satellite, and voice over IP communications currently available. While this research does not focus on the different telecommunication devices employed for emergency response, the information is useful in comparing, contrasting, and identifying the possible components that model emergency telecommunication architecture should include for effective cross-border emergency response.

Additionally, this chapter explores the history of emergency telecommunications, telecommunication failures in recent disasters, the impacts resulting from those telecommunication failures, and expands on emerging components from the literature review for model emergency telecommunication architecture. The ultimate goal of this research is to provide Texas border cities with recommendations to develop and implement model emergency telecommunication architecture for cross-border emergency response.

History of Emergency Telecommunications

While it may appear that emergency telecommunications is a new issue stemming from the attacks on the World Trade Center on September 11, 2001 and Hurricane Katrina events in 2005, the fact is that emergency telecommunications have been part of the national agenda for

quite some time. Unfortunately, it took for the World Trade Center attacks and Hurricane Katrina to redirect national attention to telecommunications once again. Houck et al. (2004, 157-158) explain how telecommunications play an important role in emergency response.

> The occurrence of a disaster event requires quick notification and mobilization of key management and recovery personnel who often reside at different locations. Coordination among key officials of various federal, state, and local government agencies normally takes place over the telecommunications networks; helping to ensure a more coordinated and measured response. While much of the communications at the disaster site occurs over the emergency communications channels, coordination of agencies, health care workers, and emergency aid and shelter providers occurs predominantly via telecommunication over public networks. As the disaster moves from the crisis phase, telecommunications' key role expands with a larger focus on data communication to support the cross infrastructure resupply operations necessary in the mitigation and reconstruction phases.

Emergency telecommunications first caught the attention of the federal government under President John F. Kennedy when he pushed for a communications system to assist in diffusing future critical situations like the one he experienced during the Cuban Missile Crisis standoff, which put the United States and Cuba on the brink of nuclear war. Because of President Kennedy's actions, the National Communications System (NCS) was created to ensure that uninterrupted, efficient, and effective communication was available during times of national security crisis (Lake 2004, 3).

In 1984, President Ronald Reagan also included telecommunications in his domestic agenda when he signed Executive Order 12472. Executive Order 12472 expanded the charge of the National Communications System (NCS) to ensure that the business communication needs of the entire federal government were met during times of national crisis. Additionally, the NCS

was also charged with ensuring that the larger national telecommunication infrastructure was reliable in meeting the needs of the nation as a whole (Lake 2004, 4).[2]

In 2001, emergency telecommunications resurfaced on the national agenda as a result of the attacks on the World Trade Center. That year, President George W. Bush signed Executive Order 13228, which directed the newly created Office of Homeland Security with coordinating the protection of public and privately owned information systems against terrorist attacks. Executive Order 13228 also mandated the Office of Homeland Security with coordinating telecommunication and information systems restoration efforts after a terrorist attack (Lake 2004, 4-5).[3]

Under President George W. Bush, the National Communications System (NCS) continues to play a key role in government. Lake (2004, 5) notes that the NCS continues its task of providing priority emergency telecommunications services to federal, state, and local governments. Additionally, the NCS also provides priority telecommunication services to key industries and organizations involved in emergency preparedness and response. The NCS provides emergency telecommunications services through the Government Emergency Telecommunication Service (GETS), the Wireless Priority Service (WPS), and the Telecommunication Service Priority (TSP). GETS, WPS, and TSP require approval by the NCS and Federal Communications Commission (FCC).

The Government Emergency Telecommunication Service (GETS) ensures that calls from key identified and designated emergency services personnel are provided with immediate access

[2] Executive Order 12472 expanded the responsibility of meeting the business and communication needs of the entire federal bureaucracy and not only the President's Office.

[3] Executive Order 13228 did not remove mandates previously placed on the NCS. Instead, EO 13228 tasked the Office of Homeland Security with specifically coordinating the protection of both public and privately owned information systems only against terrorist attacks. EO 13228 did not charge the Office of Homeland Security with meeting the needs of state and local government entities, nor did it charge that office with protecting public and private information systems against any other type of disaster.

and priority call processing during emergencies. GETS is accessed via a personal identification code provided by the federal government to pre-approved personnel to ensure their calls are prioritized above all others (Chambers and Riley 2004, 26). The Wireless Priority Service (WPS) is similar to GETS, but WPS ensures that key leaders and personnel are able to communicate via wireless networks through priority call service (Lake 2004, 6-7).

The Telecommunication Service Priority (TSP) is different because it does not provide priority call service to key personnel. Instead, TSP is geared at providing telecommunication vendors with guidance on how to prioritize requests with a TSP assignment versus a non-TSP assignment. TSP assignments are made by the FCC, where service requests are prioritized based on the importance to national security and emergency preparedness (Lake 2004, 7).

Emergency Telecommunication Failures and Impacts

The World Trade Center attacks shocked the American consciousness and forced the federal government to take a hard look at the vulnerability of America's critical infrastructure to man-made disasters. The World Trade Center attacks not only demonstrated the vulnerability of Americas telecommunication infrastructure but it also showed the interconnectedness of Americas telecommunication networks, and how that interconnectedness led to telecommunication failures that severely curtailed emergency response efforts. Grubesic and Murray (2005, 802) explain the impact of the World Trade Center attacks on America's interconnected telecommunication infrastructure.

> After the September 2001 attacks on the World Trade Center, Verizon Communications (the incumbent local exchange carrier for New York City) reported that nearly 200,000 voice lines, 100,000 business lines, 3.6 million data circuits and 10 cellular towers were damaged or destroyed. Also related to the attack, Nassau, Suffolk and Westchester counties lost their connection from the statewide health network and most of the state police network. Considering the combined population of these counties exceeds 3.5 million, this was a significant disruption, particularly in a time of crisis.

Historically, the issue of emergency telecommunication has been addressed by the federal government in growths and spurts.[4] Despite these efforts by the federal government, telecommunication failures between federal, states, local governments and key emergency personnel continues to be a problem. Lake (2004, 1) highlights the problems associated with continued lack of communication.

> Over the past three years, the NCS critical infrastructure has failed to provide uninterrupted communications support at all levels of the government during critical times of need. The terrorist events of September 11, 2001, and the northeastern states power grid failure in August 2003 are recent national events that reaffirm the requirement to leverage emerging technologies to streamline and integrate our nation's communication system at all levels of government as well as to improve our critical civilian telecommunications infrastructure.

Additionally, the Department of Homeland Security has also failed in the protection of our telecommunication and information systems as mandated by President George W. Bush in Executive Order 13228. Four years after the World Trade Center attacks, the telecommunication failures experienced on September 11, 2001, reverberated once more during Hurricane Katrina's assault on the Gulf Coast in September 2005. Cannon et al. (2005) highlight the continued telecommunication failures.

> Like a kick to the head, Hurricane Katrina didn't just hurt: It left the U.S. stunned, and staggering to respond. The same high winds and water that devastated the Gulf Coast destroyed the communications systems essential to any effort to copy with the aftermath. New Orleans police fought looters and staged rescues without the aid of working radios, while 911 calls got relayed through ham radio operators and distant cities; FEMA Director Michael Brown took days to learn of the people dying at the New Orleans convention center; the Louisiana and Mississippi emergency operations centers often struggled to get a working phone line.

If there is only one thing that America has learned from the World Trade Center attacks and Hurricane Katrina is that telecommunication infrastructure is critical in the modernization

[4] The different executive orders enacted by the different administrations demonstrate the importance of emergency telecommunications, but failed early on to provide a sense of national urgency in ensuring that effective emergency telecommunications were put in place for times of national crisis.

and development of cities. But despite the evolution of telecommunications, and the undisputed relationship between cities and their reliance on telecommunication infrastructure, urban planners have failed to prioritize telecommunications as critical infrastructure. Andrew and Petkov (2003, 277) explain that "As a development tool, telecommunications has been largely ignored by planners and theorists. It is generally grouped with public utilities and infrastructure, ranking far below roads, power supply, water, and sanitation as investment priorities. Yet telecommunications is a primary tool for the conveyance of information, and it is the lack of consideration of the role of information in development theory that is perhaps more surprising."

Components of an Effective Emergency Telecommunications Architecture

The review of literature suggests that current telecommunication infrastructure does not support effective emergency response. As a result, emergency management plans must be enhanced to mitigate the impact of not only man-made but natural disasters.[5] Jrad et al. (2004, 108) explain the importance of emergency management plans for business continuity purposes.

> Business continuity preparedness comprises the set of processes by which a business prepares itself for disasters and unplanned events. These disasters include not only natural disasters such as earthquakes and hurricanes and high-profile disasters such as terrorism, but also everyday disruptions caused by events like plumbing failures. Since it is not possible to predict precisely the nature, timing, and severity of these disasters, it is necessary to be prepared for a variety of disasters that may occur.

While the act of responding to an emergency is important, the implementation of emergency management plans before man-made or natural disasters occur is critical. Pre-event planning facilitates emergency response efforts by identifying barriers and vulnerabilities ahead of a disaster. But, emergency management plans should also approach telecommunication barriers and vulnerabilities with pragmatic solutions to achieve the highest level of readiness. For

[5] Executive Order 13228 signed by President George W. Bush charged the Office of Homeland Security with coordinating telecommunication and information systems restoration efforts after terrorist attacks, but neglected to include direction about restoration efforts after natural disasters.

example, after the World Trade Center attacks, telecommunications became a standard in emergency management plans for cities, counties, and states across the United States. But the inclusion of telecommunications in emergency management plans does not imply that a city's emergency has achieved a high level of readiness.

Emergency telecommunications should be approached as a life saving tool and should be designed in a manner that will improve the overall response while minimizing any duplication. Approaching emergency telecommunications in a pragmatic manner is important because in the United States alone, emergency telecommunications help more than 8 million U.S. emergency personnel respond to emergencies and save countless lives (Sawyer et al. 2004, 62).

Interoperability

The first step in developing effective emergency telecommunication architecture is to ensure interoperability. Interoperability is defined as "the ability of public safety personnel to communicate by radio with staff from other agencies, on demands and in real time" (Mayer-Schönberger 2002/2003, 2). Interoperability is critical because it provides a medium to effectively and efficiently respond to any given emergency with the goal of preventing or minimizing the loss of life. Interoperability has been difficult to achieve due to the large number of different telecommunication systems utilized by emergency responders. The large diversity of telecommunication systems becomes problematic when some emergency telecommunication devices are not able to interface with other telecommunication devices (Balachandran et al. 2004, 5; McGinity 2004, 16-17; Roane et al. 2004; Potter et al. 2004, 103-104; Yuan and Detlor 2005, 95; Fischer 1996, 210; Lake 2004, 8). In short, the lack of interoperability hampers emergency response efforts and contributes to additional loss of life. Mayer-Schönbeger (2005, 832) explains the lack of interoperability for emergency response.

> Numerous reports on disasters and terrorist attacks have identified the lack of radio interoperability as a major shortcoming in the rescue operations, from the first World Trade Center bombing to the shoot out at Columbine High School. Yet the impact of these reports has been limited. Thus on September 11, 2001, perhaps hundreds of first responders in the World Trade Center died because of a complete lack of communication interoperability. Moreover, the firefighters from Virginia, Maryland and the District of Columbia battling the Pentagon blaze had to use runners to communicate with each other as their radios lacked interoperability.

For emergency response efforts to be efficient and effective, emergency telecommunications must not only employ interoperability. Emergency telecommunications should include suitable technology, common standards, and common frequencies if interoperability is to be fully realized.

Suitable technology is another sub-element that is important for achieving full interoperability because it ensures that the diverse telecommunication modes are able to interface with each other when responding to an emergency. Mayer-Schönberger (2002/2003, 5) notes that any technology implemented for interoperability realization, will require the ability to integrate the various emergency services communication networks from the local, state, and federal level. Potter et al. (2004, 106) discuss the importance of suitable technology.

> Best practices using advanced technologies enable us to integrate and accelerate our emergency communications in ways never possible before. Prominent among these technologies is the emergency of the Web services approach, using M=SML and SOAP. XML is being increasingly used for data exchange, while SOAP has all the elements of an efficient transport mechanism. This enables development of standard methods for linking diverse data systems into a coherent national and global architecture. Similarly, international business has faced the challenges of integrating with legacy systems, interoperating with multiple devices and systems controlled by multiple parties, and providing powerful authentication, authorization, security, and privacy capabilities.

Common frequencies and standards are also important for interoperability because they allow for emergency personnel to communicate through devoted frequencies with common telecommunication platforms. Mayer-Schönberger (2002/2003, 6) argues that “Without such

commonality, even the best technology will be useless in terms of interoperability, and for an obvious reason: A common frequency allows all users to communicate over the same set of channels." But establishing a common frequency for interoperability is not enough; a common technological standard is also required. Potter et al. (2004, 105) explain that "The existing communication platforms among members of the emergency community vary in a number of aspects. They range from being simple to sophisticated, open standards-based to entirely proprietary, legacy to modern, analog to digital, only voice to voice and data, and more."

While review of the literature provides information on the wide array of communication networks that can be used to achieve interoperability (McGinity 2004; Chambers and Riley 2004; Hinton et al. 2005; Malone 2004; Jackson 1999; Ecklund et al. 2001; Berghel and Uecker 2004; Balachandran et al. 2004; Beroggi and Wallace 1995) there is no consensus as to which communication network provides greater interoperability at this time. However, selection of a particular communication network is recommended to achieve the full benefits of interoperability. Hoyt et al. (2004, 83) illustrate the benefits of common frequencies and networks.

> Today in the United States there are over 150 million wireless subscribers. We have the most advanced medical systems, increasingly "smart cars," thousands of 9-1-1 centers, hundreds of state-of-the-art transportation centers, almost 65,000 other emergency agencies, and now major federal homeland security investments in communications. These sit in the midst of the economy with the world's most advanced communications. These sit in the midst of the economy with the world's most advanced communications and information systems. Credit and ATM cards work anywhere in the world, yet ether is no modern network linking emergency agencies together: we are not linking these components with modern technology in order to share information with appropriate emergency responders in real time. Emergency medical technicians carry multiple radios and make notes on duct tape on their legs. We cannot automatically locate most wireless 9-1-1 callers; far too often we dispatch EMTs with the most minimal of information. There are only the faint beginnings of an emergency medical and emergency response network for the President, a Governor or Centers for Disease Control and Prevention to use in a bioterrorism event, or of any emergency.

Survivability

Survivability in emergency telecommunications is important because it ensures that communication will remain operational after a disaster has occurred to ensure business continuity (Krock 2004, 164; Houck et al. 2004, 155; Lake 2004, 12). Survivability does not imply that any emergency telecommunication architecture is fail-safe, but it does provide some reassurance that the system is reliable and repairable to perform its required functions under stated conditions for a specified period of time (Lake 2004, 12). The United States Department of Commerce has one of the most widely used definitions for survivability. Survivability refers to "a property of a system, subsystem, equipment process, or procedure that provides a defined degree of assurance that the named entity will continue to function during and after a natural or man-made disturbance" (Grubesic and Murray 2005, 802). To achieve greater telecommunication survivability, the design phase of telecommunication network paths should include diversity, separation, avoidance, and hardening.

Diversity establishes different interconnecting routes between networks. Grubesic and Murray (2005, 804) state that "Having a diverse set of interconnecting routes on a communication network increases the probability of network survival in a situation of nuclear attack. As such, the loss of a single switching or junction office will not cause the complete loss of service to an area." Diversifying interconnecting routes on a telecommunication network prevents all emergency telecommunications services from failing and allows for emergency calls to be routed through other networks when one or several networks have been disabled. Baker et al. (2004, 131) argue that the lack of diversity makes telecommunication networks vulnerable during disasters.

The May 1998 Hinsdale Fire illustrates the lack of network diversity. In 1998, the central telephone switching office in Hinsdale, Illinois, caught fire and left thousands of customers without telephone service. The repair took five weeks. But not before both Chicago airports lost crucial communication lines to the Federal Aviation Administration resulting in flight delays. (Krock 2004, 164).

Separation of current network paths from new ones is also important for emergency telecommunication survivability. Grubesic and Murray (2005, 805) explain that "adequate separation between existing and new network paths should be maintained. This reduces the risk of both routes being damaged or destroyed by a single detonation." Separation of network paths enables emergency telecommunications to continue operating should one of the network paths become compromised. For example, "if all telephone lines in a large metropolitan area must physically connect to one digital switch at one centralized location, the destruction of the switch will end all wire line telecommunications service to the entire area until the switch is restored or replaced" (Baker 2004, 126).

Avoidance recognizes the need to avoid potential targets that may facilitate telecommunication failures. Grubesic and Murray (2005, 805) recommend that "when possible, major network routes should be constructed away from potential targets, such as major cities or government installations." Avoidance requires strategic planning and placement of major telecommunication networks from harms way.

Hardening refers to the materials used to construct the telecommunication networks. Hardening is a concept that "ensures that the materials (e.g. coaxial cable) used for network construction should be able to withstand a certain level of overpressure (measured in pounds per

square inch) after a nuclear blast—although proper avoidance planning minimizes this need" (Grubesic and Murray 2005, 805).

The main function of survivability is to ameliorate catastrophic telecommunication failures. The telecommunication failures observed in the World Trade Center attacks and Hurricane Katrina relief efforts can be partially blamed on the lack of survivability. As a result, the loss of life could have been minimized if diversity, separation, avoidance, and hardening had been built into the construction of the telecommunication networks during the design and planning phase.

Security

Security is another important element because it enables the protection of emergency telecommunication networks and ensures survivability. With over two billion miles of telecommunication cables (Goodno 2005, 13) and with reports of new viruses circulating our telecommunication networks, security breaches can prove detrimental because of the amount of business conducted over telecommunication networks. Take for example, the security issues surrounding cellular phones. "Everyone, even war fighters and first responders, love cell phones, and everyone is accustomed to using them. The difference is security. Most of today's cell phones are not secured, which means anyone can listen" (Salis 2003, 533). As a result, telecommunications infrastructure can essentially be used against us (Michel-Kerjan 2003, 133). Lake (2004, 12) explains that "networks must have protection against corruption of, or unauthorized access to, traffic, and control, including expanded encryption techniques and use authentication, as appropriate."

Addressing all vulnerabilities in emergency telecommunication architecture is the first step in addressing security concerns. Rauscher (2004, 2) explains the importance of assessing vulnerabilities.

> Vulnerability is a characteristic of any aspect of the communications infrastructure that renders it, or some portion of it, susceptible to damage or compromise. A threat is anything with the potential to damage or compromise the communications infrastructure or some portion of if. Threats exercise vulnerabilities. The principle value of systematically addressing vulnerabilities is that protection is provided independent of knowing what threats there may be. While the fundamental vulnerabilities are constantly changing.

Additionally, redundancies must be built into any emergency telecommunication architecture to ensure that natural or man-made disasters do not hamper emergency telecommunications. Redundancies are often referred to as back ups and can facilitate rapid repair in the event of a security breach. "Planners can work with utilities to make sure that redundancies are built into the local infrastructure. This means assuring that back up systems are in place to deliver power, water, communications, and other services in the event of an attack" (Goodno 2005, 15).

International Connectivity

International connectivity is the most important element for effective emergency telecommunication architecture for cross-border emergency response because the literature devoted to the subject of cross-border communication explains that "communication is arguably the most cited barrier to reaching and maintaining a high level of preparedness" (Olson et al. 2005, 76).

The European Union provides a perfect example of how emergency telecommunication infrastructure can be implemented to assist in cross-border emergency response efforts. The European Union has deployed radio interoperability with the capability of permitting

interoperable communications to occur between a few to thousand users across the continent (Mayer-Schönberger 2002/2003, 28). Key to the European community is "the realizations among many European public safety officials that catastrophes neither stop at borders nor involve just one agency—as exemplified by the tragic avalanche catastrophe in Galtür—which demonstrated the need for cross-border and cross-agency cooperation" (Mayer-Schönbeger 2005, 837).

Because numerous countries around the world share borders with other nations and because disasters can occur anywhere in the world, border communities must prioritize international connectivity. While border security can provide some level of protection against man-made disasters, border security cannot solely protect border communities from disasters. Jebara (2004, 709) explains that border security cannot be mistaken for full protection.

> Recent experience has shown that no country, however, economically well-developed it may be is capable of ensuring 100% security of its borders by imposing quarantine measures or import bans on animals and animal products, nor can it totally prevent the illegal flow of migrant human populations. Humans and commodities, including live animals, may illegally enter any country in the world.

The Texas-Mexico border region must learn to embrace the European spirit of cooperation when it comes to cross-border emergencies and emergency telecommunication infrastructure through international connectivity. Olson et al. (2005, 77) note that communication methods and protocols must be established to achieve a consistent approach to response activities.

> Rapid communication and surveillance systems that can reach a variety of local and federal agencies and organizations quickly and remain functional in times of emergency are of crucial importance. The Health Alert Network (HAN), Early Aberration Reporting Systems (EARS), Metropolitan Medical Response Systems (MMRS), and other incident management systems have all been developed to streamline detection and response efforts to address some of the communication issues across borders. Yet the physical resources for communication continue to need maintenance and standardization, from computer systems to radio broadcast channels.

Conceptual Framework

The purpose of this research is to assess the practical ideal elements found in the conceptual framework for effective emergency telecommunication architecture for Texas border cities. Conceptual frameworks provide a structure that allows researchers "to help connect the problem to the observed data" (Shields 1998, 210). The practical ideal type framework allows researchers to measure a perceived problem or question against a set of criteria (Shields 1998, 210). According to Shields (1998, 215), "practical ideal types can be used as standards or points of reference."

The elements and sub-elements of the conceptual framework emerged from the review of the literature. The four elements are interoperability, survivability, security, and international connectivity, which are summarized in Table 3.1. The elements are also employed to assess the effectiveness of current emergency telecommunications for cross-border emergency response by Texas border cities.

Table 3.1 ***Linkages of Ideal Categories to Literature Review***

Ideal Categories	Sources
INTEROPERABILITY	Mayer-Schönberger 2002/2003; Balachandran et al. 2004; McGinity 2004; Roane et al. 2004; Potter el al. 2004; Yuan and Detlor 2005; Fischer 1996; Lake 2004; Mayer-Schönberger 2005
• **Suitable Technology**	Mayer-Schönberger 2005; Potter et al. 2004
• **Common Frequencies and Standards**	Mayer-Schönberger 2002/2003; Potter et al. 2004; Hoyt et al. 2004; McGinity 2004; Chambers and Riley 2004; Hinton et al. 2005; Malone 2004; Jackson 1999; Ecklund et al. 2001; Berghel and Uecker 2004; Balachandra et al. 2004; Beroggi and Wallace 1995.
SURVIVABILITY	Krock 2004; Houck et al. 2004; Lake 2004, 12; Grubesic and Murray 2005
• **Diversity**	Grubesic and Murray 2005; Baker 2004; Krock 2004
• **Separation**	Grubesic and Murray 2005; Baker 2004
• **Avoidance**	Grubesic and Murray 2005
• **Hardening**	Grubesic and Murray 2005
SECURITY	Lake 2004; Salis 2003; Michel-Kerjan 2003; Goodno 2005; Rauscher 2004.
INTERNATIONAL CONNECTIVITY	Olson et al. 2005; Michel-Kerjan 2003; Jebara 2004; Mayer-Schönberger 2002/2003; Mayer-Schönberger 2005

Chapter Summary

This chapter examined the connections between the ideal elements and their relationship to emergency telecommunications. The four ideal elements are the focus of discussion throughout the review of the literature. The conceptual framework above links the literature to the ideal elements. The next chapter discusses the methodology used to assess the effectiveness of current emergency telecommunications for cross-border emergency response for six Texas border cities.

CHAPTER 4: METHODOLOGY

This research project evaluates current emergency telecommunications for six Texas border cities against the practical ideal categories developed in Chapter 3. The six Texas border cities being assessed are Brownsville, Del Rio, Eagle Pass, El Paso, Laredo, and McAllen. The focus on these six Texas border cities is based on their regional significance to the Texas-Mexico border, which was discussed in Chapter 2.The research techniques employed for evaluating the six Texas border cities is discussed. And the conceptual framework is operationalized and used as a template for data collection. Table 4.1 expresses how each of the ideal categories is operationalized for each research technique.

Research Techniques

The main research technique used to assess the effectiveness of emergency telecommunications for cross-border emergencies for Texas border cities is survey research. Document analysis is used as a secondary research technique to compare and contrast respondent's knowledge and opinions against the actual emergency management plans for each of the six cities being assessed.

Survey Research

Survey research is the primary research technique used for this research. Shields argues that survey research can be utilized for collecting information from experts on an issue (1998). The strength of survey research stems from its unobtrusive nature as respondents can complete the survey items at their convenience (Salandt and Dillman 1994, 9 as cited in Jeffers 2003, 62). Additionally, survey research is in its nature descriptive research (Babbie 2004, 238). Given these considerations, a survey was deemed to be the appropriate medium by which to address the research purpose.

The unit of analysis for this survey is public sector employees at the city and county level responsible for emergency planning and response decisions. The opinions of public sector employees are important to this research for two reasons. Because both federal and state governments have delegated emergency planning and response efforts to city and county governments, and because public sector employees conduct emergency planning and response efforts that have been delegated to cities and counties.

A weakness of the self-administered survey is its lack of opportunity for respondents to explain why they took a certain position on a question. The inability to explain why a participant responded in a particular way leaves the research vulnerable to missing important information (Babbie 2004, 275).

Development of the Survey

The focus of this research is to assess the effectiveness of emergency telecommunication infrastructure for Texas border cities. Survey questions were developed to assess the strength of the connection between the ideal type categories and the respondent's knowledge and perceptions of their city's telecommunication infrastructure. Survey questions are particularly useful in determining "the extent to which respondents hold a particular attitude or perspective" (Babbie 2004, 244).

The survey was divided into three parts and included a total of 39 questions. A copy of the survey instrument can be found in Appendix A. The questionnaire initially posed qualifying questions designed to ensure respondents were representative of the targeted population, i.e. public sector employees who resided, were employed, and/or represented one of the six Texas border cities being assessed. The second part of the questionnaire assessed current emergency telecommunications for each of the six Texas border cities based on the respondent's knowledge

and perceptions. The four ideal elements and sub-elements discussed in Chapter 3 were used to design a survey template to conduct the respondent assessment. The final part of the survey was designed to assess the interest in developing emergency telecommunication architecture for cross-border emergency response along the Texas-Mexico border composed of the four ideal elements and sub-elements.

The survey instrument uses both questions and statements. Babbie argues that “Both questions and statements can be used profitably. Using both in a given questionnaire gives you more flexibility in the design of items and can make the questionnaire more interesting as well” (2004, 245).

Table 4.1 ***Operationalization of the Conceptual Framework for Self-Administered Survey***

Ideal Type Category	Survey Questions
INTEROPERABILITY	▪ Is telecommunications interoperability a component of your city or county emergency management plan? ▪ Does your city or county currently have interoperable telecommunication capabilities for emergency response? ▪ How important is interoperability for emergency response to your city or county? ▪ Is employing the latest most suitable technology important to your city or county in achieving interoperability? ▪ Do you consider different radio bands/frequencies a problem to achieving interoperability for your organization?
• Suitable Technology	▪ Does your city or county consider the use of different telecommunications technology a problem to achieving interoperability?
• Shared Standards	▪ How important are shared telecommunication standards to your city or county for effective interoperability? ▪ How important are common telecommunication frequencies and networks to your city or county for effective interoperability?
• Common Frequencies	▪ How important are common telecommunication frequencies and networks to your city or county for effective interoperability?
SURVIVABILITY	▪ Is telecommunications survivability a component of your city or county emergency management plan? ▪ Have telecommunication failures affected your city or county's ability to respond to an emergency? ▪ Has your city or county developed a telecommunications business continuity plan intended to assist in maintaining order and deliver minimum essential public services and emergency services in the event of a disaster?
• Diversity	▪ Do you believe that having a diverse set of interconnecting routes on a telecommunications network would increase the probability of network survival in a disaster? ▪ Is your city or county telecommunications network designed with a diverse set of interconnecting routes to increase the probability of network survival during a disaster?
• Separation	▪ Do you believe that separation between existing and new telecommunication network paths would reduce the risk of both routes being damaged or destroyed by a single disaster? ▪ Is your city or county telecommunications network designed with separated network paths between existing and new networks to ensure survivability?
• Avoidance	▪ Do you believe that the construction of telecommunication network routes should avoid potential targets or vulnerable areas, such as major cities or government installations to ensure survivability? ▪ Are your city or county telecommunication network routes near potential targets or vulnerable areas?
• Hardening	▪ Do you believe that telecommunication networks should be constructed with materials that are able to withstand any disaster? ▪ Are your city or county telecommunication networks constructed with materials that are able to withstand any disaster?
SECURITY	▪ Does your city or county emergency management plan include telecommunications security? ▪ Have telecommunication security breaches ever affected the ability of your city or county to respond to an emergency? ▪ How secure would you consider your city or county telecommunications infrastructure?
INTERNATIONAL CONNECTIVITY	▪ Does your city or county emergency management plan include international connectivity? ▪ Given your city and county geographical location along the Texas-Mexico border, do you agree that cross-border emergencies can occur? ▪ Has your city or county identified cross-border emergency telecommunications as a public safety concern? ▪ Do you believe that it is important for your city or county to have the ability to communicate with Mexican partners during a cross-border emergency? ▪ Has your city or county ever responded to a cross-border emergency? ▪ Is your city or county able to communicate with Mexican partners during emergencies?

Survey questions were pre-tested with the Community Preparedness Section staff at the Texas Department of State Health Services (DSHS) because of their expertise in emergency planning and response efforts and because of their experience with survey development. Pre-testing was conducted because it ensures protection from errors that could result from poorly written questions (Babbie 2004, 256). The DSHS Community Preparedness staff suggested questionnaire items, reviewed and edited the survey instrument, suggested possible target groups for the survey, and provided suggestions to increase the probability of respondent participation and completion.

A request was submitted to the Texas State University Institutional Review Board to obtain exemption from the United States Department of Health and Human Services (HHS) 45 CFR, Part 46, Sec. 101(b) and Texas State University's UPPS 02.02.03 regulations concerning the protection of rights and welfare of human subjects. The request for exemption and subsequent approval were based on the minimal risk that the research posed to the research participants.[6] The exemption waiver is on file with Texas State University's Institutional Review Board under approval number 05-0360.

Target Population and Sample

While the unit of analysis for this survey is public sector employees at the city and county level responsible for emergency planning and response decisions, the target population is narrowed through purposive sampling. Babbie defines purposive sampling as "a type of non-probability sampling in which you select the units to be observed on the basis of your own judgment about which ones will be the most useful or representative" (2004, 274). As a result,

[6] Texas State's Institutional Review Board Policy concerning the protection of human research subjects can be viewed at http://www.txstate.edu/osp/Compliance/irb_index.htm.

the target population for this study includes public sector elected officials at the federal and state level; state agency heads; county officials; city officials; public works personnel; emergency medical services (EMS); fire; police; sheriff; and general city, county, and state employees who work and/or live in each of the six Texas border cities being assessed.

The knowledge, attitudes, and opinions of public sector emergency response decision-makers at the federal, state, county, and local levels is important because their opinions are representative of the population, cities, counties, and constituencies they serve. Additionally, the use of this target population allows for differing view points to be considered, which ensures a more objective assessment of current emergency telecommunication infrastructure for the six border cities assessed.

A total of 346 surveys were distributed, but because a representative sample of the target population would constitute a large number of respondents, survey research is conducive to assessing respondents. According to Babbie "surveys are excellent vehicles for measuring attitudes…in a large population" (2004, 243).

Description of Returned Surveys

The internet company *Advanced Survey* administered the survey and responses were solicited through e-mail from 346 respondents.[7] Of the 346 surveys, 61 responded, resulting in a response rate of 18 percent. While the response rate is acceptable, it is lower than the recommended 50 percent rate which leaves room for biases or error (Babbie 2004, 256). The response breakdown can be observed in Table 4.2.

[7] Advanced Survey can be accessed by visiting their website at http://www.advancesurvey.com/.

Table 4.2 ***Survey Target Population Response Breakdown***

TARGET POPULATION (N=346)	N	%	CITY/COUNTY	N	%
Federal/State Elected Officials (TX Legislator, US Senator, Congressman, etc.)	3	5	Brownsville/Cameron County	16	26
State Agency Head	3	5	Del Rio/Val Verde County	10	16
County Official (County Judge, etc.)	3	5	Eagle Pass/Maverick County	3	5
County Employee	3	5	El Paso/El Paso County	23	38
City Official (Mayor, City Council, City Manager, etc.)	7	11	Laredo/Webb County	1	2
City Employee	18	30	McAllen/Hidalgo County	8	13
Public Works (Utilities)	0	0			
Fire	2	3			
EMS	11	18			
Police/Sheriff	2	3			
Other	9	15			
TOTAL	**61**	**100**	**TOTAL**	**61**	**100**

Document Analysis

The focus of this research is to assess emergency telecommunications for Texas border cities. For this research purpose, document analysis is used as a secondary research technique to help corroborate the survey findings. Yin (2003, 87) explains that document analysis may not be the most accurate source of information, and that it should be used "to corroborate and augment evidence from other sources."

The documents used to corroborate the survey findings were emergency management plans developed by each of the six Texas border cities, specifically Annex B. In Texas, the Department of Public Safety has adopted standards to be used during the development of emergency management plans by Texas cities and counties. The standards translate into a series of documents which are encompassed in the larger emergency management plans, which include legal documents, the basic emergency plan, functional annexes, and standard operating procedures as shown in Figure 4.1.

Legal documents outline the legal authority in the establishment and operation of local emergency plans. The basic emergency plan provides a general explanation of emergency

management requirements such as overall goals, resources, and responsibilities. Functional annexes provide more detailed information on planning standards, roles, and responsibilities by function on topics such as shelter and mass care, energy and utilities, evacuation, law enforcement, and telecommunications. Standard operating procedures provide prescribed courses of action in the event that emergency response is activated. Together, these documents create emergency planning standards ensuring that common emergency functions are adequately addressed and documented by cities and counties.

Figure 4.1 ***Standardized Local Planning Documents***

1. Legal Documents
2. Basic Emergency Plan ***(General Information)***
3. Annexes ***(Detailed Information by Function)***
Annex A–Warning
Annex B–Communications[8]
Annex C–Shelter & Mass Care
Annex D–Radiological Protection
Annex E–Evacuation
Annex F–Firefighting
Annex G–Law Enforcement
Annex H–Health & Medical Services
Annex I–Emergency Public Information
Annex J–Recovery
Annex K–Public Works & Engineering
Annex L–Energy & Utilities
Annex M–Resource Management
Annex N–Direction & Control
Annex O–Human Services
Annex P–Hazard Mitigation
Annex Q–Hazardous Materials & Oil Spill Response
Annex R–Search & Rescue
Annex S–Transportation
Annex T–Donations Management
Annex U–Legal
Annex V–Terrorist Incident Response
4. Standard Operating Procedures

Source: Governor's Division of Emergency Management, a Division of theTexas Department of Public Safety

[8] Annex B is a standard section found in most emergency management plans, which provides detailed information on communication planning standards, roles, and responsibilities. Additionally, the basic emergency plan also supplies information about communication, but in a more generalized manner. For this research, Annex B is of particular importance because it details specific information which is critical to the overall assessment of emergency telecommunications for Texas border cities.

Because the purpose of this research is to assess the effectiveness of emergency telecommunications for Texas border cities, an open records request was submitted to the emergency management coordinators for the cities of Brownsville, Del Rio, Eagle Pass, El Paso, Laredo, and McAllen to obtain the basic emergency plan and Annex B from the list of standardized local planning documents in Figure 4.1. The request was submitted as an open records request because of the sensitive nature of emergency management plans.[9] Despite the open records request to all six cities, the responses returned were mixed, with five cities submitting either one or both documents. Laredo was the only city to not respond to the open records request. Table 4.3 shows the link between the emergency management plans and the conceptual framework.

Table 4.3 ***Operationalization of the Conceptual Framework for Document Analysis***

Ideal Category	Document	Indication of ideal type
INTEROPERABILITY	Emergency Management Plan/Annex B	Is interoperability a component?
• Suitable Technology	Emergency Management Plan /Annex B	Is suitable technology a component?
• Shared Standards	Emergency Management Plan /Annex B	Is shared standards a component?
• Common Frequencies	Emergency Management Plan /Annex B	Is common frequencies a component?
SURVIVABILITY	Emergency Management Plan /Annex B	Is survivability a component?
• Diversity	Emergency Management Plan /Annex B	Is diversity a component?
• Separation	Emergency Management Plan /Annex B	Is separation a component?
• Avoidance	Emergency Management Plan /Annex B	Is avoidance a component?
• Hardening	Emergency Management Plan /Annex B	Is hardening a component?
SECURITY	Emergency Management Plan /Annex B	Is security a component?
INTERNATIONAL CONNECTIVITY	Emergency Management Plan /Annex B	Is international connectivity a component?

Chapter Summary

This chapter discussed the methodology used to collect data. The conceptual framework facilitated the creation of the survey and coding sheet for document analysis through the

[9] Requests for open records must meet the guidelines prescribed by the Texas Public Information Act in the Texas Government Code. The specific codes cited for this open records request included Texas Government Code, Chapter 552.023 Special Right of Access to Confidential Information, Chapter 552.229 To Release Information Under Special Right of Access, and Chapter 552.307 Special Right of Access; Attorney General Decisions.

operationalization of the ideal type categories discussed in Chapter. The following chapter will describe the data collected and provide an analysis of the statistics compiled.

CHAPTER 5: RESULTS

As previously stated, the purpose of this study is to assess emergency telecommunications for Texas border for effective cross-border emergency response. Chapter 4 outlined the methodology used in this study and operationalized the conceptual framework into a template for the survey and document analysis. This chapter presents the survey findings and data collected from the analysis of the basic emergency management plans and specifically Annex B. The findings of the survey are used to examine the connection between the assessment of current emergency telecommunications for Texas border cities and the model components.

To organize the findings, this chapter is divided into two sections—the results obtained from the survey and the findings obtained from the analysis of the basic emergency management plans and Annex B. Additionally, each section compares and contrasts the findings for each ideal element, e.g. interoperability, survivability, security, and international connectivity, which demonstrate the assessment of each model component against the status quo**.**

Survey Results

The findings suggest that Brownsville, Del Rio, Eagle Pass, El Paso, Laredo, and McAllen are taking steps to ensure some level of preparedness in the event of a man-made or natural disaster. When asked about emergency management planning efforts, 82 percent of respondents surveyed said that their city or county had developed emergency management plans.

Overall, the initial survey findings corroborate the importance of telecommunication infrastructure for emergency response efforts as observed by Houck et al. in Chapter 3. Sixty-nine percent (69%) of respondents acknowledged the inclusion of emergency telecommunications in their city or county's overall emergency management plan. Additionally,

the majority (82%) of respondents surveyed said that their city or county currently utilizes telecommunications for emergency response efforts.

But the survey findings also agree with the assessment by Andrew and Petkov in Chapter 3 that telecommunications has not been prioritized as critical infrastructure by cities, which is important in achieving a high-level of emergency preparedness. When asked to assess their city or county's current emergency telecommunication infrastructure, only 40 percent of respondents felt that current emergency telecommunication capabilities met the needs of their city or county for major emergency response activities. For minor emergencies, approximately 3 out of 4 (76%) respondents felt that current emergency telecommunication capabilities met the needs of their city or county. A copy of the survey results can be found in Appendix B.

Interoperability

Interoperability is the first component of the model emergency telecommunication architecture for effective cross-border emergency response. The findings are in line with the literature, that interoperability is important for effective emergency response as argued by Balachandran et al., McGinity, Roane et al., Potter et al., Yuan and Detlor, Fischer, and Lake. The findings corroborate the review of the literature on this subject with over half (62%) of respondents acknowledging the importance of interoperability to their cities and counties. Additionally, a little over half (51%) of the respondents indicated that interoperability was referenced in their city or county's emergency management plan.

But the importance of interoperability does not necessarily translate into urgency as reflected by the less than half (46%) of respondents indicating that their city or county was currently interoperable. This finding is key because it demonstrates a low level of emergency telecommunication preparedness by Texas border cities.

The survey findings could not yield any clear assessment about the inclusion of *suitable technology* or *common frequencies and standards* in current emergency management plans from the respondents. The survey questions designed to assess suitable technology and common frequencies and standards in current emergency management plans were poorly written and as a result could not yield any usable data. What is clear are the overarching survey findings indicating that shared standards such as employing suitable technology (67%) and common frequencies (51%) and standards (61%) are important for achieving effective interoperability.

Survivability

Survivability is the third element of the model emergency telecommunication architecture. The survey findings do not necessarily corroborate the literature because the survey failed to assess the respondent's opinion on survivability. Additionally, the survey findings could not yield any clear assessment about the inclusion of survivability as a component of current emergency management plans because 54 percent of the respondents indicated that they did not know if survivability was a component of their city or county's emergency management plan.

Moreover, when respondents were asked if their city or county's telecommunication network employed *diversity* to increase the probability of emergency telecommunication survivability, the majority of respondents (77%) did not know. Similarly, 74 percent of the respondents did not know if their city or county's emergency telecommunication networks were *separated*, 72 percent did not know if their city or county's telecommunication networks were constructed away from potential vulnerable targets (*avoidance*), and 77 percent did not know if their city or county's telecommunication networks were *hardened*, e.g. constructed with materials able to withstand disasters.

Similarly, the survey findings did not yield any clear results when gauging the importance of the four sub-elements. As a result the survey findings could not corroborate the review of the literature. When asked to provide their opinion on the importance of *diversity* for telecommunication survivability, over half of the respondents (56%) did not know if diversity was important for emergency telecommunication survivability. Approximately 54 percent of the respondents did not know if *separation* was important for emergency telecommunication survivability. Sixty percent (60%) of the respondents did not know if *avoidance* was important for emergency telecommunication survivability. But 54 percent of respondents did say that *hardening* of telecommunication networks was important to ensure survivability of emergency telecommunication networks.

The reason for the lack of clear data is not known. However, the lack of precise or technical knowledge may be a reason. But the findings do yield some other important data indicating the importance of ensuring telecommunication survivability. Although the survey finds that only a small percentage (21%) of respondents recall telecommunication failures affecting their city or county's ability to respond to an emergency, this finding underscores some level of cascading impacts resulting from telecommunication failures. As a result, this data defends Baker et al., Grubesic and Murray, Houck et al., Krock, and Lake's argument that telecommunication survivability is key for emergency response.

Security

Security is the third component of the model emergency telecommunication architecture for effective cross-border emergency response. The survey findings do not necessarily corroborate the literature on security because 62 percent of respondent did not know if telecommunications security was addressed in their city or county emergency management plan.

Similarly, 62 percent did not know if telecommunication security breaches had ever affected their city or county's emergency response efforts.

But the survey findings do show that improvements are needed in telecommunication security. When asked about their city or county's telecommunication infrastructure, 43 percent of respondents felt it was somewhat secure.

International Connectivity

International connectivity is the fourth component of the model emergency telecommunication architecture for effective cross-border emergency response. The survey findings for international connectivity are mixed. While the survey results show that the majority (69%) of the respondents surveyed do not know if international connectivity is addressed in their city or county's emergency management plan, the findings also show that a quarter (25%) of the respondents indicate that their city or county has identified cross-border emergency telecommunications as a public safety concern.

But the survey findings do show some promise in the area of international connectivity for cross-border emergency response. While less than a quarter (21%) of respondents indicate that their city or county has previously responded to a cross-border emergency, the research also shows that 44 percent of respondents consider the possibility of cross-border emergencies occurring in their city or county because of their geographical location along the Texas-Mexico border. Additionally, 46 percent of respondents believe that the ability to effectively communicate with Mexican partners during a cross-border emergency is important.

The survey findings for international connectivity may be mixed because a major cross-border emergency event has yet to occur in the Texas-Mexico border region. Another reason may be attributed to the majority of respondents (71%) not knowing if their Mexican partners

would embrace emergency telecommunications architecture designed for effective cross-border emergency response.

Document Analysis Results

Document analysis was the second research technique used to conduct the assessment of current emergency telecommunications for Texas border cities. The main purpose in conducting an analysis of emergency response plans is to determine the accuracy of the survey findings. An analysis of emergency management plans (e.g. basic emergency plan and Annex B) was conducted on 5 out of 6 cities that submitted documents, with the exception of Laredo who did not submit any documents.[10]

Overall, the document analysis support the survey findings that border cities have developed emergency management plans to ensure some level of emergency preparedness in the event of a man-made or natural disaster. This data is supported with the submittal of emergency management plans from Brownsville, Del Rio, Eagle Pass, El Paso, and McAllen, with the exception of Laredo.

It must be noted that the results obtained from the document analysis may be skewed because the request for emergency management plans submitted to the cities of Brownsville, Del Rio, Eagle Pass, El Paso, Laredo and McAllen specifically requested copies of their basic emergency plan and Annex B from the list of standardized local planning documents in Chapter 4 (See Figure 4.1). Despite the open records request to all six cities, only 5 cities submitted. Additionally, the response to the request was mixed because out of the 5 cities who submitted copies only 1 submitted both sets of the documents requested. The other cities submitted only of the documents. A copy of the document analysis results can be found in Appendix C.

[10] An open records request was submitted to all cities being assessed, including the City of Laredo. However, the City of Laredo failed to respond to the open records request. Several follow-up attempts were made via e-mail and telephone to several city officials with no success.

Interoperability

Overall, review of the emergency management plans somewhat support the survey findings that interoperability is included in the majority of emergency management plans. Only 3 out of 5 cities who submitted emergency management plans referenced interoperability in their basic emergency operations plan. The basic emergency operations plan for Brownsville (BP-7) and El Paso (BP-8) indicate that they have adopted "the National Incident Management System[11]…NIMS allows us to integrate our response activities using a set of standardized organizational structures designed to improve interoperability between all levels of government, private sector, and nongovernmental organization."

Additionally, Del Rio's basic emergency operations plan essentially calls for the development of interoperable communications for emergency response but does not concretely indicate the status of those plans. Although it does not specifically use the term interoperability, Del Rio's (BP-14) basic emergency operations plan specifically delegates responsibility for "developing plans and procedures for coordinated use of the various communications systems available in this jurisdiction during emergencies," to the police chief.

Similar to the survey results, the document analysis could not yield any direct or indirect references concerning the use of suitable technology and common frequencies and standards to enhance interoperability in any of the basic emergency operation plans or Annex B.

Survivability

While the survey findings indicate that respondents do not know if survivability is a component included in their city or county emergency management plans, review of the

[11] NIM is a standardized approach to emergency management and response developed by the Office of Homeland Security. NIMS provides guidance on emergency planning, preparedness, and response activities, procedures, equipment, information management, records retention, etc.

submitted emergency management plans indicate that 2 out of the 5 Texas border cities referenced survivability in their emergency management plans. The two cities are Del Rio and Mc Allen.

The basic emergency operations plan and Annex B for the City of Del Rio do not reference survivability directly; however, Annex B mandates the protection of radio and telephone communications.

Annex B specifically details preventative steps to protect radio communications against two possible scenarios, electromagnetic pulse (EP) from nuclear detonation or lightning, wind, and blast. In the event of an electromagnetic pulse, the plan calls for "the disconnection of radios from antennas and power source when an Attack Warning is issued. A portable radio unit will then be employed as a backup to maintain limited communications with field units. This procedure will be used until an All Clear is announced. Telephones will also be used while operable" (B-7, B-8). Similarly, the plan for protecting radio communications from lightning, wind, and blast advises that "Standard lighting protection is used including arrestors and the use of emergency power during severe weather. Damaged antennas can possibly be replaced with spare units kept in the Radio Maintenance Division. Mobile repeaters can be utilized to resume radio communications in the event of damage to radio towers" (B-7).

Telephone protection is also mandated in Annex B for Del Rio against overloaded circuits and emergency services. In the event that telephone circuits become overloaded, the plan provides that "citizens will be advised to listen to EAS[12] for information and to use telephones only if they have a genuine emergency. If overloaded circuits do become a problem, coordinate with Verizon Telephone Company to begin immediate restoration of priority circuits.

[12] EAS is an acronym for Emergency Alert System.

Similarly during disasters or emergencies, the plan explains that "a direct line to the Verizon Telephone Office is activated in the EOC[13] for emergency service calls"(B-7).

Annex B for McAllen specifically references survivability as a key component of their emergency telecommunications system. McAllen's communications annex specifically mandates the McAllen Police Department to "Develop an adequate survivable communications system," as part of their emergency management mitigation phase (B-2). However, Annex B does not provide any information detailing what "an adequate survivable communications system" should include.

Similar to the survey results, the document analysis did not yield any direct or indirect references to diversity, separation, avoidance, or hardening to enhance interoperability in any of the basic emergency operation plans or Annex B.

Security

The review of emergency management plans support the survey findings. Survey results indicate that the majority of respondents (38%) do not know if security is a component included in their city or county emergency management plans. Document analysis shows that 2 out of 5 emergency management plans reference telecommunications security for secure voice and data transmission. The two cities whose emergency management plans reference telecommunications security are Del Rio and Mc Allen.

Annex B for Del Rio specifically designates a section to the issue of security. But the security section of Annex B only focuses on security issues for Del Rio's Dispatch/Communications Center providing access only to authorized personnel (B-7). Similarly, Annex B for McAllen only focuses on security issues for their Emergency Operations Center, which ensures that only authorized personnel have access (B-7).

[13] EOC is an acronym for Emergency Operations Center.

International Connectivity

The analysis of emergency management plans for each of the Texas border cities being assessed are in line with the survey findings. While the survey findings indicated that the majority of respondents do not know if international connectivity was a component discussed in their city or county's emergency management plans, the analysis of emergency management plans corroborates the lack of international connectivity as an important component of cross-border emergency response and emergency telecommunications.

Chapter Summary

This chapter reported the results of the survey findings and document analysis. It provided an in depth analysis of the survey results against the literature. Additionally, it compared and contrasted emergency plans to determine if the document analysis corroborated the survey results.

CHAPTER 6: CONCLUSION

Research Summary

Overall, the survey and document analysis findings suggest that Brownsville, Del Rio, Eagle Pass, El Paso, Laredo, and McAllen have taken steps to develop some level of emergency telecommunications preparedness through the development of standardized local documents. But the findings also suggest that additional enhancements are required to the standardized local documents for Brownsville, Del Rio, Eagle Pass, El Paso, Laredo, and McAllen, specifically Annex B.

It must be noted that the findings may not necessarily provide an accurate assessment of the current emergency telecommunication infrastructure for effective cross-border emergency response for Texas border cities. Because the survey response rate of 18 percent is lower than the recommended 50 percent, biases or inaccurate assessments may result. Additionally, the assessment may be inadvertently skewed because the response for emergency management plans submitted by the cities of Brownsville, Del Rio, Eagle Pass, El Paso, Laredo and McAllen was mixed with cities only submitting one, both, or none of the documents.

The assessment based on the four ideal elements for both the survey and document analysis is clear. The clarity of the results may stem from the fact that definitions for each of the four ideal elements were included in the actual electronic survey. But the assessment based on the sub-elements does not provide any valuable information because the majority of responses fell in the “don’t know” category. While this data can be interpreted to mean that the respondent did not know how to respond, it can also be interpreted to mean that perhaps the respondent did not know the meaning of the sub-elements, or it can be interpreted to mean that because of the sensitivity and specificity of the questions being asked in the survey that the respondent selected

"don't know" as a response to detract from having to provide sensitive information. Table 6.1 highlights the overall results from the survey and document analysis.

Table 6.1 ***Summary of Texas Border City Emergency Telecommunications Assessment***

Ideal Categories	Survey	Document Analysis
INTEROPERABILITY	Supports	Somewhat Support
• **Suitable Technology**	Don't Know	Does Not Support
• **Common Frequencies**	Don't Know	Does Not Support
• **Common Standards**	Don't Know	Does Not Support
SURVIVABILITY	Don't Know	Does Not Support
• **Diversity**	Don't Know	Does Not Support
• **Separation**	Don't Know	Does Not Support
• **Avoidance**	Don't Know	Does Not Support
• **Hardening**	Don't Know	Does Not Support
SECURITY	Don't Know	Does Not Support
INTERNATIONAL CONNECTIVITY	Don't Know	Does Not Support

The survey and document analysis are somewhat in line with the literature on interoperability, suggesting that Texas border cities have taken steps to develop and implement some level of interoperable emergency telecommunications. More importantly, it shows that interoperability is key for emergency response efforts to Texas border cities.

Conversely, the majority of the survey respondents did not know if survivability, security, and international connectivity were components of their city or county's emergency management plan or emergency telecommunication infrastructure. When assessing the respondent's interest in an emergency telecommunication architecture which incorporated all four ideal elements; interoperability, survivability, security, and international connectivity, 43 percent of respondents surveyed did not know if their city or county would be interested in emergency telecommunication architecture that included the four ideal elements and sub-elements. Additionally, 48 percent of the respondents did not know if interoperability, survivability, security, and international connectivity were essential components for effective cross-border emergency telecommunication architecture. Future research utilizing research techniques such

as interviews and focus groups may clarify responses, improve the quality of responses, and provide important answers to unanswered questions.

This chapter provides a summary of the results as they relate to the overall research purpose, which is to assess current emergency telecommunication infrastructure for effective cross-border emergency response for Texas border cities based on the four ideal elements. Table 6.2 highlights the overall assessment of current emergency telecommunication infrastructure for Texas border cities. To view the detailed finding of the survey and document analysis go to Appendix B and Appendix C.

Table 6.2 ***Summary of Ideal Elements for Effective Emergency Telecommunications***

Ideal Categories	Survey
INTEROPERABILITY	Support
• **Suitable Technology**	Support
• **Common Frequencies**	Support
• **Common Standards**	Support
SURVIVABILITY	Don't Know
• **Diversity**	Don't Know
• **Separation**	Don't Know
• **Avoidance**	Don't Know
• **Hardening**	Don't Know
SECURITY	Don't Know
INTERNATIONAL CONNECTIVITY	Don't Know

The cascading effect theory suggests that the most unpredictable and inconsequential events can have a reverberating and unpredictable impact on the most seemingly unconnected systems. The most widely used illustration of the cascading effect theory can be found in the example of the butterfly that flutters its wings irregularly setting off unforeseen weather patterns half way around the world. But in telecommunications unforeseen failures can inadvertently impact other unseeming infrastructure critical to the well-being of any community or nation,

especially when responding to a man-made or natural disaster as exhibited in the World Trade Center attacks in 2001 and the failed Hurricane Katrina evacuations in September 2005.

The fact that two-thirds of the U.S.-Mexico border is in Texas provides reason enough in understanding that Texas may be susceptible to cross-border emergencies. As a result, contingencies for Texas border cities and counties must be developed and implemented to enable them to efficiently and effectively coordinate resources and emergency response efforts with the ultimate goal of preventing and minimizing any loss of life.

Recommendations

The havoc that telecommunication failures can wreak on business, government, and human life is catastrophic. In short, the following recommendations are made:

1. Develop and implement interoperability guidelines and standards.
2. Develop and implement emergency telecommunication network survivability and security guidelines.
3. Engage cross-border partners in dialogue to develop and implement emergency telecommunication architecture with international connectivity components.

Table 6.3 ***Texas Border City Emergency Telecommunications Recommendations Summary***

Ideal Type Categories	Evidence Supports	Recommendation
INTEROPERABILITY • Suitable Technology • Shared Standards • Common Frequencies	Yes Yes Yes Yes	• Provide comprehensive guidelines and standards based on best practices to achieve greater interoperability for emergency response during minor and major disaster events to include in Annex B.
SURVIVABILITY • Diversity • Separation • Avoidance • Hardening	Somewhat No No No No	• Conduct vulnerability assessments based on telecommunication network diversity, separation, avoidance, and hardening to develop highly survivable networks. • Develop telecommunication network guidelines to ensure survivability based on diversity, separation, avoidance, and hardening guidelines to include in Annex B.
SECURITY	No	• Conduct security vulnerability assessments. • Develop and implement telecommunication security guidelines. • Ensure contracts with telecommunications providers include telecommunication security guidelines.
INTERNATIONAL CONNECTIVITY	No	• Engage cross-border partners in dialogue about international connectivity necessary for international connectivity • Conduct feasibility study with cross-border partners for international emergency telecommunications architecture. • Develop, deploy, and conduct table top exercises for various cross-border emergency scenarios based on vulnerabilities or threats detailed in emergency management plan to include international emergency telecommunications connectivity

Suggestions for Future Research

Due to time constraints and low survey response this research was not able to fully compare and contrast the responses between each city or county assessed and the findings between the different sub-groups of the larger target population.

Future studies should focus on each Texas border city as individual units to obtain a deeper understanding of the different levels of preparedness between border cities. Additionally, future research should compare and contrast the differences in opinions between specific sub-groups of the larger target population to determine attitudinal differences. Lastly, focus groups and face-to-face interviews are recommended to provide for any future research on this subject. Face-to-face interviews and focus group research will allow researchers to directly ask questions to respondents and allow for assessment of responses to include observed behavior as a result of the questions posed, but more importantly, it will allow researchers to clarify on responses and allow participants to clarify questions which they may not understand.

Bibliography

Andrew, T.N. and D. Petkov. 2003. The need for a systems thinking approach to the planning of rural communications infrastructure. *Telecommunications Policy* 27: 75-93.

Auerswald, Phillip, Lewis M. Branscomb, Todd M. LaPorte, and Erbann Michel-Kerjan. 2005. The challenge of protecting critical infrastructure. *Issues in Science and Technology* Fall: 77-83.

Babbie, Earl. 2004. *The Practice of Social Research,* 10th ed. United States: Wadsworth/Thomson Publishing.

Baker, Mark C., Charles A. Witschorik, Jonathan C. Tuch, Waverly Hagey-Espie, and Veena B. Mendiratta. 2004. Architectures and disaster recovery strategies for survivable telecommunications services. *Bell Labs Technical Journal* 9(2): 125-145.

Balachandran, Krishna, Kenneth C. Budka, Tewfik L. Doumi, and Joseph H. Kang. 2004. Third-generation wireless services for homeland security. *Bell Labs Technical Journal* 9(2): 5-21.

Berghel, Hal and Jacob Uecker. 2004. Wireless infidelity: Airjacking. *Communications of the ACM* 47(12): 15-20.

Beroggi, Giampiero E.G. and William Wallace. 1995. Real-time decision support for emergency management: An integration of advanced computer and communications technology. *Journal of Contingencies and Crisis Management* 3(1): 18-25.

Cannon, Carl M., , David Baumann, Corine Freedber Jr., Brian Friel, Sydney J. Harris, David Hegland, Kellie Lunley, Neil Munro, Shane Serafini, Paul Singer, Bruce Strokes, and Marilyn Werber, Learning from mistakes, *National Journal* September 10, 2005, Vol. 37, Issue 37. http://web25.epnet.com.libproxy.txstate.edu/citations.asp?tb=1&_ug=sid+1164A092%2

Chambers, Michael D. and Douglas H. Riley. 2004. Implementing wireless priority services for CDMA networks. *Bell Labs Technical Journal* 9(2): 23-36.

City of Brownsville. Texas. *Basic Emergency Operations Plan*.

City of Del Rio. Texas. *Annex B, Communications*.

City of Del Rio. Texas. *Emergency Management Plan*.

City of Eagle Pass/Maverick County. Texas. *Annex B, Communications.*

City of McAllen. Texas. *Annex B, Communications*.

County of El Paso, Cities of Anthony, Clint, El Paso, Horizon, Socorro, and Vinton. *Emergency Management Plan.*

Ecklund, Carl, Jarmo T. Mäkiinen, Tero Ojanperä, and Juan Pihlaja. 2001. IP optimized broadband wireless access. *Journal of High Speed Networks* 10: 7-17.

Fischer, Henry W. 1996. What emergency management officials should know to enhance mitigation and effective disaster response. *Journal of Contingencies and Crisis Management* 4(4): 208-217.

Goodno, James B. 2005. Saying no to sabotage. *Planning* 17(7): 10-15.

Gravetter, Frederick J. and Larry B. Wallanau. 2004. *Behavioral Sciences,* 6th ed. Belmont: Wadsworth/Thomson Learning.

Grubesic, Tony H. and Alan T. Murray. 2005. Spatial-historical landscapes of telecommunication network survivability. *Telecommunication Policy* 29: 801-820.

Hinton, Danielle, Thierry E. Klein, and Mark Haner. 2005. An architectural proposal for future wireless emergency response networks with broadband services. *Bell Labs Technical Journal* 10(2): 121-138.

Houck, David J, Eunyoung Kim, Gerard P. O'Reilly, David D. Picklesimer, and Huseyin Uzunalioglu. 2004. A network survivability model for critical national infrastructures. *Bell Labs Technical Journal* 8(4): 153-172.

Hoyt, K. Sue, Jack Potter, and Thomas E. Wheeler. 2004. Introduction: A vision for 21st century emergency response communications. *Topics in Emergency Medicine* 26(2): 83-85.

Jackson, Bruce. 1999. Mobile satellite communications: The next step in prehospital care? *Topics in Emergency Medicine* 21(1): 9-25.

Jebara, K. Ben. 2004. Surveillance, detection and response: Managing diseases at national and international levels. *Rev. Sci. Tech Off. Int. Epiz.* 23(2): 709-715.

Jeffers, Rachel. 2003. *Development sprawl in Texas.* Texas State University: MPA Applied Research Project.

Jrad, Ahmad, Thomas Morawski, and Louise Spergel. 2004. A model for quantifying business continuity preparedness risk for telecommunication networks. *Bell Labs Technical Journal* 9(2): 107-123.

Kegley, Charles W. and Eugene R. Witkopf. 1995. *World Politics. Trends and Transformation.* 5th ed. New York, NY: St. Martin's Press.

Krock, Richard E. 2004. Effective quality control during disaster recovery. *Bell labs Technical Journal* 9(2): 163-171.

Lake, Timothy. 2004. *Reliable and relevant National Communications System.* U.S. Army War College: Master's Thesis.

LaPorte, Todd M. 1999. Contingencies and communications in cyberspace: The World Wide Web and non-hierarchical coordination. *Journal of Contingencies and Crisis Management* 7(4): 215-224.

Malone, Bernard. 2004. Wireless search and rescue: Concepts for improved capabilities. *Bell Labs Technical Journal* 9(2): 37-49.

Mayer-Schönberger, Viktor. 2002/2003. Emergency communications: The quest for interoperability in the United States and Europe. *International Journal of Communications Law and Policy* 7: 1-47.

Mayer-Schönberger, Viktor. 2005. The politics of public safety communication interoperability regulation. *Telecommunications Policy* 29: 831-842.

McGinity, Meg. 2004. Weaving a wireless safety net. *Communications of the ACM* 47(9): 15-18.

Michel-Kerjan, Erwann. 2003. New challenges in critical infrastructure: A US perspective. *Journal of Contingencies and Crisis Management* 11(3): 132-141.

Nagaratnam, N., Nadalin A., M. Hondo, M. McIntosh, and P. Austel. 2005. Business-driven application security: From modeling to managing secure applications. *IBM Systems Journal* 44(4): 847-867.

Olson, Debra, Christopher Atchison, Aggie Leitheiser, Susan Larson, and Cassandra Homzik. 2005. Public health and terrorism preparedness: Cross-Border issues. *Public Health Reports* Supplement 1, 120: 76-83.

Perry, Rick. 2005. Border Security Plans. http://www.governor.state.tx.us/priorities/other/border_security.

Potter, Jack M.D., Lynn Miller, Gary DuBrueler, and Amy E. DuBrueler. 2004. Interoperability now. Integrating emergency communications and information. A Virginia case study. *Topics in EmergencyMedicine* 26(2): 176-180.

Potter, Jack, David Aylward, Dale Hatfiled, and Sukumr Dwarkanath. 2004. Architecture and principles of a modern integrated emergency medical information network. *Topics in Emergency Medicine* 26(2): 103-109.

Quirk, Michaela D. and Steven J. Fernandez. 2005. Infrastructure robustness for multiscale critical missions. *Journal of Homeland Security and Emergency Management* 2(2): 1-24/

Rauscher, Karl F. 2004. Protecting communications infrastructure. *Bell Labs Technical Journal* 9(2): 1-4.

Roane, Kit R., Edward T. Pound, and Chitra Ragavan. 2004. Execuse me, can we talk? http://80web25.epnet.com.libproxy.txstate.edu/citation/asp?tb=1&_ug=sid+1164A092%2

Salis, Barry. 2003. First responders. Problems and Solutions: Communications. *Technology in Society* 25: 529-534.

Sawyer, Steve, Andrea Tapia, Leonard Pesheck, and John Davenport. 2004. Mobility and the first responder. *Communications of the ACM* 47(3): 62-65.

Shields, Patricia. 1998. Pragmatism as philosophy of science. A tool for public administration. *Research in Public Administration* 4: 199-230.

Texas Commission on Environmental Quality. Pollution Prevention Along the Border. http://www.tceq.state.tx.us/assistance/P2Recycle/border/border.html.

Texas Department of Public Safety. Division of Emergency Management. *Local Emergency Management Planning Guide*. ftp://ftp.txdps.state.tx.us/dem/plans/dem_10.pdf.

Yuan, Yufei and Brian Detlor. 2005. Intelligent mobile crisis response systems. *Communications of the ACM* 48(2): 95-98.

Appendix A – Survey Instrument

The following survey was distribute to 346 respondents via the website http://www.advancesurvey.com/

#	SURVEY QUESTION
1	Please select the border city or county you currently work for or represent? ☐ Brownsville ☐ Del Rio ☐ Eagle Pass ☐ El Paso ☐ Laredo ☐ McAllen ☐ Other (Please exit survey)
2	From the groups below, please select the one which best describes your position for the city/county which you work for or represent? ☐ Federal/State Elected Official (State Legislator, U.S. Senator, Congressman, Congresswoman) ☐ State Agency Head (Executive Director, Commissioner, etc.) ☐ County Official (County Judge, etc.) ☐ County Employee – General ☐ City Official (Mayor, City Council, City Commissioner, City Manager, etc) ☐ City Employee - General ☐ Public Works ☐ Fire ☐ EMS ☐ Police/Sheriff ☐ Other
3	In 2003, President Bush identified 13 national critical infrastructure requiring protection from internal and external threats, e.g. food, water, agriculture, public health, emergency services, government, telecommunications, defense, energy, transportation, banking and finance, chemical industry, and postal shipping. How would you rank telecommunications to other infrastructure (1 being the highest and 13 the lowest priority)? ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ 11 ☐ 12 ☐ 13
4	Does your city or county have an emergency management plan? ☐ Yes ☐ No ☐ Don't Know
5	Does your city or county emergency management plan include a telecommunications section or reference telecommunications for effective emergency response? ☐ Yes ☐ No ☐ Don't Know
6	Does your city or county currently use telecommunications for emergency response? ☐ Yes ☐ No ☐ Don't Know
7	In your opinion, do current telecommunication capabilities meet the needs of your city or county for MINOR emergency response activities? ☐ Yes ☐ No ☐ Don't Know
8	In your opinion, do current emergency telecommunications capabilities meet the needs of your city or county for MAJOR emergency response activities? ☐ Yes ☐ No ☐ Don't Know
9	Is telecommunications interoperability a component of your city or county emergency management plan? ☐ Yes ☐ No ☐ Don't Know
10	Does your city or county currently have interoperable telecommunication capabilities for emergency response? ☐ Yes ☐ No ☐ Don't Know
11	How important is interoperability for emergency response to your city or county? ☐ Important ☐ Somewhat Important ☐ Somewhat Unimportant ☐ Unimportant ☐ Don't Know
12	Is employing the latest most suitable technology important to your city or county in achieving interoperability? ☐ Yes ☐ No ☐ Don't Know
13	Do you consider different radio bands/frequencies a problem to achieving interoperability for your organization? ☐ Yes ☐ No ☐ Don't Know
14	Does your city or county consider the use of different telecommunications technology a problem to achieving interoperability? ☐ Yes ☐ No ☐ Don't Know
15	How important are shared telecommunication standards to your city or county for effective interoperability? ☐ Very Important ☐ Somewhat Important ☐ Not Very Important ☐ Don't Know
16	How important are common telecommunication frequencies and networks to your city or county for effective interoperability? ☐ Very Important ☐ Somewhat Important ☐ Not Very Important ☐ Don't Know
17	Is telecommunications survivability a component of your city or county emergency management plan? ☐ Yes ☐ No ☐ Don't Know
18	Have telecommunication failures affected your city or county's ability to respond to an emergency? ☐ Yes ☐ No ☐ Don't Know

19	Do you believe that having a diverse set of interconnecting routes on a telecommunications network would increase the probability of network survival in a disaster? ☐Yes☐No☐Don't Know
20	Is your city or county telecommunications network designed with a diverse set of interconnecting routes to increase the probability of network survival during a disaster? ☐Yes☐No☐Don't Know
21	Do you believe that separation between existing and new telecommunication network paths would reduce the risk of both routes being damaged or destroyed by a single disaster? ☐Yes☐No☐Don't Know
22	Is your city or county telecommunications network designed with separated network paths between existing and new networks to ensure survivability? ☐Yes☐No☐Don't Know
23	Do you believe that the construction of telecommunication network routes should avoid potential targets or vulnerable areas, such as major cities or government installations to ensure survivability? ☐Yes☐No☐Don't Know
24	Are your city or county telecommunication network routes near potential targets or vulnerable areas? ☐Yes☐No☐Don't Know
25	Do you believe that telecommunication networks should be constructed with materials that are able to withstand any disaster? ☐Yes☐No☐Don't Know
26	Are your city or county telecommunication networks constructed with materials that are able to withstand any disaster? ☐Yes☐No☐Don't Know
27	Has your city or county developed a telecommunications business continuity plan intended to assist in maintaining order and deliver minimum essential public services and emergency services in the event of a disaster? ☐Yes☐No☐Don't Know
28	Does your city or county emergency management plan include telecommunications security? ☐Yes☐No☐Don't Know
29	Have telecommunication security breaches ever affected the ability of your city or county to respond to an emergency? ☐Yes☐No☐Don't Know
30	How secure would you consider your city or county telecommunications infrastructure? ☐Very Secure ☐Somewhat Secure ☐Not Very Secure ☐Don't Know
31	Does your city or county emergency management plan include international connectivity? ☐Yes☐No☐Don't Know
32	Given your city and county geographical location along the Texas-Mexico border, do you agree that cross-border emergencies can occur? ☐Yes☐No☐Don't Know
33	Has your city or county identified cross-border emergency telecommunications as a public safety concern? ☐Yes☐No☐Don't Know
34	Do you believe that it is important for your city or county to have the ability to communicate with Mexican partners during a cross-border emergency? ☐Yes☐No☐Don't Know
35	Has your city or county ever responded to a cross-border emergency? ☐Yes☐No☐Don't Know
36	Is your city or county able to communicate with Mexican partners during emergencies? ☐Yes☐No☐Don't Know
37	Would your city or county be interested in emergency telecommunications architecture that incorporated interoperability, survivability, security, and international connectivity? ☐Yes☐No☐Don't Know
38	Would you agree with the statement that interoperability, survivability, security, and international connectivity are essential components for effective and robust border emergency telecommunications architecture?☐Completely Agree ☐Somewhat Agree ☐Somewhat Disagree ☐Completely Disagree ☐Don't Know
39	Do you believe that Mexican partners would embrace emergency telecommunications architecture designed for effective cross-border emergency response? ☐Yes☐No☐Don't Know

Appendix B – Survey Results

#	SURVEY QUESTION		RESPONSES							
			Brownsville	**Del Rio**	**Eagle Pass**	**El Paso**	**Laredo**	**Mc Allen**	**N (346)**	**% (61)**
1	Please select the border city or county you currently work for or represent?		**16**	**10**	**3**	**23**	**1**	**8**	**61**	**18**
2	From the groups below, please select the one which best describes your position for the city/county which you work for or represent?	Federal/State Elected Official (State Legislator, U.S. Senator, Congressman, Congresswoman)	1	1	0	0	0	1	**3**	**5**
		State Agency Head (Executive Director, Commissioner, etc.)	1	0	0	1	0	1	**3**	**5**
		County Official (County Judge, etc.)	2	0	0	0	0	1	**3**	**5**
		City Official (Mayor, City Council, City Commissioner, City Manager, etc)	1	3	0	3	0	0	**7**	**12**
		City Employee - General	6	0	1	10	1	0	**18**	**30**
		County Employee - General	0	1	0	1	0	1	**3**	**5**
		Public Works	0	0	0	0	0	0	**0**	**0**
		Fire	0	0	1	1	0	0	**2**	**3**
		EMS	2	2	1	2	0	4	**11**	**18**
		Police/Sheriff	1	1	0	0	0	0	**2**	**3**
		Other	2	2	0	5	0	0	**9**	**15**
3	In 2003, President Bush identified 13 national critical infrastructure requiring protection from internal and external threats, e.g. food, water, agriculture, public health, emergency services, government, telecommunications, defense,	1	5	2	2	4	0	3	**16**	**26**
		2	1	4	0	2	0	2	**9**	**15**
		3	7	1	0	4	0	0	**12**	**20**
		4	2	0	0	5	0	0	**7**	**12**
		5	0	1	0	4	0	0	**5**	**8**
		6	1	0	0	1	0	1	**3**	**5**
		7	0	0	0	2	0	0	**2**	**3**

			RESPONSES							
	energy, transportation, banking and finance, chemical industry, and postal shipping. How would you rank telecommunications to other infrastructure (1 being the highest and 13 the lowest priority)?	8	0	1	0	0	0	1	**2**	**3**
		9	0	0	0	0	1	0	**1**	**2**
		10	0	0	0	1	0	0	**1**	**2**
		11	0	0	0	0	0	1	**1**	**2**
		12	0	0	0	0	0	0	**0**	**0**
		13	0	1	1	0	0	0	**2**	**2**
4	Does your city or county have an emergency management plan?	Yes	15	9	2	16	1	7	**50**	**82**
		No	1	1	0	5	0	0	**7**	**12**
		Don't Know	0	0	1	2	0	1	**4**	**7**
5	Does your city or county emergency management plan include a telecommunications section or reference telecommunications for effective emergency response?	Yes	12	8	2	14	1	5	**42**	**69**
		No	4	2	0	5	0	1	**12**	**20**
		Don't Know	0	0	1	4	0	2	**7**	**12**
6	Does your city or county currently use telecommunications for emergency response?	Yes	11	10	2	21	0	6	**50**	**82**
		No	3	0	0	2	0	0	**5**	**8**
		Don't Know	2	0	1	0	1	2	**6**	**10**
7	In your opinion, do current telecommunication capabilities meet the needs of your city or county for MINOR emergency response activities?	Yes	13	8	2	16	1	6	**46**	**76**
		No	0	0	0	2	0	0	**2**	**2**
		Don't Know	3	2	1	5	0	2	**13**	**21**
8	In your opinion, do current emergency telecommunications capabilities meet the needs of your city or county for MAJOR emergency response activities?	Yes	8	1	0	10	1	4	**24**	**40**
		No	3	6	0	5	0	2	**16**	**26**
		Don't Know	5	3	3	8	0	2	**21**	**34**
9	Is telecommunications interoperability a component of your city or county emergency management plan?	Yes	5	9	2	10	1	4	**31**	**51**
		No	3	0	0	2	0	2	**7**	**12**
		Don't Know	9	1	1	10	0	2	**23**	**38**
10	Does your city/county currently have interoperable communication capabilities for emergency response?	Yes	5	7	2	10	0	4	**28**	**46**
		No	4	2	1	2	0	2	**11**	**19**
		Don't Know	7	1	0	11	1	2	**22**	**36**

			RESPONSES							
11	How important is interoperability for emergency response to your city or county?	Important	10	8	2	14	1	3	**38**	**62**
		Somewhat Important	1	1	0	3	0	3	**8**	**13**
		Somewhat Unimportant	2	1	0	1	0	0	**4**	**7**
		Unimportant	0	0	1	0	0	0	**1**	**2**
		Don't Know	3	0	0	5	0	2	**10**	**16**
12	Is employing the latest most suitable technology important to your city or county in achieving interoperability?	Yes	12	7	2	15	1	4	**41**	**67**
		No	1	2	0	1	0	1	**5**	**8**
		Don't Know	3	1	1	7	0	3	**15**	**25**
13	Do you consider different radio bands/frequencies a problem to achieving interoperability for your city or county?	Yes	5	6	0	8	0	1	**20**	**33**
		No	8	2	0	2	0	4	**16**	**26**
		Don't Know	3	2	3	13	1	3	**25**	**41**
14	Does your city or county consider the use of different telecommunications technology a problem to achieving interoperability?	Yes	3	8	0	6	0	2	**19**	**31**
		No	5	0	0	7	1	1	**14**	**23**
		Don't Know	8	2	3	10	0	5	**28**	**46**
15	How important are shared telecommunication standards to your city or county for effective interoperability?	Very Important	12	7	1	11	1	5	**37**	**61**
		Somewhat Important	0	3	1	4	0	1	**9**	**15**
		Not Very Important	0	0	1	1	0	0	**2**	**3**
		Don't Know	4	0	0	7	0	2	**13**	**21**
16	How important are common telecommunication frequencies and networks to your city or county for effective interoperability?	Very Important	10	7	0	8	1	5	**31**	**51**
		Somewhat Important	2	3	2	9	0	1	**17**	**28**
		Not Very Important	0	0	0	0	0	0	**0**	**0**
		Don't Know	4	0	1	5	0	2	**12**	**20**
17	Is telecommunications survivability a component of your city or county emergency management plan?	Yes	5	4	0	6	0	5	**20**	**33**
		No	1	2	1	3	0	1	**8**	**13**
		Don't Know	10	4	2	14	1	2	**33**	**54**
18	Have telecommunication failures affected your city or county's ability to respond to an emergency?	Yes	3	4	0	3	0	3	**13**	**21**
		No	3	5	1	7	1	3	**20**	**33**
		Don't Know	10	1	2	13	0	2	**28**	**46**
19	Do you believe that having a diverse set of interconnecting	Yes	6	5	1	9	1	4	**26**	**43**
		No	0	1	0	0	0	0	**1**	**2**

			RESPONSES							
	routes on a telecommunications network would increase the probability of network survival in a disaster?	Don't Know	10	4	2	14	0	4	**34**	**56**
20	Is your city or county telecommunications network designed with a diverse set of interconnecting routes to increase the probability of network survival during a disaster?	Yes	2	1	0	2	0	1	**6**	**9**
		No	1	2	0	2	0	3	**8**	**13**
		Don't Know	13	7	3	19	1	4	**47**	**77**
21	Do you believe that separation between existing and new telecommunication network paths would reduce the risk of both routes being damaged or destroyed by a single disaster?	Yes	4	7	0	9	1	6	**27**	**44**
		No	1	0	0	0	0	0	**1**	**2**
		Don't Know	11	3	3	14	0	2	**33**	**54**
22	Is your city or county telecommunications network designed with separated network paths between existing and new networks to ensure survivability?	Yes	2	4	0	2	0	2	**10**	**16**
		No	1	1	0	2	0	2	**6**	**10**
		Don't Know	13	5	3	19	1	4	**45**	**74**
23	Do you believe that the construction of telecommunication network routes should avoid potential targets or vulnerable areas, such as major cities or government installations to ensure survivability?	Yes	4	5	0	8	1	3	**21**	**34**
		No	1	1	0	0	0	2	**4**	**7**
		Don't Know	11	4	3	15	0	3	**36**	**60**
24	Are your city or county telecommunication network routes near potential targets or vulnerable areas?	Yes	2	1	0	5	0	3	**11**	**18**
		No	1	2	0	1	0	2	**6**	**9**
		Don't Know	13	7	3	17	1	3	**44**	**72**
25	Do you believe that telecommunication networks should be constructed with	Yes	6	8	1	11	1	6	**33**	**54**
		No	1	0	0	0	0	0	**31**	**51**

			RESPONSES							
	materials that are able to withstand any disaster?	Don't Know	9	2	2	12	0	2	**27**	**44**
26	Are your city or county telecommunication networks constructed with materials that are able to withstand any disaster?	Yes	0	0	0	0	0	1	**1**	**2**
		No	2	4	0	4	0	3	**13**	**21**
		Don't Know	14	6	3	19	1	4	**47**	**77**
27	Has your city or county developed a telecommunications business continuity plan intended to assist in maintaining order and deliver minimum essential public services and emergency services in the event of a disaster?	Yes	4	2	0	5	1	4	**16**	**26**
		No	0	2	0	2	0	0	**4**	**7**
		Don't Know	12	6	3	16	0	4	**41**	**67**
28	Does your city or county emergency management plan include telecommunications security?	Yes	3	4	0	6	0	3	**16**	**26**
		No	2	0	1	3	0	1	**7**	**12**
		Don't Know	11	6	2	14	1	4	**38**	**62**
29	Have telecommunication security breaches ever affected the ability of your city or county to respond to an emergency?	Yes	0	0	0	0	0	2	**2**	**3**
		No	5	7	1	4	1	3	**21**	**34**
		Don't Know	11	3	2	19	0	3	**38**	**62**
30	How secure would you consider your city or county telecommunications infrastructure?	Very Secure	2	2	0	3	0	1	**8**	**13**
		Somewhat Secure	6	7	1	8	1	3	**26**	**43**
		Not Very Secure	0	0	0	2	0	4	**6**	**9**
		Don't Know	9	1	2	9	0	0	**21**	**34**
31	Does your city or county emergency management plan include international connectivity?	Yes	1	2	0	0	0	1	**4**	**7**
		No	4	3	1	4	0	3	**15**	**25**
		Don't Know	11	5	2	19	1	4	**42**	**69**
32	Given your city and county geographical location along the Texas-Mexico border, do you agree that cross-border emergencies can occur?	Yes	4	6	1	11	1	4	**27**	**44**
		No	0	4	0	0	0	1	**5**	**8**
		Don't Know	12	0	2	12	0	3	**29**	**48**
33	Has your city or county identified crossborder emergency telecommunications as a public	Yes	3	4	0	5	0	3	**15**	**25**
		No	1	2	0	3	0	1	**7**	**12**
		Don't Know	12	4	3	15	1	4	**39**	**64**

			RESPONSES							
	safety concern?									
34	Do you believe that it is important for your city or county to have the ability to communicate with Mexican partners during a cross-border emergency?	Yes	4	6	1	11	1	5	**28**	**46**
		No	0	1	0	0	0	0	**1**	**2**
		Don't Know	12	3	2	12	0	3	**32**	**53**
35	Has your city or county ever responded to a cross-border emergency?	Yes	3	4	1	2	0	3	**13**	**21**
		No	1	3	0	7	0	2	**13**	**21**
		Don't Know	12	3	2	14	1	3	**35**	**57**
36	Is your city or county able to communicate with Mexican partners during emergencies?	Yes	2	5	0	5	0	2	**14**	**23**
		No	12	1	0	4	0	3	**20**	**33**
		Don't Know	3	4	2	14	1	3	**27**	**44**
37	Would your city or county be interested in emergency telecommunications architecture that incorporated interoperability, survivability, security, and international connectivity?	Yes	3	4	1	3	1	3	**15**	**25**
		No	1	1	0	0	0	1	**3**	**5**
		Don't Know	12	5	2	20	0	4	**43**	**71**
38	Would you agree with the statement that interoperability, survivability, security, and international connectivity are essential components for effective and robust border emergency telecommunications architecture?	Completely Agree	3	4	0	7	1	5	**20**	**33**
		Somewhat Agree	3	2	1	5	0	0	**11**	**18**
		Somewhat Disagree	0	1	0	0	0	0	**1**	**2**
		Completely Disagree	0	0	0	0	0	0	**0**	**0**
		Don't Know	10	3	2	11	0	3	**29**	**48**
39	Do you believe that Mexican partners would embrace emergency telecommunications architecture designed for effective cross-border emergency response?	Yes	2	2	0	2	1	2	**9**	**15**
		No	1	0	0	4	0	2	**7**	**11**
		Don't Know	14	8	1	18	0	4	**45**	**74**

Appendix C – Document Analysis Results

City	Basic Emergency Operations Plan (BP) or Annex B (B) (BP or B)	Indication of ideal element? (Yes/No)											
		Interoperability	**Suitable Technology**	**Shared Standards**	**Common Frequencies**	**Survivability**	**Diversity**	**Separation**	**Avoidance**	**Hardening**	**Security**	**International Connectivity**	**RESULTS**
Brownsville	BP	--	--	--	--	--	--	--	--	--	--	--	--
	B	**Y**	N	N	N	N	N	N	N	N	N	N	**N**
Del Rio	BP	**Y**	N	N	N	N	N	N	N	N	N	N	**N**
	B	N	N	N	N	**Y**	N	N	N	N	**Y**	N	**N**
Eagle Pass	BP	--	--	--	--	--	--	--	--	--	--	--	--
	B	N	N	N	N	N	N	N	N	N	N	N	**N**
El Paso	BP	**Y**	N	N	N	N	N	N	N	N	N	N	**N**
	B	--	--	--	--	--	--	--	--	--	--	--	--
Laredo	BP	--	--	--	--	--	--	--	--	--	--	--	--
	B	--	--	--	--	--	--	--	--	--	--	--	--
McAllen	BP	--	--	--	--	--	--	--	--	--	--	--	--
	B	N	N	N	N	**Y**	N	N	N	N	**Y**	N	**N**
TOTAL		**Y/N**	**N**	**N**	**N**	**N**	**N**	**N**	**N**	**N**	**N**	**N**	**N**