Preface

This book examines the impact of Homeland Security Information Systems (HSIS) on government. HSIS can be defined as technologies used in a national effort to prevent and respond to terrorist attacks and emergencies such as natural disasters. This book has included both the study of terrorist attacks and emergency management in its definition, since both are critical for protecting the homeland. This definition is different from the typical response by police, firefighter’s, and other first responders to emergencies since it involves a multi-jurisdictional and national effort. Therefore, the severity of the emergency requires a more coordinated effort across different levels of government than what one government can handle alone.

Some notable incidents of homeland security were the terrorist attacks of September 11, 2001 on the World Trade Center and the Pentagon and Hurricane Katrina that devastated large parts of the Gulf Coast in 2005. In these notable national disasters, the response to both of them were criticized because the different levels of government lacked adequate preparation and collaboration when responding to these incidents (Wise and Nader, 2002; Wise, 2006). This book provides knowledge of the impact and use of HSIS on all levels of government in the United States. The argument is made that in order to more successfully implement HSIS, one must understand its current impact on governments. This book through a collection of surveys of public officials, in all levels of government in the United States, provides an assessment of the degree of adoption of HSIS and its effectiveness on government.

This book makes a unique contribution through its examination of electronic government (or e-government) and homeland security preparedness research. This book melds both research themes to examine this important issue. What is especially noteworthy in this research is survey evidence presented in each of the chapters to provide baseline knowledge of what key officials in government think about HSIS and its impact on their government. The majority of the surveys were conducted by the author, with some other survey evidence provided by notable organizations such as the International City/County Management Association (ICMA) and Pew Internet and American Life Project.

Existing research on e-government focuses generally on its adoption in public sector organizations (Moon, 2002; West, 2004; Norris and Moon, 2005; Torres, Pina, and Acerete 2005; Melitski and Holzer, 2007). This book examines the development of e-government by focusing specifically on HSIS adoption at all levels of government in the United States. The purpose of this book is to outline the extent to which HSIS has impacted government. What this book does not do, is provide an elaborative discussion of all technologies available in homeland security, as other works cover that important dimension (Pine, 2006; Cutter, Emrich, and Adams, et al. 2007). The following section presents a chapter-by-chapter overview and plan for the book.
OVERVIEW OF THE BOOK

Section 1 of this book is a collection of three chapters that provides background information on homeland security preparedness, e-government and citizens, and collaboration and e-government. The message of this section is that one cannot understand the impact of HSIS on governments without understanding these three pillars that drive the implementation of HSIS.

Chapter 1 provides the reader with a knowledge base about some of the issues associated with homeland security preparedness. The focus on this chapter is the experiences of local governments in the realm of homeland security preparedness, since they are normally first on the scene if a natural disaster or terrorist incident occurs. This chapter identifies the important organizational, management, and collaborative elements that impact homeland security preparedness. There is a case study of information systems used in the response to Hurricane Katarina. After reading this chapter, the reader should be able to understand the salient issues in homeland security preparedness that governments face.

Chapter 2 provides research on how e-government is thought to create more citizen-centric government. Since HSIS is part of the e-government effort, it is important to know about the relationship between e-government and citizens, since citizens are thought to be one of the main determinates in the advancement and success of e-government. Many definitions of e-government include expanding outreach to citizens with their government because of power of the internet.

Chapter 3 provides an examination of collaboration and its impact on e-government. The purpose of this chapter is to discuss one of the most often cited and pressing issues in the realm of homeland security of collaboration and demonstrates how this is related to the e-government literature. It is essentially to know about the issues associated with collaboration, since it is the most common challenge that government face when preparing and responding to homeland security. This chapter examines some best practices of collaboration and shows how state governments measure up against some noted principles of collaboration.

The second section of this book has three chapters that examine the implementation of HSIS in the federal, state, and local governments. The chapters in this section provide evidence on the impact of HSIS on the different levels of government in the United States.

Chapter 4 provides details on the federal government, the largest purchaser of information technology in the world, and its use of HSIS. This chapter focuses on the impact of HSIS on federal departments and agencies through a survey of CIOs. This chapter covers the important pieces of federal legislation in HSIS and outlines the scope of its impact on Chief Information Officers (CIO) and their departments/agencies. The result of this chapter indicate that HSIS has significantly changed the roles and responsibilities of federal CIOs.

Chapter 5 examines the impact of IT on emergency management function through the key areas of emergency management, which are mitigation, preparedness, response, and recovery. The focus here is on state governments’ and their use of emergency management and IT. There is an examination of the impact of IT on emergency management planning efforts of state governments. The effectiveness of IT on various technologies used by emergency management departments is also assessed. Some of the barriers to the adoption of IT in emergency management are also discussed in this chapter.

Chapter 6 examines the impact of HSIS on local government, relative to other homeland security priorities. Some of the topics covered in this chapter are the assessment of the quantity and quality of information sharing from federal and state governments with local governments. There is a discussion of the financing of homeland security for local governments and where HSIS fits into local budget priorities. There is mention of the need for training in the area of local government HSIS.
The final section of this book examines some emerging issues in the realm of HSIS. These important issues faced by governments are citizens’ use of terrorism information for preparedness, information security, and assessment of information on emergency management websites.

Chapter 7 examines the impact of citizens’ use of the Internet and information on homeland security. The focus of this chapter is to assess why individuals go online for information, providing an assessment of the barriers to Internet access. There is a survey presented that shows citizens preferred methods of contacting government for information and how homeland security fits into their preferences for online information.

Chapter 8 examines the important issue of information security, with a focus on a survey from Texas state agencies. Information security is a top challenge and priority according to public and private sector CIOs. The results of this chapter give the reader information on the information security environment and the challenges that governments face in this post 9/11 world. Some of the issues discussed are the management and organizational culture and its impact on information security. There also is a discussion of the information security threats faced by government and strategies that they use to mitigate these threats.

Chapter 9 examines through a content analysis of state government emergency management websites some of the information that can be found on these websites to aid communities in preparation for an emergency. This chapter is used to provide a baseline of knowledge of the features that emergency management departments have placed on their websites, and to determine how effective this information is for their citizens and the communities that they serve.

Chapter 10 is the conclusion and provides a discussion of the main findings of the book. There also are some recommendations for future research on the implementation of HSIS in government.

HSIS is an important area of inquiry since information technology can have a tremendous influence on the preparation and response of government to a terrorist attack or natural disaster. This book will show that HSIS has pervaded many elements of preparedness and response in homeland security across all levels of government in the United States. It provides a baseline of knowledge through the use of surveys of public officials that are directly involved in homeland security preparedness efforts.

REFERENCES


