Book Review

Reviewed by Sukumar Ganapati, Florida International University, USA

Christopher Reddick
Homeland Security Preparedness and Information Systems: Strategies for Managing Public Policy
Information Science Reference (an imprint of IGI Global), Hershey, PA 2010

Dr. Christopher Reddick’s book, Homeland Security Preparedness and Information Systems: Strategies for Managing Public Policy, is a useful empirical analysis of the extent of information systems use in homeland security at the federal, state, and the local government levels. The author defines Homeland Security Information Systems (HSIS) as the “technologies used in a national effort to prevent and respond to terrorist attacks and emergencies such as natural disasters.” Drawing on surveys of public officials at all three levels of government, the book gives an assessment of the degree of adoption of HSIS and its effectiveness. The main contribution of the book is to integrate the two research themes of e-government and homeland security preparedness in order to provide baseline knowledge of the key officials’ attitudes and thinking. A central theme that recurs through the chapters of the book is the significance of organizational culture and management in the successful implementation of HSIS.

The book is organized in four sections, of which, the first three sections form the core substance (the fourth section comprises of selected readings from the author). The first section deals with a background on HSIS. In this section, Dr. Reddick identifies three key pillars in the implementation of HSIS: homeland security preparedness, citizen-centricity, and collaboration. Each of the three chapters in the section covers a pillar, drawing respectively on surveys of local government, federal government, and state government officials. The focus is on local governments for homeland security preparedness, since they are the first responders in an emergency event. In this, the main finding is that local governments do not have adequate funding for homeland security. However, local governments do have higher degree of cooperation with other levels of government. Local governments have a perception of low threat levels. With respect to citizen-centric e-government, the second chapter is an examination of the role and responsibilities of federal Chief Information Officers (CIOs). Unsurprisingly, security and privacy are the top concerns of the CIOs and managerial capacity.

DOI: 10.4018/jep.2010100107
is a key element of e-government implementation. The third chapter examines collaboration in e-government at the state level. Although collaboration exists among state agencies and some key stakeholders, citizen collaboration is not quite pronounced. These broad findings in the first section set a good background for the rest of the book.

The second section deals with the implementation of HSIS in federal, state, and local governments, with one chapter devoted to each level of government. The principal finding from federal CIOs is that HSIS has changed the CIOs’ roles and responsibilities, with IT/cyber security weighing heavily on them. The state level examination of the use of IT in emergency management shows that there is much scope for leveraging IT, but there are barriers such as digital divide in including citizens actively in emergency management. At the local government level, although the internet is viewed by citizens as the major source of information for specific routine issues (e.g. tax payments, benefits, etc.), internet is not the major source in the case of an emergency. Traditional news sources such as television are better for homeland security information. Overall, the second section provides evidence on the impact of HSIS implementation at all three levels of government.

The third section deals with the emerging issues in HSIS. In this section, the major issues faced by governments are identified. These issues include: citizens’ use of terrorism information to citizens, information security, and dissemination of terrorism information through government websites. Trust in government is a major factor for citizens to use online information from public agencies. Successful adoption of information security is conditional on an organizational culture that supports such an implementation. Websites are effective tools to communicate with citizens about emergency information, but states vary enormously in terms of their information dissemination (with states that have faced notable disasters being more e-government enabled than those that have not).

The chapters are well structured individually and empirically grounded, and some chapters include the relevant laws as appendices. Yet, attention to one major aspect could have strengthened the book for adoption by HSIS students and professionals. The three pillars of HSIS, homeland security preparedness, citizen-centricity, and collaboration, are taken as a given. The theoretical rationale for these three pillars is not explained. Although scholars are likely to agree with the premise of the three pillars, the theoretical exploration would have given a stronger intellectual basis for not only justifying the premise, but also for justifying why some other major considerations are left out. For example, institutional issues have been major impediments in furthering e-government. The individual chapters also show that these issues are relevant for HSIS at the local, state, and federal levels. The theoretical exploration could have indicated the place of institutions in the overall scheme of HSIS implementation. However, this does not reduce the usefulness of Dr. Reddick’s book as a primer to the field of HSIS.

Sukumar Ganapati is an Assistant Professor in the Public Administration department at Florida International University (FIU). His research mainly deals with the role of institutions in the urban context, particularly with respect to housing, community development, and information technology applications. He teaches the IT and E-government course at FIU.