Chapter 4
Federal Government Homeland Security Information Systems

INTRODUCTION

This chapter focuses on Homeland Security Information Systems (HSIS) in the federal government. One definition of HSIS, in the federal government, is the application of information technology to homeland security with the aim of detecting fragmented clues, assembling them as a puzzle, then using the information to stop a terrorist attack (Nunn, 2005). Nunn’s definition focuses on the use of information for data mining for deducing possible terrorist attacks and responses to these incidents. This chapter recognizes the importance of data analysis, but uses a broader definition of federal HSIS being the use of information systems to prepare for and respond to a terrorist attack or significant national emergency. This definition of HSIS covers the importance of data mining to discover how information fits together as pieces of the puzzle, but it also incorporates other elements of information technology (IT) that are used to respond and prepare for a national incident.

This chapter will first examine the Department of Homeland Security which has a tremendous influence over homeland security policy and information systems in the United States. There is an examination in this chapter of the environmental context of HSIS in the federal government, demonstrating some of the important pieces of legislation that have an influence in this area. This chapter discusses the roles and responsibilities of federal government Chief Information Officers (CIOs) to discern the scope of their responsibilities. A section of this chapter examines some principles of effective IT management in federal agencies. The final part of this chapter provides the results of a survey of CIOs in federal government departments/agencies to determine the influence of HSIS on their organizations.

DOI: 10.4018/978-1-60566-834-5.ch004
THE DEPARTMENT OF HOMELAND SECURITY

In the aftermath of the terrorist attacks of September 11, 2001, responding to potential threats to homeland security became one of the federal government’s most significant challenges (GAO, 2004a). To address this challenge, Congress passed and the President signed the Homeland Security Act of 2002 (GAO, 2008). This act merged 22 federal agencies and organizations into the Department of Homeland Security (DHS). One of the department’s most significant challenges was to integrate these 22 agencies and their IT organizations into a unified system.

In establishing the new DHS, Congress defined seven-point mission for the DHS.

- prevent terrorist attacks within the United States;
- reduce the vulnerability of the United States to terrorism;
- minimize the damage and assist in the recovery from terrorist attacks;
- carry out all functions of entities transferred to the department, including acting as a focal point regarding natural and man-made crises and emergency planning;
- ensure that the functions of the components within the department that are not directly related to securing the homeland are not diminished or neglected;
- ensure that the overall economic security of the United States is not diminished by efforts aimed at securing the homeland; and
- monitor connections between illegal drug trafficking and terrorism, coordinate efforts to sever such connections, and otherwise contribute to efforts to interdict illegal drug trafficking (GAO, 2004a).

The seven-point mission of the DHS requires that IT be adopted by this organization at each of these mission critical areas. For example, the prevention of a terrorist attack would involve looking at intelligence information and discerning patterns that predict a possible terrorist incident. Emergency planning would involve having the communications equipment to effectively communicate with first responders. Reducing the vulnerability of the United States could be done through data mining of information that terrorist might find useful to lodge an attack on the United States.

The Department of Homeland Security has the 10 principal organizations and their respective missions are shown in Table 1.

The DHS began operations in March 2003, and assumed operational control of about 209,000 civilian and military operations from 22 federal agencies. A simplified organizational chart for DHS is shown in Figure 1 (GAO, 2007).

The National Strategy for Homeland Security issued by President George W. Bush on July 16, 2002 has defined homeland security as “a concerted national effort to prevent terrorist attacks within the United States, reduce America’s vulnerability to terrorism, and minimize the damage, and recover from attacks that do occur.” (Office of Homeland Security, 2002, p. 2). The national strategy clearly recognizes the critical importance of information sharing through IT to prevent a future terrorist attack (Relyea, 2004). The National Strategy identified a plan to strengthen homeland security through the cooperation and partnering of federal, state, and private sector organizations on a number of functions (GAO, 2008).

President Bush’s National Strategy specifically addressed HSIS in the following passage (2002, p. xi):

www.igi-global.com/e-resources/library-recommendation/?id=1

Related Content

The Need for a National Data Breach Notification Law
www.igi-global.com/chapter/the-need-for-a-national-data-breach-notification-law/141046?camid=4v1a

Types of Terrorism
Gus Martin (2014). Exchanging Terrorism Oxygen for Media Airwaves: The Age of Terroredia (pp. 81-95).
www.igi-global.com/chapter/types-of-terrorism/106152?camid=4v1a

A Computer Network Attack Taxonomy and Ontology
www.igi-global.com/article/a-computer-network-attack-taxonomy-and-ontology/86073?camid=4v1a

The Open Definition of Cyber: Technology or a Social Construction?
www.igi-global.com/article/open-definition-cyber/64309?camid=4v1a