NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

CREATING A MIX OF SPOOKS AND SUITS: A NEW ROLE FOR INTELLIGENCE

by

Shawn P. Moyer

March 2003

Thesis Advisor:	Robert L. Simeral
Co-Advisor:	Robert E. Looney

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2003	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Creating a Mix of Spooks and Suits: A New Role for Intelligence			**5. FUNDING NUMBERS**
6. AUTHOR(S) Shawn P. Moyer			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT ***(maximum 200 words)***

The devastating events of 11 September 2001 demonstrated the United States no longer enjoys a sense of invulnerability to attacks on American soil. On 25 November 2002, President Bush signed legislation creating a Department of Homeland Security (DHS). The purposed of DHS is to solve intergovernmental coordination and resource allocation problems in an effort to prevent future terrorist attacks against America's homeland. The DHS transition team faces many questions and challenges. A major component of the new DHS requires a dedicated effort to monitoring, analyzing, and utilizing intelligence about domestic threats to national security. This thesis defines, describes, and advocates the role of intelligence in the proposed DHS. The role of intelligence in the new DHS is two-fold: 1) a process for the intergovernmental coordination of agencies involved in homeland security, and 2) a tailored, all-source fusion product to support DHS decision-makers. In addition, this thesis focuses on the major intelligence issues for the transition team tasked with creating an information and analysis assessment center within DHS. Defining the role of intelligence in the DHS and creating the means to accomplish this new role for intelligence is no easy task. Published proposals and ideas in general circulation provide a theoretical baseline of how DHS can accomplish this two-fold approach. In order to uncover the 'ground truth' data collection incorporated primary and secondary sources spanning across federal, state, and local intelligence and law enforcement communities. The thesis concludes with recommendations for how the DHS can accomplish this new role for intelligence. DHS policymakers must create a DHS intelligence organizational structure, manage the domestic intelligence process, establish an information-sharing network, incorporate the use of open source information (OSINT), and ensure an internal analytic capability. The time has come to create a mix of spooks and suits capable of preventing future terrorist attacks on American soil.

14. SUBJECT TERMS Intelligence, Homeland Security, Domestic Intelligence, Counter-Terrorism			**15. NUMBER OF PAGES** 129
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

CREATING A MIX OF SPOOKS AND SUITS: A NEW ROLE FOR INTELLIGENCE

Shawn P. Moyer
Lieutenant, United States Navy
B.S., United States Naval Academy, 1997

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN NATIONAL SECURITY AFFAIRS

from the

NAVAL POSTGRADUATE SCHOOL
March 2003

Author: Shawn P. Moyer

Approved by: Robert Simeral
Thesis Advisor

Robert Looney
Co-Advisor

James Wirtz
Chairman, National Security Affairs Department

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The devastating events of 11 September 2001 demonstrated the United States no longer enjoys a sense of invulnerability to attacks on American soil. On 25 November 2002, President Bush signed legislation creating the Department of Homeland Security (DHS). The new department's strategic objectives include: 1) preventing terrorist attacks within the United States, 2) reducing America's vulnerability to terrorism, and 3) minimize the damage and recover from the attacks that do occur. Intelligence will play a critical role in preventing future terrorist attacks against America's homeland. The DHS transition team faces many questions and challenges. A major component of the new DHS requires a dedicated effort to monitoring, analyzing, and utilizing intelligence about domestic threats to national security. This thesis defines, describes, and advocates the role of intelligence in the proposed DHS. The role of intelligence in the new DHS is two-fold: 1) a process for the intergovernmental coordination of agencies involved in homeland security, and 2) a tailored, all-source fusion product to support DHS decision-makers. Intelligence has emerged as the one common preventive measure applicable across the homeland security continuum. Defining the role of intelligence in the DHS and creating the means to accomplish this new role for intelligence is no easy task. Once defined, this thesis focuses on how DHS can accomplish this new role for intelligence. Published proposals and ideas in general circulation provide a theoretical baseline of how DHS can accomplish this two-fold approach. In order to uncover the 'ground truth,' data collection incorporated personal insight from experts spanning across federal, state, and local intelligence and law enforcement communities. The thesis concludes with recommendations for how the transition team tasked with creating an information and analysis assessment center within DHS. DHS policymakers must focus on creating an internal intelligence organizational structure, manage the country's domestic intelligence process, establish an information-sharing network, incorporate the use of open source information (OSINT), and ensure analytical quality within the new department. The time has come to create a mix of spooks and suits capable of preventing future terrorist attacks on American soil.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

A number of individuals and organizations were instrumental in helping complete this thesis. I wish to express my deepest appreciation to my thesis advisors, CAPT Robert Simeral and Dr. Robert Looney, their guidance throughout this project proved invaluable. Their meticulous attention to detail, professionalism, and encouragement allowed me take this project as far as my vision allowed. My sincere appreciation also goes to Stephen Marrin for helping me set my compass on the right course in the early goings. I would also like to thank my former intelligence curriculum officer CDR Stephen Recca, for encouraging me to "tackle the tough question" others shied away from.

Research for this thesis incorporated the inputs of civilian and military experts spanning across the intelligence and law enforcement communities. I cannot begin to list the number of individuals willing to provide inputs for my research so I would like to thank the Naval Intelligence Professionals (NIP) network for helping me tap into a diverse cadre of intelligence and law enforcement professionals. With NIP's help I was able to uncover the 'ground truth' about the role of intelligence in homeland security.

Most importantly, I wish to recognize my wife and best friend, Teresa. Without "my most prized possession", I would be worthless. One word captures it best, ALWAYS. To my son, Patrick, born alongside the waves of the Pacific, your face and smile calm any rough sea "da-da-da" encounters. Early in my life I learned with good fortune comes the carrying of many crosses. As long as we keep our faith in HIM, He will never give us more than we can handle.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

> Today we are taking historic action to defend the dangers of a new era. With my signature, this act of Congress will create a new Department of Homeland Security, ensuring our efforts to protect this country are comprehensive and united…This act takes the next critical steps in defending our country against the continuing threat of terrorism. The threat of mass murder on our own soil will be met with a united, effective response. (President George W. Bush during speech given on 25 November 2002, signing of the Homeland Security Act)[1]

> By 'intelligence', we mean every sort of information about the enemy and his country—the basis, in short, of our plans and operations. (Carl von Clausewitz, *On War*, 1832)[2]

A. PROTECTING THE HOMELAND

The devastating events of 11 September 2001 demonstrated the United States no longer maintains a sense of invulnerability to attacks on American soil. Protecting America's homeland requires new instruments of power. On 25 November 2002, President George W. Bush signed legislation creating the Department of Homeland Security (DHS). The creation of the DHS represents one of the most significant changes in the United States federal government since the National Security Act of 1947. DHS attempts to reorganize 22 previously disparate domestic agencies into a unified national homeland security entity. The DHS transition team, headed by Homeland Security Secretary Tom Ridge, faces many questions and challenges.

One area of concern for the new department is intelligence support. Intelligence will play a critical role in the nation's counterterrorist effort. The information analysis element within DHS will have the responsibility for monitoring, acquiring, and analyzing all-source intelligence about domestic threats from agencies within the intelligence and law enforcement communities. In addition, the DHS intelligence entity will rely on intelligence generated from state and local government agencies. As a consumer of

---

[1] "Homeland Security Agency a Reality," *MSNBC News*, 25 November 2002 (News Service On-Line); available from http://stacks.msnbc.com/news/8333668.asp.

[2] Carl von Clausewitz, *On War*, indexed ed., ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1976), 117.

intelligence, DHS will compete with other members of the national security community to ensure priority intelligence requirements are met.

Initially, this thesis defines the role of intelligence in the new Department of Homeland Security. Combining a detailed cross-section of primary and secondary sources uncovered the 'ground truth' about the newly defined role of intelligence in the DHS. Data collection incorporated the personal insights of civilian and military intelligence and law enforcement experts spanning across federal, state, and local levels. Defining the new role of intelligence in the DHS is no easy task. Numerous proposals and ideas in general circulation recommend solutions for DHS to accomplish the role of intelligence. Through an extensive description of current proposals and ideas, and the acquisition of first hand inputs from intelligence and law enforcement professionals tasked with homeland security responsibilities, this thesis defines the role of intelligence in the proposed DHS. Once defined, the thesis describes how DHS can accomplish this role. Lastly, this thesis advocates recommendations for DHS policymakers tasked with creating a new DHS intelligence entity. For the DHS to successfully accomplish the newly defined role of intelligence it must: 1) create an internal intelligence organizational structure, 2) effectively manage the domestic intelligence process, 3) establish an information-sharing network for federal, state, and local agencies, 4) incorporate the use of open source information (OSINT), and 5) ensure analytical quality within the DHS intelligence entity.

B. WHAT IS INTELLIGENCE?

1. Defining 'Intelligence'

Intelligence is a critical factor in preventing future terrorist attacks against the United States. However, definitions of intelligence vary. For example, Carl von Clausewitz states, "By 'intelligence' we mean every sort of information about the enemy and his country—the basis, in short, of our plans and operations."[3] Other experts emphasize the predictive nature of intelligence. Shlomo Gazit, Chief of Israeli Military Intelligence from 1974-1979 states,

> In antiquity (and to this day, in some countries) kings and generals used to act on the advice of diviners or fortunetellers. Not so the statesmen and

[3] Ibid., 117.

> army commanders of today. Nevertheless, they find it hard to accept a situation in which nobody can foretell the future for them. Many of them hope, or delude themselves, that the intelligence system serving them can fulfill this purpose.[4]

Intelligence is a workable concept. If this were a text on any other government function—defense, housing, transportation, diplomacy, agriculture—there would be little or no confusion about, or need to explain, what was being discussed.[5]

Before examining the role of intelligence in the proposed DHS, it is necessary to define the definition of "intelligence" used throughout this thesis. A review of various sources provided a workable definition of intelligence. *Joint Pub 1-02*, defines intelligence as "information and knowledge about an adversary obtained through observation, investigation, analysis or understanding."[6] *Naval Doctrine Publication 2: Naval Intelligence*, points out a clear distinction between information and intelligence. "Information is an assimilation of data that has been gathered, but not fully correlated, analyzed, or interpreted."[7] Intelligence results from the manipulation of information. "Intelligence is "the product resulting from the collection, exploitation, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries and areas."[8] Mark Lowenthal[9], in his book, *Intelligence: From Secrets to Policy* points out several ways to think about intelligence: intelligence as a process, intelligence as a product, and intelligence as an organization.[10] Robert David Steele[11], in

[4] Quoted *Joint Publication 2-0: Doctrine for Intelligence Support to Operations* (Washington, D.C.: Joint Chiefs of Staff, 09 March 2000) [publications on-line]; available from Joint Electronic Library, DTIC, http://www.dtic.mil/doctrine/jpintelligenceseriespubs.htm, I-1.

[5] Mark M. Lowenthal, *Intelligence: From Secrets to Policy* (Washington DC: Congressional Quarterly Press, 2000), 1.

[6] *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms* (Washington, D.C.: Joint Chiefs of Staff, 12 April 2001 [as amended through 09 January 2003]) [publications on-line]; available from Joint Electronic Library, DTIC, http://www.dtic.mil, 261.

[7] *Naval Doctrine Publication 2: Naval Intelligence* (Washington, D.C.: Department of the Navy, 1994), 4.

[8] Ibid.

[9] Mark M. Lowenthal has more than twenty-three years' experience in the executive and legislative branches of government as an intelligence official. He currently is an adjunct professor in the graduate programs at Columbia University and George Washington University and is a senior principal in the Intelligence Directorate of SRA International, Inc., where he is involved in a variety of projects in support of the U.S. intelligence community. Biographical information obtained from his book *Intelligence: From Secrets to Policy*.

[10] Lowenthal, 8.

an email exchange on the Naval Intelligence Professionals discussion forum, points out, "Intelligence is tailored decision-support, consisting of a process that leverages all available sources with the best available software and services to provide 'on target' intelligence answers—not necessarily products—that are generally actionable and always useful."[12] For purposes of this thesis intelligence is defined as *the process and product by which information, both classified and unclassified, is collected and analyzed to provide policy makers with tailored-decision support on national security issues*.

2. A New Domestic Role for Intelligence

Traditionally intelligence focused its efforts abroad. For example, before the fall of the Soviet Union, most intelligence agencies focused on containing the Soviet threat. In the 1990s, intelligence struggled with redefining the threats to the United States. The attacks on 11 September 2001 demonstrated the traditional foreign focus of intelligence no longer remains. Domestic intelligence is required to thwart future attacks launched by Al Qaeda and other groups hostile toward the United States. The United States requires a concerted effort in organizing domestic intelligence. The necessary components of homeland security intelligence, or concrete entities, have yet to formulate.

3. The Role of Intelligence in DHS

Much debate has surrounded the role of intelligence in the newly established DHS. The legislation is explicit that,

> Except as otherwise directed by the President, the Secretary (of DHS) shall have such access as the Secretary considers necessary to all information, including reports, assessments, analyses, and unevaluated intelligence relating to threats of terrorism against the United States and to other areas of responsibility assigned to the Secretary, and to all information concerning infrastructures or other vulnerabilities of the United States to terrorism, whether or not such information has been

---

[11] Robert David Steele, an intelligence expert with over twenty-five years of experience in military and strategic intelligence, is the author of *On Intelligence: Spies and Secrecy in an Open World* (AFCEA International Press, 2000 and OSS International Press, 2001), as well as *The New Craft of Intelligence: Personal, Public, and Political* (OSS International Press, 2002). He is the founder and CEO of Open Source Solutions Inc. (OSS). Biographical information obtained from OSS website at: www.oss.net.

[12] Robert David Steele, in an email exchange to members of the Naval Intelligence Professionals organization, 03 August 2002, Naval Intelligence Professionals on-line discussion forum. For more information on the Naval Intelligence Professionals visit the organization website at: http://www.navintpro.org.

> analyzed, that may be collected, possessed, or prepared by any agency of the Federal Government.[13]

A major component of the new DHS will be devoted to monitoring, analyzing, and utilizing all-source intelligence regarding threats to national security. Legislation tasks the new department with developing, as part of the Information Analysis and Infrastructure Protection Division, an intelligence center that will focus on terrorist threats and assessing vulnerabilities to attack.[14] The department, primarily as an intelligence consumer, will rely on information from other intelligence and law enforcement agencies such as the Central Intelligence Agency (CIA) and the Federal Bureau of Investigation (FBI). The role of intelligence for the proposed Department of Homeland Security is two-fold: 1) a process for the intergovernmental coordination of agencies involved in homeland security, and 2) a tailored, all-source fusion product to support DHS decision-makers and homeland security operational units.

C. ORGANIZATION

This thesis has six chapters. Chapter I: "Introduction," introduces one of the challenges for the new Department of Homeland Security, defining the role of intelligence. Through consultation of various sources, the author defines the term 'intelligence' and the role of intelligence in the proposed DHS.

Chapter II: "DHS Background," describes the current institutional status of the Department of Homeland Security (legislation, DHS proposals, organizational structure, and transition). Since the DHS is currently in the transitional stage descriptions are based on proposals and ideas, not concrete entities. In the aftermath of the terrorist attacks against America on 11 September 2001, President George W. Bush decided 22 previously disparate domestic agencies needed to be coordinated into one department to protect the nation against threats to the homeland.[15] This chapter provides a sense of ground truth for DHS organizational structure.

---

[13] Richard A. Best, Jr., *Homeland Security: Intelligence Support* (Washington, D.C.: Congressional Research Service Report for Congress, 18 November 2002), 2-3, Library of Congress Congressional Research Service, Order Code RS21283.

[14] James Jay Carafano, *Prospects for the Homeland Security Department: The 1947 Analogy* (Washington, D.C.: Center for Strategic and Budgetary Assessments, 12 September 2002). Retrieved from CSBA Website on 23 September 2002 at: http//: www.csbaonline.org.

[15] Quote from US Department of Homeland Security, 31 January 2003. Available at: http://www.dhs.gov/dhspublic/theme_home1.jsp, Keyword: DHS Organization.

Chapter III: "What's Being Proposed," describes some of the different proposals and ideas in general circulation for how DHS can accomplish this newly defined role for intelligence. This chapter breaks down how DHS can develop an intelligence process to coordinate the intelligence gathering of federal, state, and local agencies in order to produce tailored all-source decision support to DHS policymakers. Provisions include the setting up an internal DHS intelligence organizational structure, management of the domestic intelligence process, creating information-sharing network between federal/state/local agencies, and developing an internal analysis capability. Existing proposals and ideas also address what DHS is not going to do such as domestic collection. Data collection incorporated primary and secondary source material obtained from national intelligence and law enforcement agencies such as the CIA, the Drug Enforcement Agency (DEA), US Navy, Office of Homeland Security, and law enforcement working groups. In addition, research included state and local intelligence and law enforcement agencies such as the Terrorist Early Warning (TEW) working group. By describing different provisions, this chapter focuses on what is being proposed for the role of intelligence in DHS.

Chapter IV: "Solving the Issues," evaluates the positive and negative points of existing proposals. Numerous models and grassroots initiatives provide examples for DHS officials to follow. As a consumer of intelligence, DHS will place great demands on the Intelligence Community. For example, military intelligence's success in joint warfare provides a model for DHS' intelligence organizational structure. Informal information sharing-networks developed by the TEW in Los Angeles demonstrate sharing intelligence is not as technical as many proposals suggest. Despite relying on intelligence from other agencies like the CIA and FBI, the department will still require internal intelligence analysis. DHS requires a cadre of skilled analysts. Current DHS policy structure and resource allocation may provide obstacles to analyst recruitment. The department cannot afford to create "second-class analysts."

Chapter V "Conclusions," advocates solutions DHS should incorporate to carry out the new domestic role of intelligence. The DHS must strive toward a more collaborative consideration of ideas, alternative views, and, ultimately, solid analysis upon which to make decisions. Quality analysis will enhance the security of our country.

This chapter advocates several solutions for DHS: military intelligence's model is a good place to start, do not forget the value-added of OSINT, establish a "personal" information sharing system, and ensure internal analytical quality. The thesis offers insight and recommendations for the DHS transition team tasked to develop a new intelligence organization within DHS to safeguard the nation against terrorist attacks on US soil. The time has come to create a mix of spooks and suits to meet the needs of the country.

Chapter VI "Prologue" provides a brief description how the theoretical discussion and findings of this thesis serves a second purpose. The Naval Postgraduate School in conjunction with the Department of Justice and the Department of Homeland Security recently established a homeland security master's program. The new graduate-level curriculum aims to build a cadre of homeland security experts around the country. One of the core courses for the curriculum id devoted to the role of intelligence. Intelligence will play an important role in America's counterterrorist effort. The potential for real world applicability of the issues and topics presented in the following pages, in the long-term, aims to directly contribute to the nation's homeland security.

THIS PAGE INTENTIONALLY LEFT BLANK

II. DHS INSTITUTIONAL STATUS

> The United States Congress has taken an historic and bold step forward to protect the American people by passing legislation to create the Department of Homeland Security…. This bill includes the major components of my proposal—providing the intelligence analysis and infrastructure protection, strengthening our borders, improving the use of science and technology to counter weapons of mass destruction, and creating a comprehensive response and recovery division. (Statement by the President George W. Bush, November 19 2002)[16]

A. INTRODUCTION

The devastating events of 11 September 2001 forced the United States to focus federal, state, and local efforts in protecting the homeland. The country no longer maintains a sense of invulnerability to domestic attacks. In the aftermath of the terrorist attacks against America on 11 September, President George W. Bush decided 22 previously disparate domestic agencies needed to be coordinated into one department to protect the nation against threats to the homeland.[17] Intelligence will play a critical role in the new department. Before addressing proposals for the role of intelligence in DHS, a brief description of DHS organizational structure is required. This chapter describes the current institutional status of the Department of Homeland Security (legislation, DHS proposals, organization, and transition). With the DHS currently in the transitional stage, descriptions reflect proposals and ideas, not concrete entities. After providing a sense of current 'ground truth' in terms of DHS organizational structure the chapter defines the new role intelligence will play in DHS.

B. PAVING THE WAY FOR DHS

In June 2002, President Bush proposed the creation of a new Cabinet-level department to establish a unified effort against terrorist threats to the United States at home. The President's plan, outlined in the National Strategy for Homeland Security, came under intense scrutiny from members of Congress. Partisan disputes rang out on Capitol Hill. However, after the November 2002 Congressional elections the homeland

---

[16] Quoted from White House Official Website, 31 January 2003. Available at: www.whitehouse.gov/news/releases/2002/11/20021119-4.html.

[17] Quote from US Department of Homeland Security Website, http://www.dhs.gov/dhspublic/theme_home1.jsp, Keyword: DHS Organization.

security bill finally came to fruition. The road to passing the homeland security bill was tortuous to the end.[18] On 25 November 2002, President Bush signed the Homeland Security Act, marking one of the most significant transformations of the United States government since the 1947 National Security Act. The new law went into effect on 24 January 2003. Before the Homeland Security Act, the United States' domestic security organization appeared complex. Coordination and integration between federal, state, and local agencies was limited. Figure 1 depicts the domestic security organizational structure before the creation of the new Department of Homeland Security.

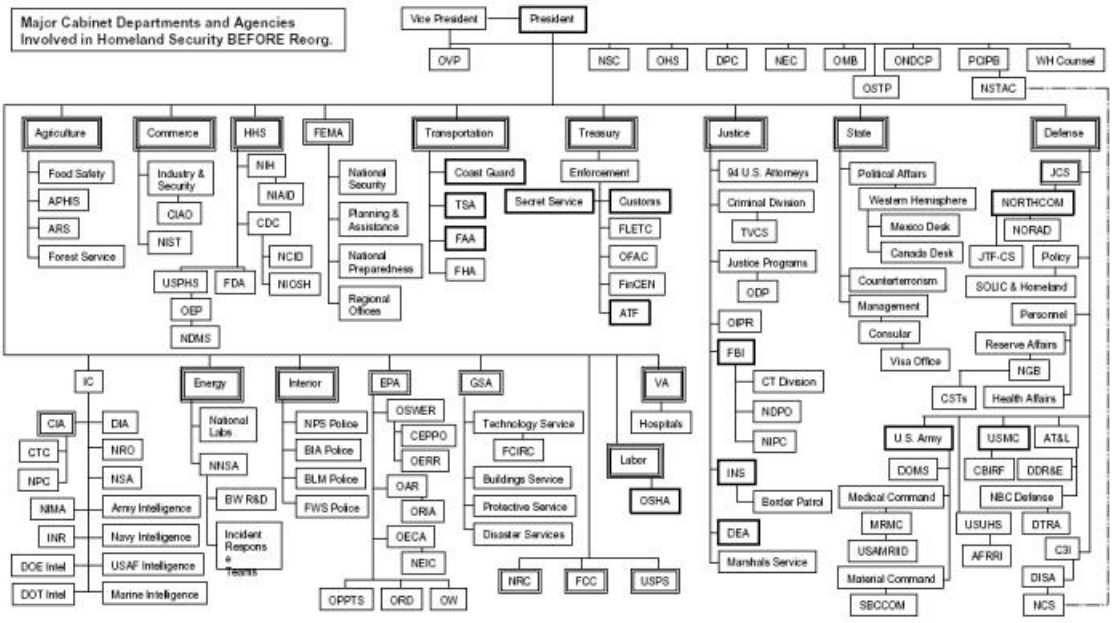

Figure 1. Organizational structure of US Cabinet departments and Agencies prior to creation of Department of Homeland Security.

Source: President Bush's Department of Homeland Security book, June 2002, www.whitehouse.gov/deptofhomeland/book.pdf

Figure 1. Organizational Structure Before the Creation of the Department of Homeland Security.

The new DHS looks to consolidate nearly 170,000 workers from 22 previously disparate domestic agencies into one department to protect the country against threats to

[18] "Bush to Sign Homeland Dept. Bill," *New York Times*, November 25, 2002. Retrieved from NY Times Website on 25 November 2002 at: http://www.nytimes.com/aponline/politics/AP-Bush-Homeland-Security.html/ex=1039242654&ei=1&en=9bbc98504ec515d7.

US soil. The National Security Strategy states three strategic objectives for DHS: 1) prevent terrorist attacks within the United States, 2) reduce America's vulnerability to terrorism, and 3) minimize damage and recover from attacks that do occur.[19] In order to accomplish its mission, the new Department of Homeland Security must mobilize and focus resources spanning across the federal government, state and local governments, the private sector, and the American people. Terrorists today can strike at any place, any time, and with virtually any weapon in a permanent condition and these new threats require our country to design a new security structure.[20]

C. DHS ORGANIZATIONAL STRUCTURE

The first priority of the new department is prevention. How can DHS protect the nation against further terrorist attacks at home? DHS is developing an organizational structure to coordinate the efforts of agencies tasked with homeland security responsibilities. Component agencies will analyze threats and intelligence, guard our borders and airports, protect our critical infrastructure, and coordinate the response of our nation for future emergencies.[21] DHS also strives to establish subordinate offices to support protecting the rights of American citizens and managing public services, such as natural disaster relief.

1. DHS Components

The DHS organizational structure delineates five major Divisions, or "Directorates": Border and Transportation Security, Emergency Preparedness and Response, Science and Technology, Management, and Information Analysis and Infrastructure Protection.[22] In addition to the five Directorates, several other critical agencies, previously or newly established, fold into the new DHS organizational structure. The United States Coast Guard, Secret Service, Bureau of Citizenship and Immigration Services, Office of State and Local Government Coordination, and the

---

[19] Strategic objectives quoted from the *National Strategy for Homeland Security*, released by the Office of the Press Secretary (Washington, D.C.: July 2002). Retrieved from the White House Official Website on 17 July 2002 at: http://www.whitehouse.gov/deptofhomeland/book/index.html.

[20] Quoted from White House Official Website, http://www.whitehouse.gov/deptofhomeland/sect2.html.

[21] Quoted from US Department of Homeland Security Website, http://www.dhs.gov/dhspublic/theme_home1.jsp.

[22] Quote from US Department of Homeland Security Website, http://www.dhs.gov/dhspublic/display?theme=10&content=11.

Office of Private Sector Liaison will come under the new department. Figure 2 depicts the organizational structure of the new DHS, as of 01 March 2003.

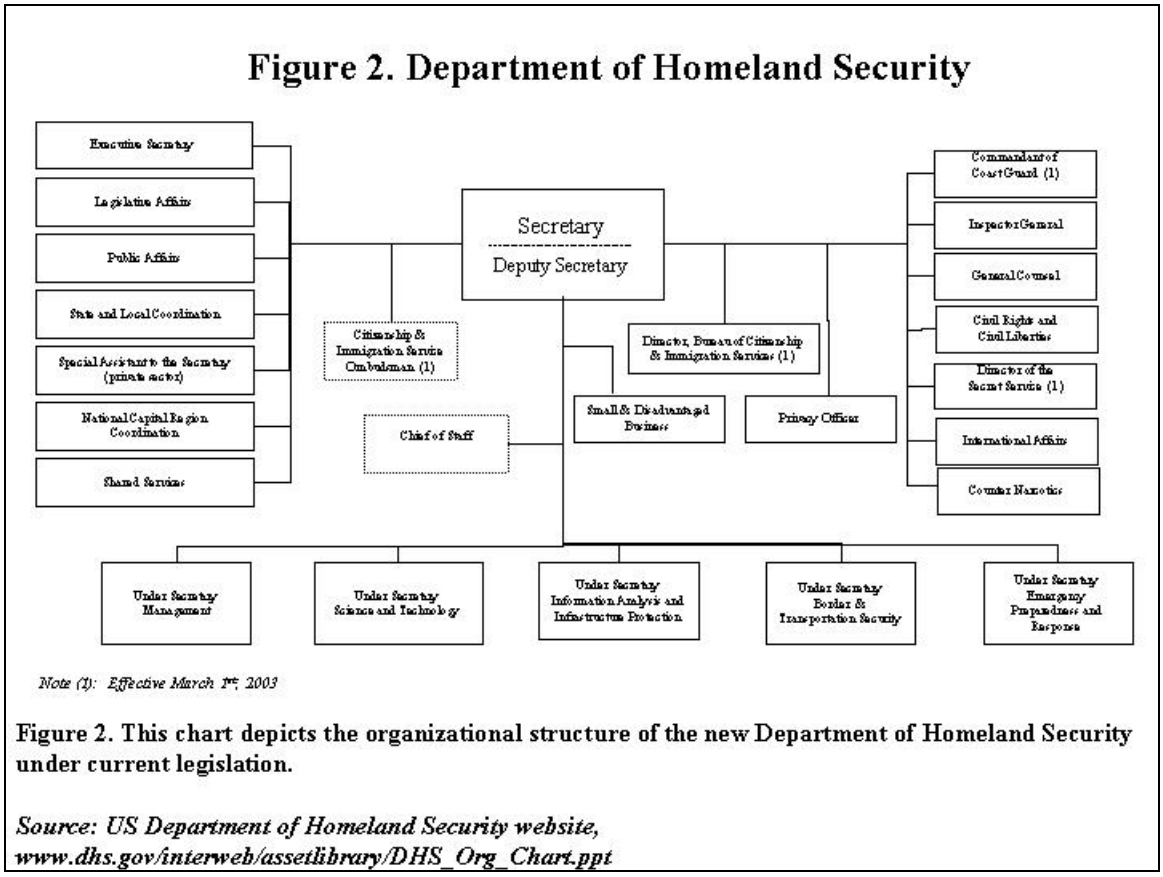

Figure 2. This chart depicts the organizational structure of the new Department of Homeland Security under current legislation.

Source: US Department of Homeland Security website, www.dhs.gov/interweb/assetlibrary/DHS_Org_Chart.ppt

Figure 2. Organizational Structure of New Department of Homeland Security.

The Information Analysis and Infrastructure Protection (IAIP) Division will provide the central repository for DHS intelligence support. Intelligence will play a critical role in the new organization.

2. DHS Transition

A Homeland Security Transition Planning Office (TPO) began contingency planning for the new Department in June 2002. Under the guidance of the Office of Homeland Security, TPO members focused on ensuring a smooth and expedient transition occurred following legislative approval of the new Department of Homeland Security. About 50 representatives from the tapped agencies, Office of Personnel Management, the Office of Management and Budget, and the White House developed options that would allow DHS to achieve new and enhanced capabilities in the most

effective and timely manner.[23] TPO transition teams structured themselves in teams paralleling the proposed Directorates of the new Department. Steven Cooper, Special Assistant to the President, Senior Director for Information Integration and Chief Information Officer, Office of Homeland Security CIO, spoke about some of the challenges the DHS transition team faced. During a speech on 19 August 2002, at the Government Symposium for Information Sharing and Homeland Security[24] he stated, "Pockets of experts exist in the United States, the question is how does the Office of Homeland Security get to them?"[25] The DHS transition team focused on coordinating homeland security initiatives and resources.

Effective 27 January 2003, the Department of Homeland Security Headquarters set up location at the Nebraska Avenue Center (NAC) in Northwest Washington, D.C.[26] The NAC is a United States Navy facility shared by the Office of Homeland Security staff.[27] The site provided the necessary components for standing up DHS operations immediately. However, the makeshift military offices reside several miles from the White House, the department's number one customer. Most of the department's personnel will work out of the NAC. In addition, some DHS personnel will work out of the newly proposed Terrorist Threat Integration Center (TTIC) (discussed further in section E of this chapter).

President Bush signed the Homeland Security Act on 25 November 2002, creating the new Department of Homeland Security. Concurrently the President submitted a Homeland Security Reorganization Plan to Congress (See Appendix A). Appendix A

[23] Ibid.

[24] Government Symposium for Information Sharing and Homeland Security, 19-21 August 2002, Philadelphia, Pennsylvania. Conference sponsored by The Government Emerging Technology Alliance (GETA), brought together members of various federal, state, and local communities to address Homeland Security-related information. Co-sponsored by the US Intelligence Community, Law Enforcement Community, Department of Defense, federal, local, and state agencies, the convention focused on gathering, sharing and interpreting information across the wide spectrum of agencies tasked with contributing to Homeland Security.

[25] Speech given by Steven Cooper, Special Assistant to the President, Senior Director for Information Integration and Chief Information Officer, Office of Homeland Security CIO, at the Government Symposium for Information Sharing and Homeland Security, Philadelphia, Pennsylvania, [19 August 2002]. (For typewritten notes of Steven Cooper's speech, see Appendix C).

[26] Quoted from US Department of Homeland Security Website, http://www.dhs.gov/dhspublic/display?theme=81&content=402.

[27] Ibid.

provides a copy of the President's reorganization plan. On 24 January 2003, the DHS officially came into existence. Setting up the new department will take time. Timelines vary on when the department will reach full operational status. By law, the DHS Secretary has one year from the time the Department becomes effective to bring all of the 22 agencies into the new organization.[28] 01 March 2003 marked the creation of the department. Several agencies such as the Customs Service and the Secret Service began transitioning to the new department.

3. Leadership

The creation of the new department establishes a single Cabinet official assigned the daunting task of protecting the American homeland from domestic terrorist threats. President Bush nominated former Pennsylvania Governor Tom Ridge as the first Secretary of Homeland Security. After receiving Congressional approval, Secretary Ridge became the 15th executive of President Bush's Cabinet. President Bush also nominated several other key senior leadership positions. For example, he nominated Gordon R. England, a former military contracting executive and Secretary of the Navy, as Mr. Ridge's deputy.[29] Many of the senior positions within the new department remain vacant (See Appendix B). Appendix B provides a current list of DHS senior officials and their nomination status.

4. DHS Agencies

Numerous component agencies will transfer to the new DHS. The agencies slated to become part of the Department of Homeland Security will be housed in one of the four major Directorates: Border and Transportation Security (BTS), Emergency Preparedness and Response (EPR), Science and Technology (S&T), and Information Analysis and Information Protection (IAIP).[30]

BTS unifies all major border security and transportations operations, to include:

- The US Customs Service (Treasury)

---

[28] Ibid.

[29] Richard W. Stevenson, "Signing Homeland Security Bill, Bush Appoints Ridge as Secretary," *New York Times,* 26 November 2002. Retrieved from NY Times Website on 29 November 2002 at: www.nytimes.com.

[30] Quoted from US Department of Homeland Security Website, http://www.dhs.gov/dhspublic/display?theme=13.

- Immigration and Naturalization Service (part) (Justice)
- The Federal Protective Service (GSA)
- The Transportation Security Administration (Transportation)
- Federal Law Enforcement Training Center (Treasury)
- Animal and Plant Health Inspection Service (part) (Agriculture)
- Office for Domestic Preparedness (Justice)

The EPR Directorate oversees coordinates disaster preparedness and response, to include:

- The Federal Emergency Management Agency (FEMA)
- Strategic National Stockpile and the National Disaster Medical System (HHS)
- Nuclear Incident Response Team (Energy)
- Domestic Emergency Support Teams (Justice)
- National Domestic Preparedness Office (FBI)

The S&T Directorate seeks to coordinate and utilize advancements in science and technology to further secure the homeland. The following assess to be part of this effort:

- CBRN Countermeasures Programs (Energy)
- Environmental Measurements Laboratory (Energy)
- National BW Defense Analysis Center (Defense)
- Plum Island Animal Disease Center (Agriculture)

Legislation directs the IAIP Directorate to analyze and assess all-source intelligence and information from other agencies (CIA, FBI, NSA, etc.) involving threats to homeland security and evaluate vulnerabilities in the nation's infrastructure. IAIP brings together:

- Critical Infrastructure Assurance Office (Commerce)
- Federal Computer Incident Response Center (GSA)

- National Communications System (Defense)
- National Infrastructure Protection Center (FBI)
- Energy Security and Assurance Program (Energy)

The creation of the new DHS marks one of the most significant transformations of the United States federal government since the 1947 National Security Act. Agencies assigned to the new department will analyze threats and intelligence, guard the country's borders, monitor port facilities and airports, protect critical infrastructure, and coordinate the nation's response to future contingencies.

D. INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION (IAIP) DIVISION

DHS, through the Directorate of IAIP will merge under one roof the capability to identify and assess current and future threats to the homeland, those threats against our vulnerabilities, issue timely warnings and take preventive and protective action.[31] On 14 March 2003, the White House announced Paul Redmond, the former chief of counterintelligence at the CIA, as assistant secretary of homeland security for information analysis.[32] Before Redmond's selection John Gannon, former chairman of the National Intelligence Council, headed the IAIP transition team. The IAIP transition team consisted of approximately seven members. John Gannon currently acts as Chief Intelligence Director for the new department. The team is tasked with the challenge to create a new and effective intelligence organization to meet the needs of the new department. "Actionable intelligence—that is, information which can lead to stopping or apprehending terrorists—is essential to the primary mission of DHS."[33] The IAIP will synthesize and disseminate information, provide intelligence analysis and alerts, develop plans to protect critical infrastructure, manage cyber security, provide indications and warning advisories, establish partnerships with federal, state, and local agencies, and provide coordination of the National Communications System (See Appendix C).

---

[31] Quote from US Department of Homeland Security Website, http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0094.xml.

[32] James Risen, "A Top Intelligence Post Goes to C.I.A. Officer In Spy Case," *New York Times*, 13 March 2003.

[33] US Department of Homeland Security Website, http://www.dhs.gov/dhspublic/interapp/editorial_0094.xml.

Appendix C provides a detailed description of the tasks assigned to the IAIP as stated by the US Department of Homeland Security.

E. TERRORIST THREAT INTEGRATION CENTER

In the January 2003 State of the Union Address, President Bush announced a new initiative to better protect America by continuing to close the "seam" between analysis of foreign and domestic intelligence on terrorism.[34] The new Terrorist Threat Integration Center (TTIC) will assess all-source intelligence gathered by the CIA, Justice Department, Pentagon, and DHS. It will enable consolidated integration of the nation's terrorist threat-related information and analysis. On 11 March 2003, after consultation with the Director of the FBI, the Attorney General, and the Secretaries of Homeland Security and Defense, Director of Central Intelligence, George Tenet, named John O. Brennan as Director of the newly created TTIC.

The new center aims to remove information-sharing and analysis barriers between intelligence and law enforcement agencies. The new TTIC has significant implications for the DHS. "Homeland Security will be a full partner and an important customer" of the center, one senior administration official, said.[35] The DHS will add critical new capabilities in the area of information analysis and infrastructure protection.[36] Lines of authority between the two organizations appear confusing. The center will consist of the counterterrorism expertise from the FBI, CIA, and other Defense Department agencies. TTIC proposals indicate DHS will be an important consumer of intelligence from the new center. In testimony before the Senate Governmental Affairs Committee on 26 February 2003, Homeland Security Deputy Secretary England said that Homeland Security would be a "partner" in the new center, but would act mainly as a consumer of the intelligence the new center produces.[37]

---

[34] "Fact Sheet: Strengthening Intelligence to Better Protect America," *Official White House News Release* (28 January 2003). Retrieved on 07 February 2003 from White House Official Website at: http://www.whitehouse.gov/news/releases/2003/01/print/20030128-12.html.

[35] Walter Pincus and Mike Allen, "Terrorism Agency Planned: Center to Integrate Intelligence, Analysis," *Washington Post*, 29 January 2003, 12.

[36] "Fact Sheet: Strengthening Intelligence to Better Protect America," 3.

[37] Shane Harris, "Homeland Security Cedes Intelligence Role," *Government Executive Magazine*, 26 February 2003. Retrieved from Government Executive Website on 28 February 2003 at: http://govexec.com/dailyfed/0203/022603h1.htm.

The current TTIC proposal does not clearly delineate operational responsibilities between TTIC and DHS. CIA Director George Tenet will have oversight authority over the organization and will choose its head.[38] However, the CIA traditional focuses on foreign intelligence. The proposed TTIC will have the authority to set requirements and assign collection operations for all intelligence agencies. DHS will have to coordinate collection operations of state and local law enforcement authorities. In addition, DHS will be responsible for ensuring threat information, produced by DHS internally, or by the TTIC, disseminates in a timely fashion to the public, private industry, and state and local governments. The center seems to parallel the intelligence analysis capabilities assigned to DHS in the Homeland Security Act. Operational chains of commands appear to overlap between the two organizations. TTIC proposals indicate some of the DHS functions be performed at the new facility housing the TTIC.[39] In addition, senior terrorism analysts from DHS will work out of the TTIC facility. How the intelligence analysis section of DHS effectively functions in coordination with the new TTIC remains unanswered. A senior multi-agency team will finalize the details, design, and implementation strategy for the stand-up of the Terrorist Threat Integration Center.[40]

F. THE ROLE OF INTELLIGENCE IN THE PROPOSED DEPARTMENT OF HOMELAND SECURITY

One area of concern for DHS is intelligence support. As a consumer of intelligence, DHS will compete with other members of the national security community to ensure DHS meets its priority requirements. Defining the role of intelligence in the DHS and creating appropriate solutions to address intelligence issues related to homeland security is no easy task. Many challenges surround the role of intelligence in the newly established DHS such as DHS' role in the Intelligence Community, establishing information-sharing networks, acquiring "raw intelligence", incorporating open source information (OSINT), and internal analytical quality. The information analysis element within DHS will have the responsibility for acquiring and reviewing information from the agencies of the Intelligence Community, from law enforcement agencies, state and local

[38] Ibid.

[39] "Fact Sheet: Strengthening Intelligence to Better Protect America," 3.

[40] Ibid., 2.

government agencies, and unclassified publicly available information (OSINT) from books, periodicals, pamphlets, the Internet, and other media.

Through an evaluation of published proposals and first hand inputs obtained from civilian and military intelligence experts from intelligence and law enforcement agencies, this thesis defines, evaluates, and advocates the role of intelligence within the newly established DHS. The proposals and ideas in general circulation addressed in this thesis available span across federal, state, and local levels. In addition, this thesis describes how DHS can accomplish the new role for intelligence and advocates solutions to the intelligence issues facing DHS policymakers. Data collection incorporated expertise from federal agencies such as the CIA, FBI, US Navy, the Office of Homeland Security, and DEA. State and local expertise included insight from groups such as the El Paso Intelligence Center and the Terrorist Early Warning (TEW) group in Los Angeles.

1. The New Domestic Intelligence Focus

In the United States, intelligence historically focused foreign intelligence. For example, during years of the Cold War, intelligence efforts sought to counter Soviet collection against the United States and its allies. The Soviet Union expended significant resources on its own intelligence collection against the United States and its allies, even during World War II, when the Soviet Union was considered and ally.[41] US intelligence did not have to focus on threats to American soil. US political sensitivities reinforced the notion, preference to intelligence focused away from the homeland.[42] Throughout the 1990s, US intelligence agencies sought to redefine threats to the nation's security.

In addition, secrecy typically dominated US intelligence. In a recent *Rand Review* article, Jeffrey Issacson and Kevin O'Connell point out, "It is not surprising that the legacy of US intelligence was to share as little as possible with potential collaborators, both inside and outside the government."[43] Superpower competition drove many in the intelligence community to feel little need share information broadly. Dissemination of intelligence precluded US domestic agencies not directly involved in national security affairs. This thesis does not look to analyze the failures of 11 September or place blame

[41] Issacson and O'Connell, *Rand Review*, 48.

[42] Ibid.

[43] Ibid.

on any agencies or individuals. Before 11 September, the intelligence community primarily focused its interest overseas, paying little attention to links between home and abroad.

The events of 11 September 2001 dictate the role of intelligence has changed. The role of intelligence must also take on a new domestic focus. US departments and agencies long considered to be outside the national security arena—such as the US Treasury, the Federal Emergency Management Agency, or the US Border Patrol—now play an important role in securing the homeland.[44] More importantly, state and local governments play a role in homeland security. The cop on the street will prove to provide valuable intelligence in conjunction with traditional intelligence agencies such as the CIA. The cities will provide valuable intelligence. State and local entities will not only benefit from disseminated intelligence, the will also provide important sources of intelligence. The primary mission of the new DHS is to protect the nation against further terrorist attacks. The role of intelligence in for the new department is two-fold: 1) a process for the intergovernmental coordination of agencies involved in homeland security, and 2) a tailored, all-source fusion product to support DHS decision-makers and homeland security operational units. A new domestic role for intelligence is required to become an effective instrument of national power. This new role for intelligence presents many challenges for the DHS. Defining the role of intelligence is only the first step. The next step is addressing how DHS can accomplish this new role for intelligence. The DHS must address several intelligence issues. For example, the DHS must establish an intelligence organization capable of producing and coordinating the dissemination of actionable intelligence to deter future terrorist attacks on American soil.

Such is the 'ground truth' and current institutional status of the new Department of Homeland Security.

[44] Ibid., 49.

III. ISSUES UNDER DISCUSSION FOR THE NEW ROLE OF INTELLIGENCE

A. INTRODUCTION

The new Department of Homeland Security represents a major reorganization of numerous agencies assigned with US homeland security responsibilities. DHS aims to unify these agencies and their functions into one operational command tasked with defending the United States against domestic terrorist threats. Presently, the federal government lacks a single institution dedicated to systematically analyzing all information, both classified and unclassified, on potential terrorist threats within the United States. A major component of the new department will focus on monitoring, analyzing, and utilizing all-source intelligence about domestic threats to US national security. Intelligence is critical for preventing future acts of terrorism against the United States. The role of intelligence in the new DHS is two-fold: 1) a process for the intergovernmental coordination of agencies involved in homeland security, and 2) a tailored, all-source fusion product to support DHS decision-makers. Numerous discussion groups, task forces, and research firms have generated proposals and recommendations addressing the role for DHS intelligence support. Utilizing data collected from proposals and ideas in general circulation, and primary source material, this chapter describes some of the intelligence issues DHS officials need to address in order to accomplish the two-fold role of intelligence.

1. Tapping into the 'Ground Truth'

In order to uncover the 'ground truth' about DHS intelligence issues, research and data collection incorporated a multitude of primary and secondary sources. Published reports from the Markle Foundation Task Force, the Center for Strategic and Budgetary Assessments, an Independent Task Force sponsored by the Council on Foreign Relations, the Rand Corporation, the Congressional Research Service, the House Subcommittee on Terrorism and Homeland Security, and the Homeland Security Practice Group, highlight some of the intelligence issues for the new DHS. More importantly, research incorporated primary source material obtained from national and regional conferences on homeland security, interviews with intelligence and law enforcement experts, and public

speeches given by officials from the Intelligence Community and the Office of Homeland Security (See Appendix D). Appendix D is a detailed list of the national and regional conferences serving as primary source venues for this thesis. These conferences provided a means to discuss the role of intelligence support in homeland security with experts from the intelligence and law enforcement communities. Primary source data provided valuable personal insights from personnel involved with homeland security responsibilities at the federal, state, and local levels. In addition, conference forums provided the opportunity to conduct interviews with civilian and military experts currently working on homeland security efforts. Anecdotal analysis of typewritten "After Action Reports" provided the means to consolidate and process the first-hand knowledge obtained from conferences and interviews (See Appendix E for an example). Appendix E provides a complete summary of the After Action report written on the 2002 Government Symposium for Information Sharing and Homeland Security. In addition, data collection incorporated inputs obtained from presentations by senior officials currently assigned to the Office of Homeland Security (See Appendix D). Testimony from senior officials in the Intelligence Community and the Office of Homeland Security helped fuse together a complete picture of how DHS can provide intelligence support. Appendix F provides a copy of the typewritten "After Action Report" from MGEN Bruce Lawlor's[45] presentation at the Naval Postgraduate School on 05 November 2002, entitled "The Future of Homeland Security" (See Appendix F).

Access to intelligence professional networks also provided valuable primary source material. For example, the Naval Intelligence Professionals (NIP)[46] organization provided the means to establish personal contacts and obtain first hand inputs from civilian and military intelligence and law enforcement professionals around the country.

[45] MGEN Bruce Lawlor, Senior Director for Protection and Prevention, Office of Homeland Security, visited the Naval Postgraduate School (NPS), Monterey, California, 04-05 November 2002. He met with faculty and students to discuss the role of intelligence in the new Department of Homeland Security. He also gave a brief to NPS faculty and students on 05 November 2002, entitled "The Future of Homeland Security."

[46] "Founded in 1985, Naval Intelligence Professionals (NIP) is a nonprofit organization incorporated to enhance awareness of the mission and vital functions of the Naval Intelligence community, as well as to foster camaraderie among Naval Intelligence Professionals. It is an association of active duty, retired and reserve officers, enlisted personnel, and civilians who serve or have served within the Naval Intelligence community, as well as those in certain other categories who qualify as a nonvoting Subscriber." Retrieved from NIP website on 25 February 2003 at: http://www.navintpro.org.

Fusing together, a diverse cross-section of all-source information helped uncover the 'ground truth' of how intelligence can provide a process for intergovernmental agency coordination in homeland security intelligence and provide a quality, all-source fusion product to support DHS decision-makers.

B. WHAT ARE THE INTELLIGENCE ISSUES?

1. Setting Up an Internal Intelligence Organizational Structure

The final version of the Homeland Security Act establishes a Directorate for Information Analysis and Infrastructure Protection (IAIP) to head DHS intelligence efforts. Legislation envisions an intelligence entity focused on receiving and analyzing intelligence from other government agencies and using it to provide warning of terrorist attacks and for addressing vulnerabilities terrorists could exploit.[47] In order to accomplish its assigned mission, the DHS must first develop an internal intelligence organizational structure. The new Department of Homeland Security must create a new intelligence entity to pull together information and intelligence from a variety of sources focused on domestic threats. The Markle Foundation Task Force on National Security in the Information Age[48] published a report in October 2002 emphasizing the critical component to establishing a DHS intelligence entity. "A successful domestic intelligence and information strategy should start with the way we organize our people to take advantage of innovation."[49] Traditional intelligence focused on threats abroad. A sound domestic intelligence organizational structure is required for DHS mission accomplishment.

Other intelligence professionals and experts also recommend first establishing a DHS' intelligence organization. Robert David Steele points out, "America lacks a theory, concepts and doctrine, and a structured approach to how we might train, equip, and organize homeland defense intelligence and related security capabilities that are—from the beginning—both networked and largely voluntary. A separate program is

[47] Best, 2.

[48] On 7 October 2002 the Markle Foundation Task Force on National Security in the Information Age published a report entitled "Protecting America's Freedom in the Information Age, offering specific recommendations on how the government can develop information collection and analysis capabilities while also protecting the civil liberties of American citizens. The entire report can be found at: http://www.markletaskforce.org/documents/Markle_Full_Report.pdf. Information on the Markle Foundation Task Force on National Security in the Information Age can be found at: http://www.markletaskforce.org/.

[49] Markle Task Force Report, 9.

needed within which to earmark federal funds and establish capabilities at federal, state and local levels that apply the new craft of intelligence."[50] Dr. Barry Zulauf[51], liaison officer, Drug Enforcement Administration (DEA) Intelligence Division adds, "The House Homeland bill calls for a fusion center, as if stating the phrase in law could summon one 'out of the vast deep.' Neither this bill, nor the Senate version puts any of the organizational, structural, legal, or technical machinery in place."[52] The new DHS will identify and assess current and future threats, inform the President, issue timely warnings and take or effect appropriate action. The first step for DHS is to develop an effective intelligence organizational structure. Ralph Norman Channell[53], a retired US Navy Captain and a Vietnam Veteran with 26 years of experience in Joint and Naval Intelligence, states, "Creating a structure so that an array of organizations can generate or analyze valuable intelligence information and provide it to officials and operations officers who can put it to good use is a daunting enterprise."[54] The new DHS intelligence entity needs to ensure it provides timely and actionable intelligence to DHS policymakers. In addition, the intelligence structure must coordinate the collection, analysis, and dissemination of time critical intelligence between federal, state, and local agencies. Channell adds, "The new department needs to ensure centralized command functions are established. It would probably be useful to create a capability to monitor and report on every stage of the terrorist "cycle."[55] Setting up a new intelligence organizational structure is no easy task. Ron Dick, former head of the National Infrastructure Protection Center (NIPC) and currently working for Computer Sciences

[50] Robert David Steele, "Talking Points on Homeland Defense Intelligence," Memorandum Prepared for Brent Scowcroft, 03 December 2001. (Electronic Copy to Naval Intelligence Professionals Organization, 03 December 2002), Naval Intelligence Professionals On-Line Discussion Forum. 03 December 2002. Memorandum can also be retrieved from www.oss.net.

[51] Dr. Barry A. Zulauf, Liaison Officer, Intel Division of Drug Enforcement Administration. Dr. Zulauf is also a naval intelligence officer reservist recently assigned to the faculty of the Joint Military Intelligence College (JMIC).

[52] Dr. Barry A. Zulauf, liaison officer of Drug Enforcement Administration Intelligence Division, interview by author, 4 December 2002.

[53] "Ralph "Norm" Channell is a retired US Navy Captain and a Vietnam Veteran with 26 years of experience in Joint and Naval Intelligence. He also served as a Senior Lecturer at the Naval Postgraduate School where he taught Joint Warfare and Intelligence for over a decade." Biographical information retrieved from Center for Contemporary Conflict website on 25 February 2003, at: http://www.ccc.nps.navy.mil/rsepResources/si/aug02/homeland2.asp.

[54] Channell, 1.

[55] Channell, 1.

Corporation's homeland security division, points out, "Any time you start up a new entity, even though you laid a good foundation, until you start to execute its mission, there's always concerns as to how that's going to work."[56]

2. Managing the Intelligence Process

Another challenge for DHS personnel is managing the intelligence process within the new department. "We must ensure a smooth and complete transition of organizational effectiveness as we cannot afford to have the new Department of Homeland Security reinventing the wheel at this critical point," warned Sen. Chuck Grassley, R-Iowa.[57] He added, "We cannot allow agencies that are turning over parts of their former domains to be parochial in their approach to this new department."[58] DHS will not have its own collection assets. The new department must ensure information from such agencies as the CIA and FBI is analyzed side-by –side with all other intelligence. The information analysis element within DHS will have the responsibility for acquiring and reviewing information from the Intelligence Community, law enforcement agencies, state and local government agencies, and unclassified publicly available information (commonly referred to as open source information or "OSINT") from books periodicals, pamphlets, the Internet, and media.[59] The new DHS intelligence entity must establish an internal intelligence process to request, collect, analyze, and disseminate actionable intelligence to agencies and personnel assigned homeland security responsibilities.

Intelligence expert Mark Lowenthal discusses the components of the intelligence process. In his book *Intelligence: From Secrets to Policy*, Lowenthal writes, "Intelligence can be thought of as the means by which certain types of information are required and requested, collected, analyzed, and disseminated; and the way in which certain types of covert action are conceived and conducted."[60] The first step for DHS is to identify the new department's intelligence requirements, or Essential Elements of

---

[56] Brock N. Meeks, "A Chink in the Infrastructure Armor? *MSNBC News*. www.msnbc.com/new/868116.asp?0cv=CB10, 06 February 2003, 5.

[57] Ibid, 5.

[58] Ibid, 5.

[59] Best, 2.

[60] Lowenthal, 8.

Information (EEI). EEI provide a starting point for DHS analysts. The EEI dictate what information is required for DHS senior officials to make real-time decisions. The next step is to standardize procedures for intelligence collection. DHS analysts can first collect EEIs from readily available classified and unclassified sources. Current DHS legislation dictates the department will have to obtain some EEIs from other intelligence and law enforcement agencies. The new DHS needs to ensure other agencies understand and carry out the department's collection requirements. The DHS intelligence process also needs to address analysis of raw and finished intelligence. Lastly, the DHS must coordinate and consolidate dissemination of actionable intelligence to state and local public safety agencies and the private sector. Traditionally, intelligence agencies focused on foreign intelligence collection. The events of 11 September 2001 dictate terrorists can cause enormous damage by attacking the country's critical infrastructure at home. Homeland Security requires a national effort to secure America. At present, the United States has no central process or institution dedicated to analyzing all-source intelligence on potential terrorist threats within the country. The new department should manage the domestic intelligence process.

a. Defining DHS' Role in the Intelligence Community

Many key agencies will contribute valuable intelligence to homeland security efforts. DHS will become a new member of the Intelligence Community. However, the Director of Central Intelligence (DCI) currently presides over the Intelligence Community. DHS will have to define its role within the Intelligence Community. Within the Intelligence Community, the DCI establishes priorities for collection (and to some extent for analysis), based in practice on inter-agency discussions.[61] The Homeland Security Act dictates the new DHS department will become a member of the Intelligence Community. DHS officials need to ensure the department's intelligence collection and analysis requirements are met. Although the FBI and CIA will not be included in the Department of Homeland Security, the new Department should be able to task these agencies and other members of the intelligence community to produce required analyses or raw data. Officials and analysts at the Homeland Security Department, however, might find themselves at a disadvantage when

[61] Best, p. 4. Outlined in 50 USC 403-3(c) (2).

dealing with other intelligence agencies because the intelligence community often makes source protection a priority.[62] The new department must devise ways to overcome classification barriers. Classification barriers cannot preclude the dissemination of actionable intelligence to those on the "frontlines of homeland security" (state and local public safety agencies, private sector, etc.). DHS intelligence personnel will also facilitate access to intelligence databases and other analytical resources.[63] Supporting Intelligence Community responsibilities will require more personnel resources than currently envisioned for DHS, thereby detracting from the intended focus on analysis of terrorist attacks.[64] The new DHS intelligence entity will have to balance a variety of tasks and responsibilities as a new member of the Intelligence Community. Based on his years of experience in intelligence and law enforcement with the DEA, Dr. Barry Zulauf provides some personal insight. Dr. Zulauf states, "From where I sit, DHS will have a broad statutory set of authorities to vacuum up all kinds of information, including Law Enforcement information as well as National Foreign Intelligence, and next to NO capability to process it or to get it to the people who need it."[65] The new DHS will have to effectively manage its internal intelligence process and define its role within the Intelligence Community.

b. The Question of "Raw" Intelligence

There has been some discussion in the media whether DHS will have access to "raw intelligence" or only to finished analytical products.[66] The new department will not have its own collection assets. Raw data, such as satellite imagery or signals intercepts, is useless without some analysis included. Including source information with raw data represents classification issues. For example, human intelligence (HUMINT) reporting is often very sensitive in nature. However, DHS would require some assessment of the reliability of the source. The new DHS intelligence division will have to address the danger of unauthorized disclosures, dissemination of

---

[62] Channell, 2.

[63] Best, 4.

[64] Ibid.

[65] Dr. Barry Zulauf interview.

[66] Best, 4.

sensitive information, and protection of sources. DHS analysts must develop a means to utilize raw intelligence without knowing some of the source details.

3. Information-Sharing

Numerous reports, publications, and conferences highlight the importance of sharing information and intelligence between organizations and agencies assigned homeland security responsibilities. Lieutenant Colonel Kenneth A. Luikart, United States Air Force[67], air intelligence officer for the 165th Airlift Wing, Georgia Air National Guard, wrote, "The attacks in September 2001 suggest that inadequate information sharing between law enforcement and national intelligence agencies led to lost opportunities to thwart the attacks launched by Al-Qaeda."[68] One reason Al Qaeda caught America by surprise on 11 September was a failure to communicate. The House Subcommittee on Terrorism and Homeland Security stated, "The failure of the Intelligence Community (IC) to provide adequate forewarning was affected by resource constraints and a series of questionable management decisions related to funding priorities."[69] Agencies involved with domestic security lacked an information-sharing network to exchange intelligence.

The new department must develop a system to share intelligence among agencies at the federal, state, and local levels. Information sharing is critical to homeland security. In a recent *Rand Review* article, Jeffrey Issacson, vice president and director of the National Security Research Division at RAND, and Kevin O'Connell, director of RAND's Intelligence Policy Center, pointed out, "Better information sharing—both

---

[67] Lieutenant Colonel Kenneth A. Luikart is the air intelligence officer for the 165th Airlift Wing, Georgia Air National Guard. Colonel Luikart served 18 months in Vietnam; supported Operation TEAM SPIRIT in Korea; Operation BADGE Torch in Thailand; Operations CORONET OAK and VOLANT OAK in Panama, providing intelligence support to anti-drug trafficking missions in Central and South America. He supported Operations PROVIDE PROMISE, JOINT ENDEAVOR, and JOINT FORGE, flying important airlift missions into Bosnia and Herzegovina. Colonel Luikart supported Operation SUPPORT HOPE, flying humanitarian missions into Rwanda and Zaire; and the 1996 Summer Olympic Games, where he supported the State Olympic Law Enforcement Command as the Senior Air Intelligence Liaison Officer for Task Force 165. Biographical information obtained from Center for Contemporary Conflict Website, 23 February 2003 at: http://www.ccc.nps.navy.mil/rsepResources/si/dec02/homeland.asp.

[68] Lt. Colonel Kenneth A. Luikart, USAF. "Homeland Security: Intelligence Indications and Warning." *Strategic Insights*. 02 December 2002. Retrieved from Center for Contemporary Conflict Website on 23 February 2003 at: http://www.ccc.nps.navy.mil/rsepResources/si/dec02/homeland.asp.

[69] House Permanent Select Committee on Intelligence, Subcommittee on Terrorism and Homeland Security, *Counterterrorism Intelligence Capabilities and Performance Prior to 9-11,* report prepared by Saxby Chambliss, July 2002.

within and beyond the U.S. government—is essential to combat a networked, global terrorist threat."[70] In October 2002, the Markle Foundation Task Force on National Security in the Information Age released a report describing the need to build an information-sharing network to connect federal, state, and local levels. The report calls for "a networked information technology system that effectively shares information among local, state, regional, and federal agencies and the private sector, and sets forth a blueprint for how such a system can be established under a set of Presidential guidelines."[71] Other published reports advocate establishing an information-sharing network to coordinate the interaction between individuals and agencies tasked with homeland security missions. Some highlighted the lack of current networking capabilities. A Center for Strategic and Budgetary Assessments (CSBA) report by James Jay Carafano pointed out, "There are, for example, insufficient information sharing and intelligence networks, or shared data bases that link federal, state, and local agencies.[72] In order to accomplish its stated mission the DHS must establish integrated information sharing systems. Current systems are inadequate. For example, a Department of Justice study group found that 22 percent of the cities it surveyed with populations over 250,000 had not municipal-wide systems for sharing information.[73]

a. Integrating the Front Lines

A major contributor to the homeland security mission is those agencies working the "frontlines" of homeland security such as local police and firefighters. Information sharing systems need to include the integration of first responders into DHS intelligence. State and local public safety agencies, and the private sector play a key role in domestic intelligence efforts. The Markle Foundation Task Force report stated,

> Most of the real frontlines of homeland security are outside of Washington, D.C. Likely terrorists are often encountered, and the targets they might attack are protected, by local officials—a cop hearing a complaint from a landlord, an airport official who hears about a plane some pilot trainee left on a runway, an FBI agent puzzled by an odd flight

[70] Issacson and O'Connell, *Rand* Review, 1.

[71] Markle Foundation Task Force, 17-18.

[72] Carafano, 9.

[73] Ibid, 9.

> school student in Arizona, or an emergency room resident trying to treat patients stricken by an unusual illness.[74]

In a November 2002 presentation to students and faculty at the Naval Postgraduate School in Monterey, CA, MGEN Bruce Lawlor, Senior Director for Protection and Prevention, Office of Homeland Security, reiterated the location of the true front lines of DHS intelligence. He stated,

> The true front line of homeland security intelligence and information collection lies with the cities themselves. Police provide the security mechanism to detect terrorist activity in the cities. Intelligence is in the communities. An enormous piece to the Department Homeland Security is the creation of a state, local, and federal information-sharing network.[75]

In a presentation given at the Government Symposium for Information Sharing and Homeland Security in August 2002, Dr. Steven Gale[76], Director of the Center for Organizational Dynamics, provided an interesting analogy summarizing the level of information sharing needing to take place within the United States. Dr. Gale stated, "When it comes to information sharing on homeland security the intelligence analyst must be connected to the railroad car conductor to the chemical producers and to the first responders."[77] Information sharing needs to be driven by clear cut objectives and existing capabilities, if not "we are merely swapping stories."[78] The new Department of Homeland Security must develop plans to connect organizations and agencies at the federal, state, and local levels.

b. No Easy Task

In theory, establishing an information sharing system sounds simple, but in practice, numerous challenges exist. For example, many local officials do not have security clearances or secure facilities to protect classified data. Classification barriers present a difficult challenge for exchanging information between agencies. Numerous

---

[74] Markle Task Force Report, 10.

[75] MGEN Lawlor Speech. See Appendix C.

[76] Dr. Steven Gale, Director of the Center for Organizational Dynamics, over 25 years of experience studying terrorism.

[77] Speech by Dr. Steven Gale, at the Government Symposium for Information Sharing and Homeland Security, Philadelphia, PA, (August 2002). See AFCEA After Action Report (Appendix E) for detailed account of Dr. Gale's remarks.

[78] Ibid (See Appendix E).

handling caveats and accesses for intelligence exist. Many intelligence agencies share intelligence on a "need to know" basis. Homeland Security requires sharing information on a "need to share" basis. Another obstacle is funding. President Bush and Congress resolved the issues over creating a Department of Homeland Security, but funding for new programs has not yet been resolved. "The reason is that only 2 of the 13 appropriations bills to provide money for the government's departments and agencies have been enacted…The government is no operating under what is called a continuing resolution, which limits departments and agencies to spending at last year's levels."[79] How will all these different agencies share data in order to accomplish the homeland security mission?

4. The Use of Open Source Information (OSINT)

Information from unclassified sources—books, pamphlets, Internet sources, television and radio programs—is arguably an important resource for gaining information about terrorist groups and the larger political movements with which they are associated.[80] Traditionally intelligence focuses on the realm of secrecy. More often, the intelligence community relies on classified information for intelligence analysis and assessments. Views among intelligence agencies vary on the incorporation of open source information. DCI George Tenet in prepared testimony for the Senate Government Affairs Committee on 27 June 2002, stated that, "In every possible case, we will provide intelligence at the lowest permissible level of classification, including sensitive, but unclassified."[81] As Director Tenet's remarks indicate, all-source analysis typically overlooks open source information.

Incorporating open source information will provide a valuable resource to the new DHS intelligence entity. Robert David Steele, in his book *On Intelligence—Spies and Secrecy in an Open World*, points out the importance of incorporating open source information. Mr. Steele emphasizes the need for,

[79] David E. Rosenbaum, "Spending Deadlock Will Delay Some Programs of New Security Department." *New York Times,* 21 November 2002. Retrieved from New York Times Website on 21 November 2002 at: http://www.nytimes.com/2002/11/21/politics/21HOME.html?ex=1028897315&ei=1&en=2ac0efe386c4f94f. 1.

[80] Best, 4.

[81] Testimony of Hon. George J. Tenet, US Congress, Senate, 107th Congress, 2d session, Committee on Governmental Affairs, A Review of Relationship Between a Department of Homeland Security and the Intelligence Community, Hearings, 26 and 27 June 2002, S. Hrg. 107-562, 69.

> Emerging concepts and doctrine for a more open intelligence community—one that is fully connected to a larger national information community as well as to a global architecture for more deliberate information-sharing between governmental and non-governmental organizations across national and cultural boundaries.[82]

Open source intelligence should not replace classified intelligence. However, understanding the terrorist threat facing the United States does not lie in a "secret vault."

a. An Academic Example

For example, publications from the found in the academia community provide credible open source information. Students at the Naval Postgraduate School, Monterey, California can take a course on Islamic fundamentalism. The course educates students on such topics as Islamic fundamentalist profiles, the causes of Islamic fundamentalism, and the strategic objectives of Islamic fundamentalist groups. Course materials go beyond the contemporary publications one finds exploited by the news media. Students review primary source material written by Islamic fundamentalists such as Ayatollah Khomeini and Osama bin Laden. Analyzing the works of Islamic fundamentalists provides an example of utilizing credible open source information. DHS officials must understand not all the answers to preventing future terrorist threats to the United States lie locked behind a secret vault. The new DHS intelligence entity will have to integrate classified and unclassified intelligence.

5. Analytical Quality

> Aside from the disadvantage of diverting scarce talent from other agencies, a number of the specific needed skills may not exist in adequate supply in the federal government at all. There is a particular shortage of people with both the needed analytical and data skills. At a minimum, significant investment in training will be needed, training oriented to the analytic methods and challenges described above and the networked, decentralized approach to using these methods.[83]

Information exchange between government agencies is only one issue for DHS. The Information Analysis and Infrastructure Protection (IAIP) division will also provide the core of domestic intelligence analysis. In a televised speech last year President Bush stated, "This new department will review intelligence and law enforcement information

[82] Robert David Steele. *On Intelligence—Spies and Secrecy in an Open World. 1.*

[83] Markle Task Force Report, 37.

from all agencies of government and produce a single daily picture of threats against our homeland."[84] At present, the federal government lacks an institution dedicated to analyzing systematically all information on domestic terrorist threats. The new DHS must provide quality analysis of domestic intelligence to support protecting the nation's critical infrastructure. "Analysts will be responsible for imagining the worst and planning to counter it."[85] Jeffrey Issacson and Kevin O'Connell suggested, "The intelligence community needs to rebuild an analytical cadre of highly skilled and continuously retrained specialists who can integrate knowledge pertinent to counterterrorism gained from multiple data sources, professional disciplines, and social sectors."[86] The DHS needs to build a cadre of skilled intelligence analysts trained in focusing on domestic threats. This cadre of DHS intelligence professionals must produce quality intelligence assessments and analyses to disseminate across federal, state, and local levels. The Markle Foundation Task Force point out the problem is broader than just sharing information.

> It is the challenge of using information effectively, linking collection with sound and imaginative analysis derived from multiple perspectives, and employing cutting-edge technology to support end-users, from emergency responders to Presidents. In other words, we need to *mobilize* information for the new era of national security we have entered…to take domestic intelligence seriously we must address the specifics of the analytical work that needs to be done. To link analysis to action, we give some illustrations of how information can empower people in the field, while also recommending guidelines to protect American liberties, not just American lives.[87]

Assessments and analyses produced by DHS intelligence analysts will influence the decision-making of numerous agencies. Ensuring analytical quality among DHS intelligence professionals is critical to the nation's homeland security effort. In a recent Congressional Research Service report, Richard Best points out,

---

[84] Brock N. Meeks. "A Chink in the Infrastructure Armor?" *MSNBC News*. 06 February 2003. Retrieved from MSNBC News Website on 07 February 2003 at: www.msnbc.com/news/868116.asp?0cv=CB10. 5.

[85] Ibid, 5.

[86] Issacson and O'Connell, *Rand Review,* 1.

[87] Markle Task Force Report, 9.

> Along with obtaining intelligence reporting from other agencies, DHS intelligence personnel will also produce vulnerability assessments of key resources and infrastructure, identify priorities for protection by the DHS, other agencies of the federal government, state and local government agencies and authorities, the private sector and other entities.[88]

DHS intelligence personnel reporting will influence a multitude of homeland security organizations.

The primary focus of the new Department of Homeland Security is preventing future terrorist attacks on American soil. DHS intelligence analysts will have to focus on predicting and deterring domestic threats. The key test for the DHS will be the quality of the analytical product—whether terrorist groups can be identified and warning given of plans for attacks on the US.[89] DHS personnel will not only be consumers of intelligence. They will have to assess multi-source intelligence, both classified and unclassified, in order to provide DHS policymakers with actionable intelligence. According to Issacson and O'Connell, "US decision makers must be careful to understand that we can paralyze our efforts to secure the homeland by disseminating information that is 'inactionable' (or not useful), incomplete, or simply lacking in solid analysis."[90] In order to provide timely operational intelligence support to DHS policymakers, the new DHS intelligence entity requires quality analysis.

Based on proposals and ideas in general circulation, and primary source material obtained from intelligence and law enforcement professionals, this chapter described some of the pressing intelligence issues for the new Department of Homeland Security. These issues highlight how the new department can accomplish the role defined for intelligence in DHS. The next step is advocating solutions.

---

[88] Best, 3.

[89] Ibid, 5.

[90] Issacson and O'Connell, *Rand Review,* 2.

IV. SOLVING THE ISSUES

A. INTRODUCTION

The previous chapter described some of the major intelligence issues the new DHS officials to address in accomplishing the department's new role for intelligence. Highlighting concepts and ideas in general circulation is only the first step. This chapter advocates how the DHS can provide a process for intergovernmental agency intelligence coordination and produce actionable intelligence to deter future terrorist attacks against America at home.

B. ORGANIZING THE DHS INTELLIGENCE DIVISION

1. Military Intelligence Provides a Model

Intelligence support will be critical to the new department's ability to deter future terrorist threats. The first step for DHS officials is creating an organizational structure for the new department's intelligence division. The US military's intelligence organizational structure provides the best model for DHS officials to follow. Ralph Channell points out, "The US military's recent experience, especially in organizing for joint warfare, might be a place to turn for some lessons."[91] Other intelligence professionals reinforce why the military's intelligence organizational structure is a good model to follow. CAPT Tom Ward, a naval intelligence officer working on homeland security issues at the Joint Forces Command, pointed out, "The military intelligence community itself is not having difficulty implementing change to support homeland security. Common practices and concepts are pretty much in place already."[92] MGEN Bruce Lawlor, Senior Director for Protection and Prevention, Office of Homeland Security, expressed similar sentiments in a November 2002 brief to faculty and students at the Naval Postgraduate School, Monterey, California. MGEN Lawlor stated, "The main contribution the military can make to the DHS is helping to provide a security mindset that deals with doctrine, tactics, procedures, and skills needed for homeland

[91] Channell, 1.

[92] CAPT Tom Ward, Joint Forces Command J2 for Joint Task Force on Homeland Security, interview by author, 20 August 2002, conducted at the Government Symposium for Information Sharing and Homeland Security, Philadelphia, PA, typewritten interview notes (See Appendix E).

security."[93] He added, "The military thinks in security terms to guide planning. The civilian sector is just not used to thinking in this paradigm."[94] Utilizing the military intelligence model would provide a foundation for the new department's domestic intelligence construct.

2. Centralized Command Functions

Another component for the department's intelligence structure is developing a centralized command. DHS officials should establish a headquarters near Washington, D.C. to coordinate the nation's domestic intelligence effort. A centralized headquarters would allow for collation and analysis of data provided from agencies or field offices dispersed throughout the United States. In addition, the centralized headquarters would dictate policy guidelines for agencies and organizations at the federal, state, and local levels. Without a centralized command, dispersed organizations will have no common standards or principles to dictate how the various agencies fit into the "big picture" of securing the homeland. Distinct grassroots initiatives for conducting domestic intelligence will continue without a governing authority. Without a centralized command, these disparate agencies, working as individual "stovepipes," will fail to fuse together all-source intelligence. Domestic intelligence collection, analysis and dissemination spans across federal, state, and local levels. The country cannot afford to have individual agencies work in their own unique stovepipe. A centralized command will coordinate the efforts of all those involved in homeland security intelligence. DHS must take the lead in setting domestic information and intelligence priorities.

3. Decentralized Command Functions

The new intelligence division must also create a balance of decentralized command functions. The Markle Task Force Report pointed out, "The intelligence and other information critical to homeland security will come from across the country and around the world. Washington, D.C., is a critical node in that network, but only one of many."[95] Information and intelligence sharing cannot only focus on the capital of the

---

[93] MGEN Lawlor Speech Given at the Naval Postgraduate School, Monterey, California, 05 November 2002. See Appendix F for notes from MGEN Lawlor's presentation. After Action Report Written by Author.

[94] Ibid (See Appendix F).

[95] Markle Task Force Report, 11.

country. Domestic intelligence cannot only support DHS policymakers. The new DHS intelligence agency will have to support the frontlines of homeland security. Most of the people, information, and action will be in the field—in regional or local federal offices, in state, regional, and local governments, and in private firms.[96] DHS officials must understand that states have their own sovereignty and capabilities. The DHS intelligence entity must also address state-based capabilities.

The new department should create regional intelligence centers throughout the country. Regional intelligence centers create a link between DHS and state and local organizations. These regional centers would create 24/7 all-source fusion cells to maintain intelligence preparation of the battle space for the entire country. Homeland security deals with a multitude of issues requiring specialized expertise. As intermediaries, regional intelligence centers would provide the ability to conduct specialty area analysis. Different regions of the country focus on distinct homeland security issues. Regional offices could establish specialized bureaus to deal with specific functional problems such as monitoring of shipping containers, chemical and biological defense, and tracking immigration activity. Several grassroots initiatives demonstrate the infrastructure for regional intelligence centers is already in place.

a. Terrorist Early Warning Working Group in Los Angeles

The Los Angeles County Sheriff's Department created a Terrorism Early Warning (TEW) group to connect law enforcement, fire, health, and emergency management agencies to circulate warnings, analyze possible dangers, check public health and epidemiological indicators, and manage possible consequences of a terrorism event.[97] Through routine monthly meetings, the TEW group provides a simple forum to overcome interagency cooperation difficulties on homeland security issues. The group has also developed methods to avoid classification barriers for sharing information. For example, the group publishes a TEW OSINT report for agencies affiliated with the group. The TEW group emphasizes a "need to share" philosophy. The group rewards information sharing. TEW avoids having too many handling caveats and accesses for intelligence. For more details on operating procedures of the TEW group, refer to

[96] Ibid, 2.

[97] Markle Task Force Report, 14.

Appendix G. Appendix G provides an After Action Report from the 26 September 2002, TEW group conference. The report describes the TEW organization, conference agenda, and procedures. Other regional intelligence centers should follow the TEW concept. The new DHS will require information from various homeland security authorities ranging from law enforcement to state and local public safety to national foreign intelligence. Models like the TEW group provide an example of the regional intelligence infrastructure, already in place, for the new Department of Homeland Security to incorporate.

b. Addressing State-Based Capabilities

The new DHS must incorporate doctrine, tactics, and procedures for developing state-based capabilities. Robert David Steele explains the importance of creating state-based intelligence capabilities. "Federal bureaucrats rarely understand the vital reality that states have their own sovereignty and that federal solutions are neither desired nor able to be implemented at the state level. Needed instead is a systematic means for transferring the proven process of intelligence and counterintelligence down to the state level.[98] He recommends three initiatives:

> 1) A national training program for state-based intelligence and counter intelligence specialists, 2) the creation of 24/7 Community Intelligence Centers in each state (each subordinate to the Governor) utilizing federal funds and expertise, and 3) the appointment by each Governor of trusted senior State Intelligence Officers (SIO); some to oversee all state-based intelligence operations, and others to represent the Governor within the Homeland Defense Intelligence Center. Mobilize all citizens as "watch standers.[99]

The new intelligence organizational structure within DHS does not have to start from scratch. Models currently exist for DHS officials to follow. The DHS intelligence division must ensure a balance of centralized and decentralized command functions. In addition, procedures must develop for addressing state-based capabilities. Establishing a sound intelligence structure within the new DHS creates the foundation for "unity of effort" and "economy of force" against domestic terrorist threats.

---

[98] Steele, "Talking Points on Homeland Defense Intelligence," 1.

[99] Ibid.

C. CREATING AN ALL-SOURCE FUSION CENTER

One major component of the DHS intelligence division is the creation of an all-source fusion center where DHS analysts can evaluate and assess intelligence information, both classified and unclassified, obtained from agencies involved in homeland security. The lack of all-source intelligence contributed to the intelligence shortfalls that made the terrorist attacks of 11 September possible.[100] The new DHS must become the hub for accumulating, and analyzing all-source domestic intelligence. Creating an all-source fusion center is not a new concept.

1. Navy's Operational Intelligence (OPINTEL) Model

The US Navy, for example, ran a successful Ocean Surveillance Information System (OSIS) during the Cold War intended to monitor and track the threat posed by the Soviet Navy. Functions of this system included monitoring long-term trends (e.g., new ship construction or doctrinal debates), fusion of multiple sources of information to track and analyze worldwide Soviet ship movements in near real time dissemination of useful information directly to US ships at sea.[101] The Navy's operational intelligence (OPINTEL) model provided the ability to take existing and missing evidence, link it to long-term trends and patterns, and make OPINTEL assessments regarding Soviet naval activity. In order to prevent future domestic terrorist attacks DHS must create the ability to provide long-term trends and pattern analysis. With the Navy's OPINTEL model, "A global effort that unfolded over many months was thus required to provide real-time support to operational units."[102] The new DHS will require the ability to provide operational units around the country with actionable intelligence to deter terrorist activity. The Navy's OSIS model provides an example for DHS to follow in creating an all-source fusion center.

2. El Paso Intelligence Center

Another model for an all-source fusion center is the El Paso Intelligence Center. Dr. Barry Zulauf, DEA Intelligence Division liaison officer, provides a brief description of the El Paso Intelligence Center. "The El Paso Intelligence Center performs its multiple database analysis on request and provides immediate actionable intelligence to

[100] Channell, 2.

[101] Ibid., 1.

[102] Ibid.

first responders and emergency services people around the country 24/7. The concept tracks with its 'First Cousin' the Navy OPINTEL model—designed to serve the operating forces."[103] The El Paso Intelligence Center coordinates the all-source fusion of intelligence provided by organizations and agencies in the El Paso, TX region. The center provides the ability to take existing and missing evidence, link it to long-term trends and patterns, and timely assessments regarding homeland security issues. The organization provides a current feed of domestic intelligence to its customers. In order to prevent future domestic terrorist attacks DHS must create the ability to provide an intelligence product based on long-term trends and pattern analysis.

3. Army's Information Dominance Center (IDC)

The IDC is the research and development center for Defense Advanced Research Projects Agency's (DARPA) Total Information Awareness (TIA) program headed by Dr. John Poindexter. The organization provides a prototype for total information awareness. Philosophically, IDC/TIA is similar in its approach and goals to the Navy's OSIS. In a recent interview, retired Navy Captain Joe Mazzafro summarized IDC's capabilities. He stated,

> IDC/TIA employs massive computing capacity in train with powerful data mining, fusion/correlation algorithms, analytical tools, and visualization technologies to do high volume at high-speed transactional analysis to provide all source situational awareness and predictive intelligence. IDC's goal is to provide analysts with fused all source near real time reports to complement current scheduled production reporting of the intelligence community. IDC is clearly able to do nodal analysis on vast amounts of transactional events (phone calls, faxes, emails, etc.) and display the results in a meaningful way.[104]

The IDC/TIA transformed the Navy's OSIS model through application of information technology. Mazzafro adds, "The IDC is not a linear extrapolation of OSIS, but rather its transformation through the IT revolution."[105]

The creation of an all-source fusion center for the new DHS is a critical component to ensuring DHS policymakers gain full situational awareness of domestic

[103] Dr. Barry A. Zulauf interview.

[104] Mazzafro, Joe, Retired Navy Captain, Johns Hopkins Applied Physics Lab, Interview by Author, 02 March 2003, Interview Via E-Mail Correspondence.

[105] Ibid.

threats to the United States. The Navy's OPINTEL model, the El Paso Intelligence Center, and the Army's IDC provide examples of all-source intelligence fusion centers for the new DHS to follow. Developing an all-source fusion center will help ensure DHS provides actionable intelligence to homeland security decision-makers and operational units.

D. INFORMATION SHARING NETWORKS NOT SO TECHNICAL AFTER ALL

A significant obstacle for the new DHS is coordinating information sharing between disparate agencies spanning across federal, state, and local levels. Numerous proposals recommend the creation of technologically advanced information sharing systems, databases, and data mining techniques. However, proposals and recommendations for sophisticated computer networks require time and money. More importantly, they overlook a much simpler solution, personal networking. Until DHS acquires appropriations and development for sophisticated databases and connectivity infrastructure, the new department should focus on knowledge management and establishing communities of practice. Developing personal networking systems provides a solution to information sharing obstacles now.

The new Department of Homeland Security is an extensive group of organizations and personnel with vastly varying homeland security expertise and responsibilities. In today's environment, there is significant overlap of mission and duplication of effort within and between organizations with homeland security responsibilities. Since the tragedy of 11 September 2001, the new DHS has been fortunate in that is has seen a windfall of funding to support protecting the homeland. However, as the attacks of 11 September move farther into the past, the purse strings of Congress will begin to tighten again. Into the future, the new DHS may receive more appropriations but the burgeoning coffers will fade. Establishing a Homeland Security Community of Practice is an opportunity for DHS to organize and make real change that will make it viable, respected, and unmatched into the future. The new DHS must find ways to prevent the duplication of effort, increase collaboration between organizations at the federal, state, and local levels and better manage the resources available in personnel. One method DHS should implement to meet the demand for information-sharing across federal, state, and local

levels is to begin establishing communities of practice to coordinate DHS organizations, policies, and practices.

1. What are Communities of Practice (CoPs)?

Intelligence analysts working an intelligence problem may sometimes stop and think, "I know someone in organization X has dealt with this particular problem before I just don't know who…?" Communities of Practice provide the best means for enabling organizations to share knowledge community-wide. An improved network of personal contacts and better results strengthen organizations. Personnel benefit through peer-group recognition and continuous learning.

CoPs are groups of people who share a concern, a set of problems, or a passion about a topic, and who deepen their knowledge and expertise in this area by interacting on an ongoing basis.[106] Although the term "Community of Practice" is relatively new, CoPs are not. Such groups have been around since people in organizations realized they could benefit from sharing their knowledge, insights, and experiences with others who have similar interests or goals. One of the best-known, early examples of a CoP is one formed by the copier repair technicians at Xerox Corporation.[107] Through networking and sharing their experiences, particularly the problems they encountered and the solutions they devised, a core group of these technicians proved extremely effective in improving the efficiency and effectiveness of efforts to diagnose and repair Xerox customers' copy machines. The impact on customer satisfaction and the business value to Xerox was invaluable. Yet, for the most part, this was a voluntary, informal gathering and sharing of expertise, not a "corporate program." Because CoPs generate extraordinary learning, they are among the most important structures for any organization where thinking matters and information sharing is required for mission accomplishment, whether officially recognized by senior leadership or not.

2. Personal Networking Provides an Answer Now

---

[106] Etienne Wenger, Richard McDermott, and William M. Snyder, *Cultivating Communities of Practice* (Boston: Harvard Business School Press, 2002), 4.

[107] John Seely Brown and Estee Solomon Gray, "The People Are the Company," *Fast Company Magazine*, No. 1, November 1995. Retrieved from Fast Company website on 12 March 2003 at: http://www.fastcompany.com/online/01/people.html.

In theory, establishing an information sharing system sounds simple, but in practice, numerous challenges confront DHS. For example, many local officials do not have security clearances or secure facilities to protect classified data. Many agencies disseminate information on a "need to know" basis. Homeland Security information sharing requires a "need to share" philosophy. Establishing personal contacts with various agencies provide a means to work around classification barriers.

Database systems and computer-based networks provide long-term solutions to the information-sharing problem. In addition, information sharing technology initiatives remain long term until due to funding constraints. At the working level in the federal agencies in Washington, D.C., the problem of information and homeland security has been seen, first of all, as a problem of buying new technology.[108] Sums are being spent to modernize each agency's own information systems, some of it relevant to homeland security, almost none of this money is being spent to solve the problem of how to *share* this information and intelligence among those federal agencies."[109] Adequate appropriations to fund the development of new information systems do not seem to exist yet. However, the terrorists will not wait until this infrastructure is in place. Establishing a homeland security community of practice, building personal networks, and creating a liaison officer network provides solutions now.

a. Establish a Homeland Security Community of Practice

The new DHS must devise an approach to ensure knowledge management. DHS policymakers should strongly consider the effects of applying communities of practice to the new DHS and its potential to contribute to domestic intelligence information sharing. If the new DHS is to flourish and meet the increasing demands of homeland security as outlined in the National Strategy for Homeland Security, the new department must find short-term solutions to transform. Terrorists will not stand by and wait until they new department develops the necessary components to protecting the homeland. Numerous organizations have embraced knowledge management. For example, the US Navy looks to be a front-runner in the implementation of knowledge management. The naval intelligence community in particular is conducting research and

[108] Markle Task Force Report, 10.

[109] Ibid.

development for the creation of an intelligence skill set and experience database, co-hosted with a collaborative environment such as threaded news groups.[110]

Agencies involved with homeland security need to collaborate and exchange information and ideas. A multitude of agencies from the intelligence and law enforcement communities will provide valuable intelligence for DHS analysts. In order to conduct all-source analysis a good intelligence professional must establish a diverse network of personal contacts. Bill Moffett, a retired intelligence officer with 28 years of service at the CIA, pointed out, "The best way to tap into intelligence produced by the CIA is through establishing personal contacts."[111] The key to gaining access to other intelligence agencies is personal networking. DHS intelligence personnel should create communities of practice to build a cadre of homeland security expertise. Inexpensive software programs can provide the means for DHS intelligence personnel to connect with personnel assigned homeland security responsibilities around the country. In addition, DHS personnel should subscribe to various intelligence networking forums such as the Naval Intelligence Professionals and the Association of Former Intelligence Officers. Communities of Practice are working around the country. The Terrorist Early Warning (TEW) working group in Los Angeles, discussed earlier in Chapter II, illustrates how personal networking can make a difference. Based on a foundation of a personal networking database, the TEW is able to coordinate regional information sharing in a simple yet effective manner. DHS analysts should establish a homeland security community of practice.

b. Establish a Liaison Network

Establishing liaisons can also enhance personal networking for DHS personnel. The DHS should not rely solely on computer-based information sharing systems. Liaison with various intelligence (CIA, NSA, NORTHCOM) and law enforcement (FBI, chiefs of police) agencies will be required. In addition, liaison with state, city, and other local officials will be crucial because these officials have the

[110] Presentation given by LT Ray Kendall and LT Kevin McHale, "1630 Community of Practice," 6 March 2003, Naval Postgraduate School, Monterey, CA. The presentation highlighted the naval intelligence community's research and development efforts in building a community of practice for naval intelligence officers.

[111] Bill Moffett, "CIA Capabilities Brief." Presentation to NS4159 students at the Naval Postgraduate School, Monterey, CA, 13 February 2003.

resources needed to act on warnings issued by the Homeland Security Department.[112] Local officials play a key role in homeland security because they reside on the front lines. In addition, they have the ability to detect specific evidence of terrorist activity that is often uncovered in traffic stops, citizen reports of strange activity or people, or local arrests.[113] An established information sharing system provides the means for these reports to reach national level organizations. In turn, as national organizations receive local reporting then can combine it with multiple source intelligence to create the correct "big picture." Personal networking and establishing communities of practice is the short-term solution to ensuring homeland security information sharing.

E. UTILIZING OPEN SOURCE INTELLIGENCE (OSINT)

Information from open sources such as books, pamphlets, journals, and Internet sources is an important resource for gaining intelligence about terrorist groups and their intended political agendas. Intelligence agencies often overlook incorporating OSINT. Traditional intelligence tradecraft typically did not fuse OSINT with other types of classified intelligence such as imagery intelligence (IMINT) or signal intelligence (SIGINT). The new DHS will have to incorporate tactics, techniques, and procedures to collect and analyze OSINT. Robert David Steele is his book *On Intelligence: Spies and Secrecy in an Open World,* writes,

> Analysts should be able to use classified information to inform themselves and validate their views, but they should focus production efforts on the unclassified side, providing information that can not only go to the individual government consumers, but which can also go into the public domain through the open architecture.[114]

Homeland security responsibilities span across a wide spectrum of federal, state, and local levels. Domestic intelligence cannot rely solely on classified information. Not all personnel assigned with homeland security responsibilities will have security clearances. Classification systems used by agencies such as the CIA or NSA does not apply to the "cop on the beat." Utilizing open source information provides a means to avoid classification barriers.

---

[112] Channell, 1.

[113] Ibid., 2.

[114] Robert David Steele. *On Intelligence: Spies and Secrecy in an Open World*. (Oakton, Virginia: OSS International Press, 2001), p. 79.

Secret intelligence alone cannot protect America's homeland. All parts of government, federal, state, and local provide valuable intelligence to safeguard the United States. Homeland security requires a new tradecraft of intelligence, incorporating open source information. In his book *The New Craft of Intelligence: Personal, Public, and Political*, Robert David Steele provides a recommendation for incorporating open source information. "Before pattern analysis can be useful, a global open source benchmarking endeavor is needed across all countries and topics. Essentially, the art and science of pattern analysis from signals intelligence must now be brought over to the open source world, both in print and broadcast media monitoring."[115] DHS must undertake procedures to collect and analyze OSINT. The United States today faces "non-traditional threats from cultural traditions that we do not understand very well—such as terrorism rooted in extremist Islamic groups."[116] Many of the keys to unlocking the answers to these non-traditional threats lie in the unclassified realm of web-based exchanges, not secret or top-secret databases. The new DHS must tap into existing open sources such journals, domestic and foreign news services, and most importantly the Internet. Individuals and agencies assigned with homeland security responsibilities should have an unclassified channel for exchanging domestic intelligence. In today's technological advanced world, open source information is at an analyst's fingertips. The question is whether DHS intelligence analysts incorporate OSINT into their all-source fusion of intelligence.

F. SETTING A PLACE AT THE INTELLIGENCE COMMUNITY'S TABLE

The new Department of Homeland Security should manage the domestic intelligence process. Although the FBI and CIA will not be included in the Department of Homeland Security, the new Department should be able to task these agencies and other members of the intelligence community to produce required analyses or raw data. Officials and analysts at the Homeland Security Department, however, might find themselves at a disadvantage when dealing with other intelligence agencies because the intelligence community often makes source protection a priority.[117]

---

[115] Robert David Steele. *The New Craft of Intelligence: Personal, Public, and Political.* (Oakton, Virginia: OSS International Press, 2002), 152.

[116] Ibid., 158.

[117] Chanell, 2.

The State Department's Bureau of Intelligence and Research (INR) provides a model for creating a balance between providing intelligence input to support the policymaking process and providing accurate intelligence analysis of the threat. Most observers credit INR with having performed responsibly over the years.[118] Being a component of the Intelligence Community has allowed INR to have direct and close access to intelligence data and analysis as well as to influence the establishment of collection and analysis priorities.[119] Legislation does not provide the new department with its own collection assets. DHS intelligence will come from a variety of agencies. The management of the intelligence process is crucial, especially the establishment of a secure information system to support databases and the rapid exchange of information. Close liaison with, and the ability to task the intelligence community, especially the CIA, NSA, and the FBI, is required.[120] The Markle Report reemphasizes the need for the new DHS to drive domestic intelligence collection. The report stated,

> The DHS should be the lead agency for shaping domestic intelligence products to inform policymakers, especially on the analytical side, so that there is some separation between the attitudes and priorities of intelligence analysis and the different, more concentrated, focus of law enforcement personnel authorized to use force on the street to make arrests and pursue or detain citizens.[121]

G. ENSURE ANALYTICAL QUALITY

Despite rhetoric that DHS will be a consumer of intelligence from other agencies, the new department still requires skilled intelligence analysts. Ralph Norman Channell points out, "The new department needs analysts and managers in both headquarters and field offices and liaison officers serving with other intelligence agencies."[122] DHS intelligence personnel will have to analyze and assess information received from other sources before turned over to DHS policymakers. Quality analysis does not currently exist within the new DHS. A recent report by Richard Best, Specialist in National Defense Foreign Affairs, Defense, and Trade Division points out, "The types of

[118] Best, 4.

[119] Ibid.

[120] Channell, 3.

[121] Markle Task Force Report, 3.

[122] Channell, 2.

information that have to be analyzed come from disparate sources and require a variety of analytical skills that are not in plentiful supply."[123] For example, analysts will require training on foreign environments from which terrorist groups emerge. In addition, combining personnel from other agencies requires coordinating different cultures and paradigms. Personnel from other agencies will require analytical training on DHS intelligence requirements. In a *Rand Review* article Jeffrey Issacson and Kevin O'Connell summarize,

> Analyzing terrorism is not like analyzing Russian naval strength or Latin American political systems; such analyses rely upon well-defined indicators and data sources. In contrast, counter terrorism analysis must provide structure to information that can be highly fragmentary, lacking in well-defined links, and fraught with deception. It must infer specific strategies and plans from small pieces of information. It must find common threads among seemingly disparate strands. And unlike the terrorist, who needs only a single vulnerability to exploit, the analyst must consider all potential vulnerabilities.[124]

The DHS must ensure the development of analytical quality within the new department. As a consumer, DHS still requires a cadre of skilled analysts to conduct its own internal intelligence analyses and assessments. DHS intelligence analysts will have to work with other relevant agencies to map and prioritize critical infrastructure within the United States. The capability to analyze the vulnerability of potential targets and the means used to attack critical infrastructure must reside in one place. This is why it is so essential that the intelligence and critical infrastructure protection both be placed under the DHS's Undersecretary for Intelligence.[125] Ensuring analytical quality is vital to DHS mission accomplishment. However, the primary function of the new department is not intelligence. This creates a problem for anyone involved in intelligence analysis within DHS. Quality intelligence analysts become prime candidates for recruitment by the CIA or other intelligence agencies. As a result, intelligence analysis in the new department becomes a collateral duty, in turn leading to second-class analysts. No current organization within the United States is currently exceptional at solely domestic intelligence. The FBI maintains a collective and investigative culture for developing

[123] Best, 5.

[124] Issacson and O'Connell, *Rand Review,* 49.

[125] Markle Task Force Report, 25.

material for prosecuting purposes. The CIA focuses its intelligence efforts on foreign threats. The new DHS intelligence should take the lead in domestic intelligence efforts. Doing so requires a cadre of skilled intelligence analysts. DHS officials must ensure quality domestic intelligence analysis capabilities exist within the new department.

1. Manning

Recent reports indicate the department's intelligence division may face analyst-manning issues. One member of the new department's transition team stated, "This vital division will be 'way behind the power curve in the intelligence game' and forced to make do with a patchwork of temporary workers on loan from various agencies drawn from civilian contractors."[126] For example, the bulk of Information Analysis and Infrastructure Protection (IAIP) personnel will come from an existing FBI unit, the National Infrastructure Protection Center (NIPC). However, the law creating the Homeland Security Department does not mandate FBI agents working for NIPC voluntarily give up their jobs in the bureau.[127] NIPC controls the Key Asset Initiative, a program staffed by 216 field agents whom identify potential threats to US critical infrastructure. However, Commander David Wray, a Naval Reserve officer called back to active duty and working as spokesman for NIPC, pointed out, "Those [Key Asset Initiative] functions, under law, transfer with NIPC but those FBI agents in the field will not transfer to Homeland Security."[128] In the initial stages, the new DHS will begin with analysts detailed from existing intelligence and law enforcement agencies. In addition to analysts from the FBI's NIPC, a small number of analysts from the Department of Commerce, the National Communications System, the Department of Energy, the National Infrastructure Simulation and Analysis Center and the General Services Administration, will augment the Homeland Security Department's intelligence branch.[129]

2. Training

---

[126] Brock N. Meeks, 1.

[127] Ibid, 2.

[128] Ibid.

[129] Ibid, 4.

Ensuring analytical quality within the new department requires development and investment in training. The Markle Task Force points out,

> Aside from the disadvantage of diverting scarce talent from other agencies, a number of the specific needed skills may not exist in adequate supply in the federal government at all. There is a particular shortage of people with both the needed analytical and data skills. At a minimum, significant investment in training will be needed, training oriented to the analytic methods and challenges described above and the networked, decentralized approach to using these methods.[130]

The new DHS needs to create a national program for training domestic intelligence analysts. Analysts within the new department will not be the only ones requiring adequate training. Intelligence specialist training needs to extend across federal, state, and local levels.

Intelligence support is a key area of concern for the new DHS. Within the new department, the role of intelligence is two-fold: 1) provide a process for the intergovernmental coordination of exchanging domestic intelligence, and 2) the production of tailored all-source intelligence analysis to support homeland security decision-makers and operational units. This chapter advocated recommendations and solutions for accomplishing intelligence's two-fold approach.

[130] Markle Task Force Report, 37.

V. CONCLUSIONS

A. DEFINING THE NEW ROLE FOR INTELLIGENCE

The creation of the new Department of Homeland Security represents one of the most significant changes in the federal government since the 1947 National Security Act. The new department aims to organize over 170,000 personnel spanning 22 previously disparate agencies into a unified operational structure capable of defending American citizens and their infrastructure against domestic terrorists threats. DHS officials face numerous challenges in creating a new homeland security apparatus. How can DHS prevent future attacks against America at home? Intelligence provides part of the answer. A critical component of the new department will be devoted to monitoring, analyzing, and utilizing intelligence pertaining to potential threats against the US homeland. DHS legislation proposes an analytical element within DHS with the capability to draw upon all the information gathering resources of federal, state, and local agencies.

This thesis defined 'Intelligence' as *the process and product by which information, both classified and unclassified, is collected and analyzed to provide policy makers with tailored-decision support on national security issues*. The role of intelligence for the proposed Department of Homeland Security is two-fold: 1) a process for the intergovernmental coordination of agencies involved in homeland security, and 2) a tailored, all-source fusion product to support DHS decision-makers and homeland security operational units.

Various publications and ideas in general circulation describe how to accomplish the new the role of intelligence within DHS. The success of the new DHS intelligence analysis element largely depends on addressing DHS intelligence organizational structure, managing the domestic intelligence process, creating an information network between federal, state and local agencies, and ensuring analytical quality. This thesis outlines some of the major intelligence issues for the new DHS. It by no means is all-inclusive. For example, DHS will have to address other issues such as striking a balance between privacy and security or developing new policies for federal counterintelligence. However, based on the primary and secondary source material collected for this thesis,

setting up DHS intelligence structure, managing the domestic intelligence process, sharing information, ensuring internal analytical quality, and incorporating open source information, represent the most important issues requiring immediate solutions. Organizational "growing pains" exist with the creation of any new agency. A great naval officer, John Paul Jones, in engagement between the *Bonhomme Richard* and the *Serapis*, once said, "I have not yet begun to fight."[131] March 1, 2003, marked the date when most of the 22 disparate agencies officially moved into the new Department of Homeland Security. That date marked only the beginning for the new department. DHS personnel currently engage in the process of mobilizing an effective internal intelligence organization. The new department is just beginning its fight to prevent future attacks against the American homeland. Intelligence will play a pivotal role in the new DHS. The new DHS faces many challenges. Solving the intelligence issues described in this thesis will allow the new Department of Homeland Security and its intelligence division to accomplish its assigned mission, protecting the American homeland.

B. KEY TAKEAWAYS FOR DHS OFFICIALS

The following is a list of recommended solutions for DHS policymakers.

1. The Military Intelligence Model is a Good Place to Start

Develop an intelligence organizational structure based on military intelligence. Create a centralized command structure capable of collecting and utilizing all-source intelligence. In addition, the new department needs to ensure a decentralized information sharing system is in place to disseminate raw intelligence and analyses to first responders on the frontlines of homeland defense. The success of military intelligence in joint warfare provides a model for DHS officials. The military's intelligence model has a history of success in providing all-source intelligence to support operational units. The main contribution the military can make to DHS is providing a security mindset that deals with doctrine, tactics, procedures, and required skill-set for homeland security. For example, the Navy's Ocean Surveillance System during the Cold War effectively utilized all-source intelligence to monitor Soviet Navy activity. The naval intelligence community demonstrated a mastery of operational intelligence (OPINTEL) support. The

[131] *Reef Points 1997-98.* (Annapolis, Maryland: United States Naval Academy Character Development Division, 1997) 215.

new DHS intelligence entity will require the ability to provide timely OPINTEL to DHS policymakers and homeland security operational units.

2. Don't Forget OSINT

DHS intelligence analysts cannot rely solely on classified information from other agencies. Analysts cannot afford to disregard or discredit OSINT. DHS intelligence assessments must incorporate OSINT. Understanding the philosophy and strategic objectives of potential threats posed by the likes of Islamic fundamentalist groups do not lie inside "secret vaults." Open source information provides a valuable piece of the DHS intelligence "big picture."

3. Establish a "Personal" Information Sharing System Now

The DHS intelligence entity will require coordination between federal, state, and local agencies. State and local agencies need to know there is no "green door" to the intelligence community in Washington D.C. DHS must develop an intelligence information sharing system that harnesses the effort of the entire country. In the short-term, the department's intelligence personnel should strive to build and rely on personal networking. Establishing a Homeland Security Community of Practice will create an epistemic community of expertise focused on domestic intelligence. Through an informal and unclassified personal networking system, DHS intelligence analysts can conduct all-source fusion of intelligence spanning across federal, state, and local levels. Developing close liaison with national intelligence agencies such as the CIA, NSA, and NORTHCOM is also required. In addition, DHS personnel should establish a liaison network with state and local authorities, and organizations overseas. The long-term establishment of secure information sharing networks and technologically enhanced data basing and data mining systems will be a critical factor in the new department's mission success. However, these advanced systems require resources and appropriations not currently available. The short-term solution to information sharing resides with establishing personal networks or communities of practice.

4. Ensure Analytical Quality

One of the most controversial issues is analytical quality. Legislation for the new department indicates DHS is primarily a consumer of intelligence. In testimony before the Senate Governmental Affairs Committee on 26 February 2003, Homeland Security

Deputy Secretary Gordon England said the new department would not have its own intelligence analysis group, even though the law establishing the department gives it broad authority to receive and analyze information form across the government in order to protect the nation from terrorist attacks.[132] However, the findings presented here indicate otherwise. The new DHS intelligence entity will require a cadre of skilled intelligence analysts. DHS personnel will have to sort through vast amounts of information, both classified and unclassified, and produce timely intelligence assessments to support DHS policymakers. Assessments and analyses from other agencies will have to match with analysis of critical infrastructure. Threat analysis and target vulnerability assessments will have to fuse together in order to inform DHS decision makers and homeland security operational units. With multiple agencies such as the CIA, FBI, NSA, and NORTHCOM, providing all-source intelligence, DHS personnel assigned to the Information Analysis and Infrastructure Protection (IAIP) division will require enhanced analytical quality. The new DHS must recruit and develop a cadre of skilled intelligence analysts. DHS policy and resource allocation must emphasize the importance of DHS analyst recruitment. The department's intelligence analyst positions are not collateral duties. If viewed as a collateral duty, second-class DHS intelligence analysts will result. The country will be no safer.

C. TO KNOW THE ENEMY IS TO KNOW ONESELF

In the words of the great strategist Sun Tzu, "Know the enemy and know yourself; in a hundred battles you will never be in peril."[133] DHS officials must understand and create the necessary components within the new Department of Homeland Security. Intelligence—timely, accurate and useful information about threats that can be used by police or military units to stop terrorist incidents before they occur—is the basis of any successful effort to combat the threat of domestic terrorism.[134] In the new department, intelligence must play a proactive and focused role in detection and deterrence. Knowing the enemy starts with knowing yourself. In order to deter future

[132] Shane Harris. "Homeland Security cedes intelligence role." *Government Executive Magazine.* 26 February 2003, 1. Retrieved from Government Executive Website on 28 February 2003 at: http://govexec.com/dailyfed/0203/022603h1.htm.

[133] Sun Tzu, *Art of War*, translated and introduction by Samuel B. Griffith, foreword by B. H. Liddell Hart (London: Oxford University Press, 1963) 84.

[134] Channell, 1.

terrorists threats to Americans, their infrastructure, and most importantly their way of life, DHS policymakers must clearly define the role of intelligence and address the intelligence issues facing the new Department of Homeland Security.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. PROLOGUE

A. REAL WORLD APPLICATION

A concise application of theory to real world problems leads to mission success. This thesis examined the role of intelligence in the new Department of Homeland Security and the intelligence issues DHS policymakers need to address in order to create an organization to deter future terrorists attacks on US soil. Research for this thesis tapped into a variety of primary and secondary sources. Unquestionably, intelligence will play a critical role in the new Department of Homeland Security. The research and analysis presented in this thesis aims to serve more than just DHS policymakers. This thesis serves a second purpose, supporting the education of federal, state, and local government officials (civilian and military) with homeland security responsibilities.

B. SUPPORTING A NEW HOMELAND SECURITY MASTER'S PROGRAM

On 06 January 2003, the Naval Postgraduate School, in conjunction with the Department of Homeland Security and the Justice Department, started the first master's program to study homeland defense and security. The Homeland Security curriculum came about in response to the attacks of 11 September 2001 and President Bush's demand to build a homeland security effort. Homeland security officials need to develop a cadre of people who can develop a preventive homeland security plan. The program covers a wide range of subjects related to terrorism, security, and civil-military relations.[135] The purpose of the program is three-fold: 1) prepare local and state leaders for future Homeland Security challenges, 2) equip leaders with the specialized knowledge and skills they will need, and 3) promote and build interagency cooperation at the local, State, and Federal levels.[136] Students and faculty at the from the Naval Postgraduate School's national security affairs, computer security, operations research, and international affairs curricula designed the courses for the new Homeland Security Curriculum. One of the core-courses for the new Homeland Security Curriculum is

[135] Kevin Howe, "NPS Master's Program First in the U.S," *Monterey County Herald,* 06 January 2003.

[136] "Homeland Security Leadership Development: New Master's Degree Program—Executive Education for Tomorrow's Homeland Security." *Center for Contemporary Conflict website*. Retrieved from Center for Contemporary Conflict Website on 28 February 2003 at: www.ccc.nps.navy.mil/nsa/homeSecurity.asp.

NS4156 “Intelligence Support to Homeland Security.” The research and findings of this thesis provide a foundation for the new course. The new course on intelligence will incorporate the source material, issues, and conclusions presented in this thesis. The course design aims to shape and sharpen the intelligence and intelligence processes needed to support homeland security across federal, state, and local levels. For more information on the new Homeland Security master’s program at the Naval Postgraduate School go to the Homeland Security Leadership Development website at www.hsld.org.

Conducting research as a graduate school student helped uncover some of the ‘ground truth’ about homeland security and the role intelligence should play. Incorporating the findings of this thesis into a new intelligence course for Homeland Security Curriculum students at the Naval Postgraduate School will help arm leaders in America’s homeland security effort. The course hopes to provide personnel assigned with homeland security responsibilities the necessary intelligence problem-solving skills, along with “new” insights on intelligence, and “new” approaches to respond to the President’s top priority—to deter, defeat, and respond to domestic terrorist threats.

APPENDIX A. DEPARTMENT OF HOMELAND SECURITY REORGANIZATION PLAN, 25 NOVEMBER 2002

Source: US Department of Homeland Security website, www.dhs.gov/interweb/assetlibrarty/reorganization_plan.pdf.

Introduction

This Reorganization Plan is submitted pursuant to Section 1502 of the Department of Homeland Security Act of 2002 ("the Act"), which requires submission, not later than 60 days after enactment, of a reorganization plan regarding two categories of information concerning plans for the Department of Homeland Security ("the Department" or "DHS"):

(1) The transfer of agencies, personnel, assets, and obligations to the Department pursuant to this Act.

(2) Any consolidation, reorganization, or streamlining of agencies transferred to the Department pursuant to this Act. Section 1502(a).

Section 1502(b) of the Act identifies six elements, together with other elements "as the President deems appropriate," as among those for discussion in the plan. Each of the elements set out in the statute is identified *verbatim* below, followed by a discussion of current plans with respect to that element.

This plan is subject to modification pursuant to Section 1502(d) of the Act, which provides that on the basis of consultations with appropriate congressional committees the President may modify or revise any part of the plan until that part of the plan becomes effective. Additional details concerning the process for establishing the Department will become available in the coming weeks and months, and the President will work closely with Congress to modify this plan consistent with the Act.

Plan Elements

(1) Identification of any functions of agencies transferred to the Department pursuant to this Act that will not be transferred to the Department under the plan.

Except as otherwise directed in the Act, all functions of agencies that are to be transferred to the Department pursuant to the Act will be transferred to the Department under the plan. The functions of agencies being transferred to the Department which the Act directs are not to be transferred are the following:

• Pursuant to Section 201(g)(1) of the Act, the Computer Investigations and Operations Section ("CIOS") of the National Infrastructure Protection

Center ("NIPC") of the Federal Bureau of Investigation ("FBI") will not transfer to the Department with the rest of NIPC. CIOS is the FBI headquarters entity responsible for managing all FBI computer intrusion field office cases (whether law enforcement or national security related).

• Pursuant to Sections 421(c) & (d) of the Act, the regulatory responsibilities and quarantine activities relating to agricultural import and entry inspection activities of the United States Department of Agriculture ("the USDA") Animal and Plant Health Inspection Service ("APHIS") will remain with the USDA, as will the Secretary of Agriculture's authority to issue regulations, policies, and procedures regarding the functions transferred pursuant to Sections 421(a) & (b) of the Act.

• Pursuant to Subtitle B of Title IV of the Act, the authorities of the Secretary of the Treasury related to Customs revenue functions, as defined in the statute, will not transfer to the Department.

• Functions under the immigration laws of the United States with respect to the care of unaccompanied alien children will not transfer from the Department of Justice to DHS, but will instead transfer to the Department of Health and Human Services pursuant to Section 462 of the Act.

(2) Specification of the steps to be taken by the Secretary to organize the Department, including the delegation or assignment of functions transferred to the Department among officers of the Department in order to permit the Department to carry out the functions transferred under the plan.

A. Steps to be taken by the Secretary to organize the Department. The President intends that the Secretary will carry out the following actions on the dates specified. All of the following transfers shall be deemed to be made to DHS, and all offices and positions to be established and all officers and officials to be appointed or named shall be deemed to be established, appointed, or named within DHS.

January 24, 2003 (effective date of the Act pursuant to Section 4):

• Establish the Office of the Secretary.
• Begin to appoint, upon confirmation by the Senate, or transfer pursuant to the transfer provisions of the Act, as many of the following officers as may be possible:
(1) Deputy Secretary of Homeland Security
(2) Under Secretary for Information Analysis and Infrastructure Protection
(3) Under Secretary for Science and Technology
(4) Under Secretary for Border and Transportation Security

(5) Under Secretary for Emergency Preparedness and Response
(6) Director of the Bureau of Citizenship and Immigration Services
(7) Under Secretary for Management
(8) Not more than 12 Assistant Secretaries
(9) General Counsel
(10) Inspector General
(11) Commissioner of Customs

• Name, as soon as may be possible, officers to fill the following offices created by the Act:

(1) Assistant Secretary for Information Analysis
(2) Assistant Secretary for Infrastructure Protection
(3) Privacy Officer
(4) Director of the Secret Service
(5) Chief Information Officer
(6) Chief Human Capital Officer
(7) Chief Financial Officer
(8) Officer for Civil Rights and Civil Liberties
(9) Director of Shared Services
(10) Citizenship and Immigration Ombudsman
(11) Director of the Homeland Security Advanced Research Projects Agency

• Establish, within the Office of the Secretary, the Office for State and Local Government Coordination, the Office of International Affairs, and the Office of National Capital Region Coordination.

• Establish the Homeland Security Advanced Research Projects Agency and the Acceleration Fund for Research and Development of Homeland Security Technologies.

• Establish within the Directorate of Science and Technology the Office for National Laboratories.

• Establish the Bureau of Border Security, the Bureau of Citizenship and Immigration Services, and the Director of Shared Services.

• Establish the Transportation Security Oversight Board with the Secretary of Homeland Security as its Chair.

March 1, 2003:

• Transfer the Critical Infrastructure Assurance Office ("CIAO") of the Department of Commerce, the National Communications System ("the

NCS"), the NIPC of the FBI (other than the CIOS), the National Infrastructure Simulation and Analysis Center ("NISAC"), the Energy Assurance Office ("EAO") of the Department of Energy, and the Federal Computer Incident Response Center of the General Services Administration ("FedCIRC")

• Transfer the Coast Guard.

• Transfer the Customs Service, the Transportation Security Administration ("the TSA"), functions of the Immigration and Naturalization Service ("the INS"), the Federal Protective Service ("the FPS"), the Office of Domestic Preparedness ("the ODP"), and the Federal Law Enforcement Training Center ("the FLETC").

• Transfer the functions of the Secretary of Agriculture relating to agricultural import and entry inspection activities under the laws specified in Section 421(b) of the Act from the Animal and Plant Health Inspection Service.

• Transfer the United States Secret Service.

• Transfer the following programs and activities to the Directorate of Science and Technology:

- The chemical and biological national security and supporting programs and activities of the nonproliferation and verification research and development program of the Department of Energy.
- The life sciences activities related to microbial pathogens of the Biological and Environmental Research Program of the Department of Energy.
- The National Bio-Weapons Defense Analysis Center of the Department of Defense.
- The nuclear smuggling programs and activities within the proliferation detection program of the nonproliferation and verification research and development program of the Department of Energy.
- The nuclear assessment program and activities of the assessment, detection, and cooperation program of the international materials protection and cooperation program of the Department of Energy and the advanced scientific computing research program and activities at Lawrence Livermore National Laboratory of the Department of Energy.
- The Environmental Measurements Laboratory of the Department of Energy.

• Transfer the Federal Emergency Management Agency ("FEMA").

• Transfer the Integrated Hazard Information System of the National Oceanic and Atmospheric Administration, which shall be renamed "FIRESTAT."

• Transfer the National Domestic Preparedness Office of the FBI, including the functions of the Attorney General relating thereto.

• Transfer the Domestic Emergency Support Team of the Department of Justice, including the functions of the Attorney General relating thereto.

• Transfer the Metropolitan Medical Response System of the Department of Health and Human Services, including the functions of the Secretary of Health and Human Services and Assistant Secretary for Public Health Emergency Preparedness relating thereto.

• Transfer the National Disaster Medical System of the Department of Health and Human Services, including the functions of the Secretary of Health and Human Services and Assistant Secretary for Public Health Emergency Preparedness relating thereto.

• Transfer the Office of Emergency Preparedness and the Strategic National Stockpile of the Department of Health and Human Services, including the functions of the Secretary of Health and Human Services and Assistant Secretary for Public Health Emergency Preparedness relating thereto.

• Transfer to the Secretary the authority (in connection with an actual or threatened terrorist attack, major disaster, or other emergency in the United States) to direct the Nuclear Incident Response Team of the Department of Energy to operate as an organizational unit.

June 1, 2003:

• Transfer the Plum Island Animal Disease Center of USDA.

• Establish the Homeland Security Science and Technology Advisory Committee.

By September 30, 2003:

• Complete any incidental transfers, pursuant to Section 1516 of the Act, of personnel, assets, and liabilities held, used, arising from, available, or to be made available, in connection with the functions transferred by the Act.

B. Delegation or Assignment Among Officers of Functions Transferred to the Department. The President intends that the Secretary will delegate or assign transferred functions within the Department as follows:

1. Information Analysis and Infrastructure Protection

a. Under Secretary for Information Analysis and Infrastructure Protection ("IA and IP"): Will be responsible for oversight of functions of NIPC, NCS, CIAO, NISAC, EAO, and FedCIRC transferred by the Act, the management of the Directorate's Information Analysis and Infrastructure Protection duties, and the administration of the Homeland Security Advisory System.

b. Assistant Secretary for Information Analysis: Will oversee the following Information Analysis functions:

• Identify and assess the nature and scope of terrorist threats to the homeland; detect and identify threats of terrorism against the United States; and, understand such threats in light of actual and potential vulnerabilities of the homeland.

• In coordination with the Assistant Secretary for Infrastructure Protection, integrate relevant information, analyses, and vulnerability assessments (whether such information, analyses, or assessments are provided or produced by the Department or others) in order to identify priorities for protective and support measures by the Department, other agencies of the Federal Government, State and local government agencies and authorities, the private sector, and other entities.

• Ensure the timely and efficient access by the Department to all information necessary to discharge the responsibilities under Section 201 of the Act, including obtaining such information from other agencies of the Federal Government.

• Review, analyze, and make recommendations for improvements in the policies and procedures governing the sharing of law enforcement information, intelligence information, intelligence-related information, and other information relating to homeland security within the Federal Government and between the Federal Government and State and local government agencies and authorities.

• Disseminate, as appropriate, information analyzed by the Department within the Department, to other agencies of the Federal Government with responsibilities relating to homeland

security, and to agencies of State and local governments and private sector entities with such responsibilities in order to assist in the deterrence, prevention, preemption of, or response to, terrorist attacks against the United States.

• Consult with the Director of Central Intelligence and other appropriate intelligence, law enforcement, or other elements of the Federal Government to establish collection priorities and strategies for information, including law enforcement-related information, relating to threats of terrorism against the United States through such means as the representation of the Department in discussions regarding requirements and priorities in the collection of such information.

• Consult with State and local governments and private sector entities to ensure appropriate exchanges of information, including law enforcement-related information, relating to threats of terrorism against the United States.

• Ensure that—

1. Any material received pursuant to the Act is protected from unauthorized disclosure and handled and used only for the performance of official duties; and

2. Any intelligence information under the Act is shared, retained, and disseminated consistent with the authority of the Director of Central Intelligence to protect intelligence sources and methods under the National Security Act of 1947 (50 U.S.C. Section 401, et seq.) and related procedures and, as appropriate, similar authorities of the Attorney General concerning sensitive law enforcement information.

• Request additional information from other agencies of the Federal Government, State and local government agencies, and the private sector relating to threats of terrorism in the United States, or relating to other areas of responsibility assigned by the Secretary, including the entry into cooperative agreements through the Secretary to obtain such information.

• Establish and utilize, in conjunction with the Chief Information Officer of the Department, a secure communications and information technology infrastructure, including data-mining and other advanced analytical tools, in order to access, receive, and analyze data and information in furtherance of statutory

responsibilities, and to disseminate information acquired and analyzed by the Department, as appropriate.

• Ensure, in conjunction with the Chief Information Officer of the Department, that any information databases and analytical tools developed or utilized by the Department—

1. Are compatible with one another and with relevant information databases of other agencies of the Federal Government; and

2. Treat information in such databases in a manner that complies with applicable Federal law on privacy.

• Coordinate training and other support to the elements and personnel of the Department, other agencies of the Federal Government, and State and local governments that provide information to the Department, or are consumers of information provided by the Department, in order to facilitate the identification and sharing of information revealed in their ordinary duties and the optimal utilization of information received from the Department.

• Coordinate with elements of the intelligence community and with Federal, State, and local law enforcement agencies, and the private sector, as appropriate.

• Provide intelligence and information analysis and support to other elements of the Department.

c. Assistant Secretary for Infrastructure Protection: Will oversee the following Infrastructure Protection functions:

• Carry out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States, including the performance of risk assessments to determine the risks posed by particular types of terrorist attacks within the United States (including an assessment of the probability of success of such attacks and the feasibility and potential efficacy of various countermeasures to such attacks).

• In coordination with the Assistant Secretary for Information Analysis, integrate relevant information, analyses, and vulnerability assessments (whether such information, analyses, or assessments are provided or produced by the Department or others) in order to identify priorities for protective and support measures by the Department, other agencies of the Federal Government, State and local government agencies and authorities, the private sector, and other entities.

• Develop a comprehensive national plan for securing the key resources and critical infrastructure of the United States, including power production, generation, and distribution systems, information technology and telecommunications systems (including satellites), electronic financial and property record storage and transmission systems, emergency preparedness communications systems, and the physical and technological assets that support such systems.

• Recommend measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other agencies of the Federal Government and in cooperation with State and local government agencies and authorities, the private sector, and other entities.

• In coordination with the Under Secretary for Emergency Preparedness and Response, provide to State and local government entities, and upon request to private entities that own or operate critical information systems, crisis management support in response to threats to, or attacks on, critical information systems.

• Provide technical assistance, upon request, to the private sector and other government entities, in coordination with the Under Secretary for Emergency Preparedness and Response, with respect to emergency recovery plans to respond to major failures of critical information systems.

• Coordinate with other agencies of the Federal Government to provide specific warning information, and advice about appropriate protective measures and countermeasures, to State and local government agencies and authorities, the private sector, other entities, and the public.

2. Science and Technology

Under Secretary for Science and Technology: Will be responsible for performing the functions set forth in Section 302 of the Act, including the following:

• Advise the Secretary regarding research and development efforts and priorities in support of the Department's missions.

• Develop, in consultation with other appropriate executive agencies, a national policy and strategic plan for identifying priorities, goals, objectives, and policies for, and coordinating the Federal Government's civilian efforts with respect to, identifying

and developing countermeasures to chemical, biological, radiological, nuclear, and other emerging terrorist threats, including the development of comprehensive, research based definable goals for such efforts and of annual measurable objectives and specific targets to accomplish and evaluate the goals for such efforts.

• Support the Under Secretary for Information Analysis and Infrastructure Protection by assessing and testing homeland security vulnerabilities and possible threats.

• Conduct basic and applied research, development, demonstration, testing, and evaluation activities that are relevant to any or all elements of the Department, through both intramural and extramural programs, except that such responsibility does not extend to human health-related research and development activities.

• Establish priorities for directing, funding, and conducting national research, development, test and evaluation, and procurement of technology and systems for—

1. Preventing the importation of chemical, biological, radiological, nuclear, and related weapons and material; and

2. Detecting, preventing, protecting against, and responding to terrorist attacks.

• Establish a system for transferring homeland security developments or technologies to Federal, State, and local governments, and to private sector entities.

• Enter into work agreements, joint sponsorships, contracts, or any other agreements with the Department of Energy regarding the use of the national laboratories or sites and support of the science and technology base at those facilities.

• Collaborate with the Secretary of Agriculture and the Attorney General as provided in Section 212 of the Agricultural Bioterrorism Protection Act of 2002 (7 U.S.C. § 8401), as amended by Section 1709(b) of the Act.

• Collaborate with the Secretary of Health and Human Services and the Attorney General in determining any new biological agents and toxins that shall be listed as ‘select agents’ in Appendix A of

part 72 of title 42, Code of Federal Regulations, pursuant to Section 351A of the Public Health Service Act (42 U.S.C. § 262a).

• Support United States leadership in science and technology.

• Establish and administer the primary research and development activities of the Department, including the long-term research and development needs and capabilities for all elements of the Department.

• Coordinate and integrate all research, development, demonstration, testing, and evaluation activities of the Department.

• Coordinate with other appropriate executive agencies in developing and carrying out the science and technology agenda of the Department to reduce duplication and identify unmet needs.

• Develop and oversee the administration of guidelines for merit review of research and development projects throughout the Department, and for the dissemination of research conducted or sponsored by the Department.

3. Border and Transportation Security

The Directorate of Border and Transportation Security ("BTS") will include the following: the Bureau of Border Security; the Office for Domestic Preparedness; the Customs Service; the Transportation Security Administration; FLETC; and FPS.

The BTS Directorate will also have in place the key leaders of the new Directorate to include:

a. Under Secretary for BTS: Will be responsible for oversight of all responsibilities set forth in Section 402 of the Act, including the following:

• Prevent the entry of terrorists and the instruments of terrorism into the United States.

• Secure the borders, territorial waters, ports, terminals, waterways, and air, land, and sea transportation systems of the United States, including managing and coordinating those functions transferred to the Department at ports of entry.

• Establish and administer rules, in accordance with Section 428 of the Act, governing the granting of visas or other forms of permission, including parole, to enter the United States to

individuals who are not a citizen or an alien lawfully admitted for permanent residence in the United States.

• Establish national immigration enforcement policies and priorities.

• Administer the customs laws of the United States, except as otherwise provided in the Act.

• Conduct the inspection and related administrative functions of the USDA transferred to the Secretary of Homeland Security under Section 421 of the Act.

• In carrying out the foregoing responsibilities, ensure the speedy, orderly, and efficient flow of lawful traffic and commerce.

• Carry out the immigration enforcement functions specified under Section 441 of the Act that were vested by statute in, or performed by, the Commissioner of the INS (or any officer, employee, or component of the INS) immediately before the date on which the transfer of functions takes place.

b. Assistant Secretary for Border Security: Will report directly to the Under Secretary for Border and Transportation Security, and whose responsibilities will include the following:

• Establish and oversee the administration of the policies for performing such functions as are--

1. Transferred to the Under Secretary for Border and Transportation Security by Section 441 of the Act and delegated to the Assistant Secretary by the Under Secretary for Border and Transportation Security; or

2. Otherwise vested in the Assistant Secretary by law.

• Advise the Under Secretary for Border and Transportation Security with respect to any policy or operation of the Bureau of Border Security that may affect the Bureau of Citizenship and Immigration.

c. Director of the Office for Domestic Preparedness - Will report directly to the Under Secretary for Border and Transportation Security and will have the primary responsibility within the Executive Branch of the Federal Government for the preparedness of the United States for acts of terrorism, including the following responsibilities:

• Coordinate preparedness efforts at the Federal level, and work with all State, local, tribal, parish, and private sector emergency response providers on all matters pertaining to combating terrorism, including training, exercises, and equipment support.

• Coordinate or, as appropriate, consolidate communications and systems of communications relating to homeland security at all levels of government.

• Direct and supervise terrorism preparedness grant programs of the Federal Government (other than those programs administered by the Department of Health and Human Services) for all emergency response providers.

• Incorporate homeland security priorities into planning guidance on an agency level for the preparedness efforts of the Office for Domestic Preparedness.

• Provide agency-specific training for agents and analysts within the Department, other agencies, and State and local agencies, and international entities.

• As the lead executive branch agency for preparedness of the United States for acts of terrorism, cooperate closely with the FEMA, which shall have the primary responsibility within the executive branch to prepare for and mitigate the effects of nonterrorist-related disasters in the United States.

• Assist and support the Secretary, in coordination with other Directorates and entities outside the Department, in conducting appropriate risk analysis and risk management activities of State, local, and tribal governments consistent with the mission and functions of the Directorate.

• Supervise those elements of the Office of National Preparedness of FEMA that relate to terrorism, which shall be consolidated within the Department in the ODP established pursuant to Section 430 of the Act.

4. Emergency Preparedness and Response

The Emergency Preparedness and Response Directorate will be headed by the Under Secretary for Emergency Preparedness and Response.

Under Secretary for EP&R: Will be responsible for all of those functions included within Section 502 of the Act, including:

• Helping to ensure the effectiveness of emergency response providers to terrorist attacks, major disasters, and other emergencies.

• With respect to the Nuclear Incident Response Team (regardless of whether it is operating as an organizational unit of the Department pursuant to the Act):

1. Establishing standards and certifying when those standards have been met;

2. Conducting joint and other exercises and training and evaluating performance; and,

3. Providing funds to the Department of Energy and the Environmental Protection Agency, as appropriate, for homeland security planning, exercises and training, and equipment.

• Providing the Federal Government's response to terrorist attacks and major disasters, including:

1. Managing such response;

2. Directing the Domestic Emergency Support Team, the Strategic National Stockpile, the National Disaster Medical System, and (when operating as an organizational unit of the Department pursuant to the Act) the Nuclear Incident Response Team;

3. Overseeing the Metropolitan Medical Response System; and

4. Coordinating other Federal response resources in the event of a terrorist attack or major disaster.

• Aiding the recovery from terrorist attacks and major disasters;

• Building a comprehensive national incident management system with Federal, State, and local government personnel, agencies, and authorities, to respond to such attacks and disasters.

• Consolidating existing Federal Government emergency response plans into a single, coordinated national response plan; and

• Developing comprehensive programs for developing interoperative communications technology, and helping to ensure that emergency response providers acquire such technology.

5. Other Officers and Functions

a. Director of the Bureau of Citizenship and Immigration Services: Will report directly to the Deputy Secretary; and will be responsible for the following:

• Establishing the policies for performing such functions as are transferred to the Director by Section 451 of the Act or otherwise vested in the Director by law.

• Oversight of the administration of such policies.

• Advising the Deputy Secretary with respect to any policy or operation of the Bureau of Citizenship and Immigration Services that may affect the Bureau of Border Security of the Department, including potentially conflicting policies or operations.

• Establishing national immigration services policies and priorities.

• Meeting regularly with the Ombudsman described in Section 452 of the Act to correct serious service problems identified by the Ombudsman.

• Establishing procedures requiring a formal response to any recommendations submitted in the Ombudsman's annual report to Congress within three months after its submission to Congress.

b. Citizenship and Immigration Services Ombudsman: Will report directly to the Deputy Secretary; and will be responsible for the following:

• Assisting individuals and employers in resolving problems with the Bureau of Citizenship and Immigration Services;

• Identifying areas in which individuals and employers have problems in dealing with the Bureau of Citizenship and Immigration Services; and

• Proposing changes in the administrative practices of the Bureau of Citizenship and Immigration Services to mitigate identified problems.

(3) Specification of the funds available to each agency that will be transferred to the Department as a result of transfers under the plan.

• The attached tables provide estimates of the funds available to the agencies and entities that will be transferred to the Department by operation of the Act. The two tables include total funding (mandatory and discretionary including fees) and discretionary funding net of fees. The tables provide the enacted levels for 2002 and 2002 supplementals, and the President's requested levels for
2003.

Because of the current state of the 2003 budget process, information concerning the funds that will be available to each transferring agency on the date of the proposed transfers is not currently available and will not likely be available during the time period in which the President is to submit this Reorganization Plan. As additional information becomes available, it will be provided as may be required in accordance with the procedures under the Act for modification of this Plan or other applicable law.

(4) Specification of the proposed allocations within the Department of unexpended funds transferred in connection with transfers under the plan.

• The attached tables provide estimates of the unobligated balances as of September 30, 2002, for the agencies and programs that will be transferred to the Department. The first table provides estimates of unobligated balances for the accounts that are moving to the Department in whole. The second table provides estimates of the unobligated balances in the accounts of which only a portion will be transferring to the new Department. These latter estimates, however, are of the unobligated balances for the full account, only a portion of which are associated with the activities that will be transferred to the Department. In addition, these unobligated balances are based on the Department of Treasury's estimates as of September 30, 2002, which are the latest available figures. Since October 1, 2002, Departments and agencies (except the Department of Defense) have been operating under continuing resolutions, and, as such, have been spending these balances to maintain current operations.

Authority to reallocate unexpended funds of agencies transferred under this Plan is found in H.J. Res. 124, the continuing resolution in effect currently and until January 11, 2003. The resolution provides authority for the Office of Management and Budget to transfer an amount not to exceed $140,000,000 from unobligated balances of appropriations enacted before October 1, 2002 "for organizations and entities that will be transferred to the new Department and for salaries and expenses associated with the initiation of the Department." Such authority may be exercised upon providing 15 days' notice to the Appropriations Committees. We anticipate that it may be necessary to provide funding through such transfers both for transferring entities and for salaries and expenses

associated with the initiation of the Department, including, for example, those associated with establishing the Office of the Secretary and other new offices provided for in the Act. Any plan to use such funding will follow the procedures required under the continuing resolution, including the provision of at least 15 days' notice to the Appropriations Committees.

(5) Specification of any proposed disposition of property, facilities, contracts, records, and other assets and obligations of agencies transferred under the plan.

• There is no intention to dispose of property, facility, contracts, records, and other assets and obligations of agencies transferred under the plan. All of such assets and obligations will transfer with each agency pursuant to Section 1511(d)(1) of the Act.

• Prior to and during the transition period (as defined by Section 1501(a)(2) of the Act), the Department may identify property, facilities, contracts, records, and other assets and obligations of agencies transferred that would be candidates for disposition due to duplication, non-use, obsolescence, and the like. If and when any such proposed dispositions are identified, we will follow provisions of the Act relating to modification of this plan or further notification of Congress.

(6) Specification of the proposed allocations within the Department of the functions of the agencies and subdivisions that are not related directly to securing the homeland.

• As agencies and subdivisions are transferred into the Department, any functions of those entities that are not directly related to securing the homeland will continue to be allocated to the agencies and subdivisions in which they are currently incorporated.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. LIST OF CURRENT DHS SENIOR LEADERSHIP AND THEIR NOMINATION STATUS

Secretary: Governor Tom Ridge

On October 8, 2001, Tom Ridge was sworn in as the first Office of Homeland Security Advisor in the history of the United States of America.

Deputy Secretary: Gordon England

On January 30, Gordon England was confirmed as Deputy Secretary, Department of Homeland Security.

Under Secretary for Border & Transportation Security: Asa Hutchinson

On January 23, Asa Hutchinson was confirmed as Under Secretary for Border and Transportation Security.

Under Secretary for Science and Technology: Dr. Charles E. McQueary

On January 10, President Bush announced his intention to nominate Dr. Charles E. McQueary to be Under Secretary for Science and Technology.

Under Secretary for Management: Janet Hale

President Bush intends to nominate Janet Hale as Under Secretary for Management. Ms. Hale is currently the Assistant Secretary for Budget, Technology and Finance for the U.S. Department of Health and Human Services

Under Secretary of Emergency Preparedness & Response: Michael Brown

President Bush announced on January 10 his intention to nominate Michael Brown as the first Under Secretary of Emergency Preparedness and Response (EP&R) in the newly created Department of Homeland Security.

Inspector General: Clark Kent Ervin

President Bush has announced his intention to nominate Clark Kent Ervin as Inspector General. Mr. Ervin currently serves as Inspector General of the Department of State.

Director, United States Secret Service: W. Ralph Basham

Since January 2002, Mr. Basham has served as Chief of Staff for the Transportation Security Administration (TSA). Among his responsibilities at TSA, Mr. Basham oversaw the hiring of federal security directors for the nation's 429 airports.

Commandant, U.S. Coast Guard: Admiral Thomas H. Collins

Admiral Thomas H. Collins assumed the duties of Commandant of the U.S. Coast Guard on May 30th, 2002. His leadership priorities are readiness, people and stewardship.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION (IAIP) DIVISION GUIDANCE

(***Source***: *US Department of Homeland Security website,* http://www.dhs.gov/dhspublic/display?theme=52.)

Synthesizing and Disseminating Information.

The Department of Homeland Security, through the Directorate of Information Analysis and Infrastructure Protection (IAIP) will merge under one roof the capability to identify and assess current and future threats to the homeland, map those threats against our vulnerabilities, issue timely warnings and take preventive and protective action.

Intelligence Analysis and Alerts.

Actionable intelligence - that is, information which can lead to stopping or apprehending terrorists--is essential to the primary mission of DHS. The timely and thorough analysis and dissemination of information about terrorists and their activities will improve the government's ability to disrupt and prevent terrorist acts and to provide useful warning to the private sector and our population. The Directorate will fuse and analyze information from multiple sources pertaining to terrorist threats. The Department will be a full partner and consumer of all intelligence-generating agencies, such as the National Security Agency, the CIA, and the FBI.

The Department's threat analysis and warning functions will support the President and, as he directs, other national decision-makers responsible for securing the homeland from terrorism. It will coordinate and, as appropriate, consolidate the federal government's lines of communication with state and local public safety agencies and with the private sector, creating a coherent and efficient system for conveying actionable intelligence and other threat information. The IAIP Directorate will also administer the Homeland Security Advisory System.

As designed, IAIP fully reflects the President's commitment to safeguard our way of life, including the integrity of our democratic political system and the essential elements of our individual liberty. To further ensure such protections, DHS will establish an office for a chief Privacy Officer.

Critical Infrastructure Protection.

The attacks of September 11 highlighted the fact that terrorists are capable of causing enormous damage to our country by attacking our critical infrastructure -food, water, agriculture, and health and emergency services; energy sources (electrical, nuclear, gas and oil, dams); transportation (air, road, rail, ports, waterways); information and

telecommunications networks; banking and finance systems; postal and other assets and systems vital to our national security, public health and safety, economy and way of life.

Protecting America's critical infrastructure is the shared responsibility of federal, state, and local government, in active partnership with the private sector, which owns approximately 85 percent of our nation's critical infrastructure. IAIP will take the lead in coordinating the national effort to secure the nation's infrastructure. This will give state, local, and private entities one primary contact instead of many for coordinating protection activities within the federal government, including vulnerability assessments, strategic planning efforts, and exercises.

Cyber Security.

Our nation's information and telecommunications systems are directly connected to many other critical infrastructure sectors, including banking and finance, energy, and transportation. The consequences of an attack on our cyber infrastructure can cascade across many sectors, causing widespread disruption of essential services, damaging our economy, and imperiling public safety. The speed, virulence, and maliciousness of cyber attacks have increased dramatically in recent years. Accordingly, the Directorate places an especially high priority on protecting our cyber infrastructure from terrorist attack by unifying and focusing the key cyber security activities performed by the Critical Infrastructure Assurance Office (currently part of the Department of Commerce) and the National Infrastructure Protection Center (FBI). The Directorate will augment those capabilities with the response functions of the Federal Computer Incident Response Center (General Services Administration). Because our information and telecommunications sectors are increasingly interconnected, DHS will also assume the functions and assets of the National Communications System (Department of Defense), which coordinates emergency preparedness for the telecommunications sector.

Indications and Warning Advisories. In advance of real-time crisis or attack, IAIP will provide:

- Threat warnings and advisories against the homeland including physical and cyber events.
- Processes to develop and issue national and sector-specific threat advisories through the Homeland Security Advisory System.
- Terrorist threat information for release to the public, private industry, or state and local government.

Partnerships. The IAIP team will establish:

- Partnerships with key government, public, private, and international stakeholders to create an environment that enables them to better protect their infrastructures.
- Awareness programs, development of information sharing mechanisms, and sector focused best practices and guidelines.

National Communications System. The IAIP team will provide:

- Coordination of planning and provision of National Security and Emergency Preparedness (NS/EP) communications for the Federal government

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D. LIST OF NATIONAL AND REGIONAL CONFERENCES ON HOMELAND SECURITY ATTENDED TO COLLECT RESEARCH

Note: The following is a list of national and regional conferences on homeland security and intelligence support attended, or obtained conferences summaries from, in collecting research for this thesis. In addition, the list includes presentations from officials currently tasked with homeland security responsibilities. These conferences and presentations provided a forum to discuss thesis research with intelligence and law enforcement experts at the federal, state, and local levels and uncover the 'ground truth' about the role of intelligence in the new Department of Homeland Security.

- AFCEA Fall Intelligence Symposium, DIAC, Bowling Air Force Base, 23-24 October 2002
- AFCEA and the Naval Institute West 2003, "The Next Step: From Change to Transformation," San Diego Convention Center, 14-16 January 2003
- AFCEA Intelligence Committee February meeting, "Army Intelligence's Information Dominance Center," Army Intelligence and Security Command Headquarters, Fort Belvoir, Virginia, 13 February 2003
- Association of Former Intelligence Officers (AFIO) Annual Symposium, "Terrorism, Technology, and Strategy," Northern Virginia, 01-02 November 2002
- El Paso Intelligence Center conference, "Intelligence, Security, and Terrorism: Our Role in Homeland Defense," El Paso, Texas, 17-18 September 2002
- Government Symposium for Information Sharing and Homeland Security, Philadelphia, PA, 19-21 August 2002
- Joint Military Intelligence College (JMIC) 40th Anniversary Conference, "Preparing America's Leaders," Defense Intelligence Agency's Tighe Auditorium, Bolling Air Force Base, 19 June 2002
- Los Angeles Terrorist Early Warning (TEW) group monthly meeting, Los Angeles, California, 26 September 2002
- McGraw Hill/Aviation Week & Space Technology Homeland Security Summit, Ronald Reagan International Trade Center in Washington, D.C., 06-07 May 2002.
- MGEN Bruce Lawlor, Senior Director for Protection and Prevention, Office of Homeland Security, presentation entitled "The Future of Homeland Security"

- National Defense University and University of Maryland conference, "Homeland Security: The Civil-Military Dimensions," Fort McNair, Washington, D.C., 19-20 September 2002.

APPENDIX E. 2002 GOVERNMENT SYMPOSIUM FOR INFORMATION SHARING AND HOMELAND SECURITY AFTER ACTION REPORT

Note: The following is a copy of the After Action Report written on the 2002 Government Symposium for Information Sharing and Homeland Security, Philadelphia, Pennsylvania, 19-21 August 2002.

To: Distribution
From: LT Shawn Moyer

Subject: GOVERNMENT SYMPOSIUM FOR INFORMATION SHARING AND HOMELAND SECURITY, PHILADELPHIA, PA 19-21 AUG 02

1. **Conference Summary:**

From 19-21 August 2002, I attended the Government Symposium for Information Sharing and Homeland Security in Philadelphia, Pennsylvania to obtain research to support my thesis development at NPS. The conference, sponsored by The Government Emerging Technology Alliance (GETA), brought together members of various federal, state, and local communities to address Homeland Security-related information. Co-sponsored by the US Intelligence Community, Law Enforcement Community, DoD, Federal, Local and State Agencies, the convention focuses on gathering, sharing and interpreting information across the wide spectrum of agencies tasked with contributing to Homeland Security. Government experts from the CIA, NSA, DIA, NRO, ATF, DISA, US Navy, Office of Homeland Security, IMO, IC CIO, Law Enforcement Working Group, the Departments of Justice, Interior and Energy and various other organizations planned the content and co-hosted the convention. The conference provided an initial and unprecedented attempt for experts to share insights and expertise. Most importantly, the conference highlighted the unique challenges surrounding Homeland Security.

My purpose for attending the conference was to obtain inputs from experts within the Intelligence Community and law enforcement agencies regarding what should go into developing NS3156 Intelligence Support to Homeland Security at NPS. The conference agenda included numerous plenary sessions with a wide range of keynote speakers such as Congressman Curt Weldin (7th District Pennsylvania), Steven Cooper (Special Assistant to the President, Senior Director for Information Integration and Chief Information Officer, Office of Homeland Security CIO), and Mr. Shabtai Shavit (former Head of Israeli Intelligence Agency-Mossad). The conference also broke down into four distinctive tracks: 1) Intelligence for Homeland Security: Integrating Policy, Law, and Culture, 2) Information Technology: Applicability to Information Sharing, 3) Critical Information Needs of the First Responder, and 4) Training and Education for Homeland Security. I attended the track 4 panel discussions looking to obtain inputs, resources, and insights for my thesis research.

2. Plenary Session Highlights:

The plenary sessions featured presentations from the President's Office of Homeland Security, a Media Panel, and Congressional Panel. The Media panel consisted of Broadcast, News, and Print media highlighting the critical role the Media plays in Information Sharing for Homeland Security. Discussions included the media's role to help prevent crisis, dissemination of critical information during local and national emergencies, and the responsibility of the media to cooperate with government in the dissemination of sensitive information. The Congressional panel featured representatives and senators on the various intelligence and related committees to discuss issues pertinent to information sharing and actions of Congress to fight the war against terrorism. The congressional panel highlighted a discussion on the progress on the President's proposed new Department of Homeland Security and included audience interaction.

Congressman Curt Weldin provided a motivational presentation during the first plenary session. He highlighted some of the frustrations and chaos that existed around the events of 9/11 stating, "The American government failed the American people on September 11th." The overriding theme in his speech called for the need to develop an integrated domestic communications capability because of the frustrations experienced in information sharing between the Intelligence Community and law enforcement agencies. Two outstanding issues for HLS experts to address are 1) Information sharing with the technology currently existing and 2) Taking a political stance on Homeland Defense.

Steven Cooper spoke during the second plenary session. Mr. Cooper provided a unique perspective of the challenges the Office of Homeland Security faces. He demanded the audience become thoroughly familiar with the Administration's HLS Strategy released in July. In addition, he outlined the "CONOPS for HLS" as a trinity composed of 1) National Strategy, 2) Functional Capabilities, and 3) Information. From this trinity individual agencies can see how they fit into the **national** enterprise architecture (not federal). Mr. Cooper added that pockets of experts exist in the United States; the question is how does the Office of HLS get to them? For, example the Office HLS CIO has established three working groups: 1) Border Security (farthest along), 2) First Responder Community, 3) CBRN (least amount done). Mr. Cooper emphasized the need to gather a knowledge base among various agencies within the US in order to secure the Homeland. He called upon the audience to bring forth the best practices, centers of excellence, and initiatives underway that are relevant and should be incorporated by the Office HLS. The Office of HLS is in the process of establishing an unclassified website for coordinating HLS initiatives and resources. The goal is to build upon what already exists and not to start from scratch. Lastly, he highlighted the inherent risks/challenges associated with HLS: balancing privacy and civil liberties with security, aligning policy and laws with desired outcomes, leveraging cultural beliefs and diversity to achieve collaborative change, consolidating/replicating good efforts, working together to overcome political and cultural barriers, introducing new technologies, money, and communicating expectation management. I personally enjoyed Mr. Cooper's speech because instead of making a public relations pitch he chose to highlight some of the unique challenges and tasks the Office of HLS is taking on and more importantly the need for every individual agency to become involved.

Mr. Shabtai Shavit, former director Israeli Intelligence Agency, provided one of the conference's most intriguing presentations during the third plenary session. He

provided initial background data on the workings of the Israeli Intelligence Agency (Mossad). Mossad provides Israel with a service for intelligence collection and special functions, operating outside Israeli borders. Mr. Shavit noted the Mossad does not work directly with Israeli law enforcement and security forces. He also noted "the United States needs to refine its definition of terrorism." The West has a difficulty dealing with terrorism because it mixes terrorists with guerillas, vigilantes, etc. making it difficult to identify not only the threat but also how to counter the threat. He suggested defining terrorism as the use of violence against civilians to enhance political gains. The three required components being the nature to act, the aim, and the target (civilians). Terrorism needs to be differentiated from guerilla warfare. This critical step will help the US Intelligence Community pull other resources into place. His presentation also provided a few assumptions/guidelines for intelligence: 1) protecting the secrecy of sources must be HOLY, 2) intelligence needs to get to the people who need it, 3) intelligence requires a balance of judgment and regulation, and 4) command challenges must be as concise and short as possible. The later part of his presentation focused on the similarities and differences between the Mossad and the US Intelligence Community and the implications for conducting homeland defense. In 1991, Israel established the Homefront Command to protect people. The Homefront Command was an intelligence consumer not a producer. The Homefront Command is integrated with the Israeli national intelligence system unlike the Department of Homeland Security. The Department of Homeland Security will have both regulatory and operational power requiring the US to work through establishing a system of reciprocity between consumers and producers of intelligence. On a side note, Mr. Shabit concluded you know you are winning the War on Terrorism when the enemy raises white flags from the rooftop of its houses.

Dr. Stephen Gale, Director of the Center for Organizational Dynamics, chaired a provocative fourth plenary session. Adding an academic perspective to the conference, Dr. Gale focused on the issue of information sharing. He posed three questions for HLS agencies: 1) what is it we want to sharing information for, 2) how do we organize the information under one department to make decisions, and 3) how do we develop an integrated information sharing system? He provided numerous examples of the detailed level of information sharing required in protecting the United States. Answering the first question requires coming to grips with what Al Qaeda is and what its intentions are. From his 25 years of experience in studying terrorism, he stated Al Qaeda is detailed highly integrated organization focused on conducting small-scale attacks that disrupt the United States way of life. He emphatically emphasized the threat of terrorism is serious beyond our wildest dreams. He also noted information sharing has to be driven by objectives and existing capabilities, if not "we are merely swapping stories." Information sharing must be directed to what the threat is. In an analogy he stated, "When it comes to information sharing on homeland security the intelligence analyst must be connected to the railroad car conductor to the chemical producers and to the first responders." Establishing an integrated information sharing system to conduct such efforts proves to be the most difficult obstacle for Homeland Security.

I also attended a panel discussion of senior representatives from several national intelligence agencies that discussed the agencies' role in HLS. Mr. Philip Lago, Executive Secretary Central Intelligence Agency, noted the HLS is a new role for the

CIA. The CIA has little expertise on what's inside the borders of the US. The agency is working enhancing relations with the Federal Bureau of Investigation (FBI) by exchanging analysts and liaisons. However, he noted the CIA is not a domestic law agency and a number of laws and regulations prohibit the CIA from becoming fully immersed in HLS. Russ Travers, Deputy Director for Policy Support, Defense Intelligence Agency (DIA), discussed DIA's role in HLS. HLS is not primarily a military task but there are some things the agency can contribute to Homeland Defense. Several examples given he highlighted were the Joint Intel Task Force-CT, the DHS counterintelligence terrorist group, ONI's partnership with the Coast Guard, the Armed Forces Medical Center involvement in CBN education and prevention, Central MASINT, and the inter-department liaisons existing at the Unified Commands. He noted DIA has a long way to go with numerous legal questions to work through. For the time being the best work will continue to be done at the grassroots level. Lastly, he highlighted several outstanding issues for information sharing: technical issues, cultural issues, what information should be shared, legal limits, and policy-making issues; the most difficult being cultural and policy-making issues. He envisioned a move towards a global intelligence world where all-source analytical fusion will take place in a central location.

The final day of the conference had two plenary sessions. The first consisted of a panel discussion among members of the law enforcement community. Jeffrey Baxter, Consultant of the Law Enforcement Working Group, moderated the session. Panelists included Karen Rowan, General Counsel to the Superintendent, Chicago Police Department, Chief Jose Cordero, Newton, MA Police Department, Deputy Chief William Casey, Boston Police Department, and Kathleen Kiernan, Assistant Director, ATF, member of Law Enforcement Working Group. Ms. Rowan talked about the Chicago Police Departments' CLEAR (Citizen and Law Enforcement Analysis and Reporting) Program. She demonstrated how CLEAR helps solve the unsolvable crimes, emphasizes linking information, and guides police where to focus, and shares data from 132 suburban areas.

The second panel discussion brought together various representatives from different sources of the media. Led by moderator Les Schwartz, CIA, the panel addressed the media's role in HLS. Tom Tetter, Government Computer News journalist, discussed the importance of data sharing between all the various agencies involved in HLS. One of the major challenges continues to be developing a technological means for transmitting data to the people who need it. Dana Priest, Washington Post reporter, addressed the difficult relationship existing between the government and the media. She made several comments regarding the recent leaks of classified information from the media. In her view the media tries to balance what information should be shared with the public through personal discernment policies that sometimes become controversial. The controversy exists because the media stands by protecting its sources. Dan Burton, Computer World reporter, provided some controversial insights regarding the media's role in reporting. He stated the lack of professionalism exhibited by a lot of current reporting on the events of 9/11 and the War on Terrorism. He stated the media has an obligation to not only report the news but also ensure they take into consideration their role as citizens in the War on Terrorism. His analogy of the "Mike Wallace story" exemplified the types of inappropriate principles some media members are following. The most important point Mr. Burton made was, "The leaks must stop." This panel

discussion marked some of the controversial views existing in the relationship between the Intelligence Community and the media.

3. Track 4 Panel Discussion Highlights:

"An organization's ability to learn and translate that learning into action is the ultimate competitive advantage." Jack Welch, CEO GE

Training and education for Homeland Security is the absolute critical underpinning of an overall long-range success strategy. This track developed synergy within the education and training organizations of the Intelligence and (recently expanding) national security Communities (Intelligence, Law Enforcement, Federal, State, and Local Governments). Featured presentations included professional intelligence education and training, analytical training, and Operational Security (OPSEC) training with representatives of major institutions and programs. The track highlighted best practices and shared equities to assist in the development of an effective, inclusive, and comprehensive education and training program--essential for Homeland Security. "The advancement of learning depends on community leadership...and the products of that learning, in turn, are essential to the leadership's hopes for continued progress and prosperity..." (To have been delivered at Dallas, Texas, November 22, 1963) John F. Kennedy

Track 4 was chaired Mr. A. Denis Clift, President, Joint Military Intelligence College and coordinated by Mr. Radar O'Reilly, Intelligence Community CIO.

Session #1: The Joint Military Intelligence College and The Joint Intelligence Virtual University (JIVU) Online Distributive Training

Chairmen: Mr. Denis Clift and H. David Banks Jr., Chief, Training Technology & Operations Division Joint Military Intelligence Training Center

Mr. Denis Clift discussed the role of the Joint Military Intelligence College (JMIC). JMIC is the only accredited school offering graduate and undergraduate degrees in intelligence. JMIC provides a vanguard of research on classified and unclassified material on intelligence issues. Charted by the DoD in 1962, the mission of JMIC focuses on the education of civilian and military intelligence professionals. Mr. Clift highlighted some of the issues students are tackling at JMIC: the establishment of NORTHCOM, intelligence and law enforcement, the intelligence cycle, intelligence and policy-making, information superiority, all-source analysis, information sharing, and predictive intelligence (ex. Terrorism). He emphasized the need to incorporate intelligence resources such as INTELINK, JWICS, JDISS, and NIST Teams. One valuable aspect HLS training and education can incorporate to enhance learning is the Case Study method.

The presentation also provided an overview of the capabilities of the Intelligence Community's online distributive training capability - the Joint Intelligence Virtual University (JIVU), an interactive, web-centric learning environment. It connects students and instructors to expand learning access, reduce costs, and increase collaborative information flow. It is "anytime, anywhere" training, providing the full spectrum of support materials for community training. Starting out as a DIA initiative to support the DoD intelligence training community, JIVU has evolved into the sole online distributive training capability for the entire U.S. Intelligence Community. In just over 18 months,

JIVU has over 4000 registered users, and offers over 200 intelligence courses with several courses being developed. The presentation concluded with a screen-capture demonstration of the various JIVU capabilities. One shortfall to JIVU is the fact access is restricted to those with DoD security clearances. The JIVU has not developed a strategy to connect, coordinate, and tap into law enforcement agency resources. One recommendation would be for JIVU to develop ways to get around classification requirements to expand its reach to all agencies contributing to intelligence support to HLS.

Session #2: Training & Information Considerations for Homeland Security

Chairman: Ed Jopeck, Director of Security Analysis & Risk Management, Veridian

The increased focus on homeland security has rapidly brought into focus two major shortcomings . First, the shortage of skilled antiterrorism analysts to assess security needs of critical infrastructures and potential terrorist targets in the U.S. Second, the difficulty that most agencies are having in obtaining and assessing threat information for their areas of responsibility. A successful response to terrorism in the U.S. will require significant improvements in both areas. This presentation provided a corporate civilian's observations and experiences based on nearly a decade of performing antiterrorism and risk assessments, both in the classified and unclassified environment. Mr. Jopeck explored the challenge law enforcement agencies and non-national security related agencies face in trying to perform their new homeland security roles. His presentation provided actions training professionals can implement to better prepare their students to assume the responsibilities of providing the type of intelligence and security analysis absolutely required to truly effect homeland security in the future. Mr. Jopeck's Risk Management model provided one way for the Department of HLS (DHS) to standardize risk assessment of US critical infrastructure. The presentation failed to address how the DHS can go about conducting an initial assessment of the vast amount of work involved in mapping out all of the United States' infrastructure (transportation, telecommunications, electric, government operations, finance, water, oil and gas, and emergency services). How can the DHS coordinate infrastructure mapping of the United States similar to the way the Joint Warfare Analysis Center (JWAC) maps foreign infrastructure?

Session #3: Operational Security (OPSEC): An Out of Body Experience

Thomas P. Mauriello, Director of Interagency OPSEC Support Staff

Mr. Mauriello presented a dynamic and informative briefing on the principles of Operational Security (commonly referred to as OPSEC). His briefing included an overview of the five-step analytical OPSEC process. He explained how OPSEC can and should be integrated into all operations to provide effective protection of critical and proprietary information. OPSEC is being implemented throughout the national and homeland security communities as a planning methodology vital to the success of securing homeland assets. He also discussed the mission of the Interagency OPSEC Support Staff (IOSS) that acts as a consultant to all U.S. government departments and agencies, and contractors sponsored by the U.S. government that have a national security mission. OPSEC is more than a program--it is a state of mind. It focuses on the

protection of critical, but unclassified information that becomes advantageous in the hands of the adversary.

Session #4: Lessons in Homeland Security: Learning by the Case Method

Chairman: Thomas Shreeve, Thomas W. Shreeve & Associates

Mr. Shreeve described how a powerful and effective learning methodology known as the "case method"" can be applied to homeland security. The case method is the predominant form of teaching at leading U.S. graduate schools of business and public administration. The speaker, Thomas W. Shreeve, is the director of the US Intelligence Community Case Method Program and is widely regarded as the nation's leading practitioner of case-based teaching in intelligence, national security, and federal law enforcement. Mr. Shreeve retired from the Central Intelligence Agency in 1998 following a career that included service in the Marine Corps, the New York City Police Department, and the Drug Enforcement Administration.

Mr. Shreeve's brief outlined the methodology required for implementing this valuable educational tool. He defined the case-based discipline; goals associated with the method, and provided examples to use. Most importantly, he addressed the dos and don'ts for instructors and the lessons learned he is experienced using this method.

Session #5A: Role of the Central Intelligence Mission Academy and the CIA University

Chairman: Dr. Elaine Riddle, Director CIA Mission Academy (CIA University)

Dr. Riddle discussed the mission and organizational structure of the CIA University. She noted the CIA is making an effort to contribute to the new and increasing demands of Homeland Security. I obtained copies of her presentation if anyone is interested.

Session #5B: National Geospatial Intelligence School: HS Initiatives

Chairman: MAJ Wesley Baker, Chief Homeland Security Training, USAF

Major Baker presented NIMA's reorganization initiative of its training and doctrine arm to better support national priorities (including) homeland security; a brief overview of the NIMA's new Homeland Security Training program with course offerings; a report on a recent series of Geographic Information System conferences that have direct implication for Homeland Security information needs; and a proposal for a new geospatial training consortium partnering his organization with other DoD, government, and civilian agencies. His brief highlighted some of the grassroots effort being done by NIMA to share information between national intelligence agencies and state, local, and tribal sector agencies and overcome cultural barriers currently existing amongst the various agencies.

Session #6: Training, Services, and Operational Support Provided by the ATF

Chairman: Mark Logan, Assistant Director Training & Professional Development, Bureau of Alcohol, Tobacco and Firearms

Participants in this session received information about training, services, and operational support available from the Bureau of Alcohol, Tobacco and Firearms, a Bureau of the U.S. Department of Treasury that enforces the Federal laws and regulations

involving alcohol, tobacco, firearms, arson, and explosives. Federal, state, and local agencies can tap these ATF resources to develop effective and comprehensive homeland security and critical incident training and response programs. Training programs discussed included domestic and international firearms trafficking programs (including President Bush's Project Safe Neighborhoods); explosives post-blast investigation and disposal; explosive and accelerant detecting canines; crisis management response; alcohol and tobacco diversion crimes, the proceeds of which fund terrorist and criminal enterprises; arson investigation and prosecution; and criminal investigative analysis (arson and explosives profiling). ATF operational support and services available to Federal, State, and local entities include the National Tracing Center, explosive and accelerant detecting canines, the National Explosives Repository; National Response Teams, and forensic laboratory services.

Session #7: Nevada Test Site (NTS) Weapons of Mass Destruction (WMD) and Counter Proliferation Training

Chairman: Charles E. Sheville, Senior Project Specialist, National Center for Combating Terrorism

The presentation provided an overview of the training and exercise support capabilities of the Nevada Test Site. The NTS is a member of the National Domestic Preparedness Consortium formed in 1998 by the Department of Justice, Office for Domestic Preparedness (OPD). The NTS is the National Center for Exercise Excellence and conducts training for the enhancement of the capabilities of the state and local jurisdictions to prepare to respond to incidents of terrorism involving weapons of mass destruction. The NTS provides training and exercise support to the National Guard WMD Civil Support Teams, as well as active duty and reserve military organizations. The NTS is establishing the National Center for Combating Terrorism to maintain training and exercises in support of the current and future needs for the war on terrorism.

4. Conclusions:

This conference provided a valuable forum for highlighting and addressing the current issues facing agencies involved in Homeland Security such as what type of information sharing needs to take place, what are the best practices and methods currently out there, and what are the roles for not only the Intelligence Community but also such agencies as federal, state, and local law enforcement, private industry, the media, and the average American citizen. Homeland Security presents a unique challenge to the United States that requires the involvement of a plethora of entities. Even though the Office of Homeland Security is being tasked to head the charge, it will truly take the involvement of multiple resources developing innovative techniques to truly defense our homeland. The conference also taught me about the culture and role of local law enforcement agencies in Homeland Security. The representatives from those agencies were very impressive in outlining their needs and desire to become integrated with the Intelligence Community. They seem to be more innovative in how to integrate the two sides whereas the Intelligence Community seemed to be somewhat leery and desiring the law enforcement agencies to meet IC standards vice some middle road. In order for Homeland Security to succeed vast improvements, need to be addressed regarding the relationship between the two realms.

5. Thesis Research Inputs:

Most importantly, this conference provided a plethora of data to incorporate into my thesis. Some of the highlights include:

- Establishing points of contact for follow on research at key intelligence and law enforcement agencies
- Learning about the case study method
- Gaining knowledge on valuable resources such as JMIC, JIVU
- Issues to incorporate into NS3156 syllabus such as coordination between the Intelligence Community and law enforcement agencies, USCG integration, the case study method (which cases to use), integrated domestic communications, and HLS documents
- NS3156 syllabus should build upon what's already been done, not start from scratch
- Possible thesis recommendation: discuss with JIVU about adding NS3156 to course catalog to reach more consumers
- Possible thesis recommendation: NS3156 should establish a joint collaborative environment to maximize student learning. Instructors will have to learn to develop a teaching method consistent with the on-line realm. No longer can instructors rely on standing in front of the classroom and teaching students. NS3156 needs to incorporate a multi-sensory, student-centric approach. Utilizing NPS Blackboard.com develops a student's analytic production process and skill set.
- NS3156 syllabus should not only educate students on intelligence support to HLS but also teach students to become HLS analysts.
- Thesis should be careful using Homeland DEFENSE and SECURITY interchangeably.
- I talked to CAPT Tom Ward (Navy 1630), Joint Forces Headquarters-HLS. He works on the JTF for HLS within Joint Forces Command as the J2. He noted NORTHCOM is still sorting through moving around resources, manpower, etc. primarily because Secretary Rumsfeld put a cap on funding. NORTHCOM will be stood up from existing forces in the DoD. The new command will not have a traditional Joint Intelligence Center (JIC). Rather, a Intelligence Fusion Center (IFC) will be stood up as an intelligence consumer vice producer of raw intelligence. CAPT Ward added the military intelligence side is not difficult to implement change for HLS. Practices pretty much in place already. The difficulty exists in working with law enforcement agencies such as the FBI who bring a very different intelligence perspective and culture. CAPT Ward promised to make NORTHCOM briefs available later for consumption.

- After hearing Tom Shreeve's brief on the Case Study Method strongly believe NS3156 should incorporate this teaching approach to enhance student learning. The presentation provided a thorough education on the method and further discussion should follow. Mr. Shreeve provided point of contact information and welcomes follow-on consultation.
- Interagency Process module should look to incorporate the relationship between the FBI and CIA, role of federal, state, and local law enforcement agencies. NS3156 could invite members from the local law enforcement community in Monterey to speak to NS3156 students. Possible panel discussion might include Ambassador Minott, Monterey chief of police, and someone with an FBI background to address the HLS interagency process.
- If NS3156 looks to cater to DOJ officials then the course material might want to remain on the unclassified level or at least look to ways to ensure all participants have access to course material.
- Another valuable resource to exemplify the HLS interagency process is looking at the work of the Los Angeles Terrorist Early Warning working Group (TEW). I have established a point of contact with Col Wilson (USMC ret.) to conduct follow on research. Another valuable resource is the Law Enforcement Working Group headed by Kathleen Kiernan, Assistant Director, ATF, Office of Public and Governmental Affairs.
- Module 8 objectives should include the point the US is a unique country based on initiative and thinking out of the box. Students should become familiar with some of the grassroots work being done on information sharing and Homeland Security such as the TEW, Chicago Police Department's CLEAR program, and NIMA's Geographic Information System and GeoBase Concept.
- A few items to take away from attending three days of discussion from various experts: 1) people are looking for a repository for HLS, 2) agencies like DIA, CIA, etc. deal in the classified realm and want law enforcement agencies to get on board with way "they" do business (Representative from Customs Department stated that takes too long for them), 3) where is the Office of HLS because everyone continues guessing what the intelligence needs are without set guidelines to follow, and 4) the Intelligence Community has a lot of refining to do to overcome cultural barriers between the various intelligence agencies on the federal, state, and local levels in order to develop an efficient intelligence system for Homeland Security.

6. <u>Miscellaneous Notes:</u>

- Conference Chair, Executive Director GETA: FREDRICK THOMAS MARTIN began his career with the U.S. Intelligence Community in 1960 on the front lines as a linguist and intelligence analyst in the Middle East. He retired from the National Security Agency as a computer scientist and

Deputy Director of their Information Services Group in 1998. He then founded Martin Consulting Associates, Inc. to provide consulting and business development services on advanced information technology applications to meet the requirements of the Intelligence Community, other government agencies, and companies within the private sector. Mr. Martin was an Adjunct Professor for twenty-five years at The American University in Washington, D.C., developing and teaching courses in mathematics, statistics, and computer science. He is the author of the first commercially published book on current intelligence operations within the US Intelligence Community entitled, "TOP SECRET Intranet: How US Intelligence Built INTELINK, the Largest, Most Secure Network." Mr. Martin holds a masters degree in computer systems/operations research from the American University. His undergraduate degree is in mathematics.

- List of government experts represented: CIA, NSA, NRO, DIA, ATF, DISA, DARPA, US Navy, Office of Homeland Security, IC CIO, IMO, Law Enforcement Working Group, the Departments of Justice, Interior and Energy.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX F. AFTER ACTION REPORT FROM INTERVIEW WITH MGEN BRUCE LAWLOR, SENIOR DIRECTOR FOR PROTECTION AND PREVENTION, OFFICE OF HOMELAND SECURITY

Note: The following is a copy of the After Action Report written on the MGEN Bruce Lawlor's presentation entitled, "The Future of Homeland Security." The presentation was given to Naval Postgraduate School faculty and students on 05 November 2002, at the Naval Postgraduate School, Monterey, California.

Subject: MGEN LAWLOR BRIEF-- "THE FUTURE OF HOMELAND SECURITY"

1. On November 5, 2002, MGEN Bruce Lawlor, Senior Director for Protection and Prevention, Office of Homeland Security gave a brief to NPS faculty and students entitled "The Future of Homeland Security." He provided a first hand account of the Office of Homeland Security's overall strategy. His presentation also provided suggestions for the NPS audience of possible areas of study for future research. MGEN Lawlor outlined the operational directives of the Office of Homeland Security using an Army analogy of the deep battle, the close battle, and the rear battle.
2. THE DEEP BATTLE: The deep battle is overseas, interdiction of the threat before getting on US soil. One example is surveillance of nuclear weapons smuggling abroad. Another example is US Customs officials working with officials from other large foreign ports like Rotterdam, Tokyo, and Singapore to conduct shipping containers overseas. An enormous concern for the Office of HLS is shipping containers. The problem is how to detect nuclear material. Enhanced technology is required for active and passive detection of nuclear material. Another example is extending surveillance through biometrics. Enhanced technology such as rapid fingerprinting is required to track entry and exits into and out of the country.
3. THE CLOSE BATTLE: The close battle is protecting our borders. The required efficiency of the American system causes a bleeding out of security measures. Tracking land transportation along and within US borders remains a concern. Improved detection technology is required along US borders.
4. THE REAR BATTLE: The rear battle is made up of several components: 1) critical infrastructure, 2) monitoring transportation systems, 3) disrupting the threat, 4) preparing the response, and 5) communicating with the public. HLS requires identification of *critical* infrastructure that supports society. The need exists to look at systems not facilities. One example is chlorine transportation safety through the rail system to ensure the water system remains in tact. Systems should then break down into nodal analysis. Detailed analysis is required to determine which critical infrastructure systems are actually critical. A good measuring stick is whether penetration of the system leads to the death of

American lives. Protection of all critical infrastructures is difficult given the open nature of American society. Therefore, HLS officials need to think of different ways to protect critical infrastructures of the United States. HLS also requires new and innovative ways to protect the US transportation system. The federal government cannot afford to pay for all of it. The idea of dual use is required to integrate security improvements with the demands of the private sector. An example is shipping container safety. Disrupting the threat entails increased involvement by the FBI, better tracking of foreign students in country, and developing an integrated intelligence system. A misperception exists in the United States that a "green door" exists in Washington DC where all the secrets to disrupting the threat lay in the wings. The reality is DC does not have the information to share. The true front line of HLS intelligence and information collection lies with the cities themselves. Police provide security mechanism to detect terrorist activity in the cities. "Intel is in the communities." An enormous piece to the Department of Homeland Security is the creation of a state, local, and federal information-sharing network. Another component of the rear battle is prepared response, addressing the issues of first responders. One example is the dissemination of vaccinations. The most important component of the rear battle is communicating with the public. How do we take away the strategic threat of fear that is fundamental to terrorists? HLS requires the DHS to conduct a PR campaign. The DHS OUTREACH PROGRAM is providing information addressing steps people can take in their daily lives to instill the notion "the current situation is not hopeless."

5. Questions and Answers:

A question and answer session followed MGEN Lawlor's presentation. The following is a list of some of the highlights:

- DHS is learning from other HLS models in place in Israel, Britain, and France
- The issue of protection vs. not instilling fear; DHS trying to tell folks to make individual judgments regarding what precautionary measures to take in order to feel safe. After all, that is the American way. Alerts help but intelligence very rarely gets exact details such as a time, place, and location.
- HLD vs. HLS; HLD is used to distinguish between DoD operational functions (combat operations) from other supporting roles like intelligence gathering, and medical support which makeup HLS. NORTHCOM is trying to reach out and establish communications with states in order to integrate military and civilian support. However, currently the support structure is still in flux.
- The main contribution the military can make to DHS is helping to provide a security mindset that deals with doctrine, tactics, procedures, and skills needed for HLS. The military thinks in security terms to guide planning (Ex: Deep, close, and rear battle). DHS has yet to develop an organizational security structure. "Civilian sector just not used to thinking in this paradigm." This is where the military can make the greatest contribution to HLS.

3. HLS Intel Discussion:

MGEN Lawlor also met with several NPS representatives to discuss the role of intelligence in DHS. The following are some of the highlights from the meeting:

- DHS needs to create an OPINTEL center where all-source fusion takes place.
- DHS will have an Intelligence Directorate to coordinate intelligence efforts within DHS.
- DHS is a customer of intelligence. The Intelligence Directorate will generate intelligence requirements like the other agencies in the intelligence community but it will not have tasking authority. The Administration feels tasking authority is not essential right now.
- Analytical capability is needed and it doesn't currently exist in DHS
- From his perspective, no current organization within the US is good at domestic intelligence. The FBI maintains a collective and investigative culture for developing material for prosecution purposes. New DHS wants to create and analytical center or "domestic CIA" similar to Britain's MI-5. As a consumer DHS can conduct their own analysis and therefore requires a cadre of analysts. However, the primary function of HLS is not to do intelligence. This creates a problem for anyone involved in intelligence analysis within DHS because "if you're good CIA will hire you." As a result, intelligence analysts in DHS become collateral, leading to a second-class analyst.
- Policy-makers within the DoD have many misperceptions about the DoD's ability to conduct domestic intelligence collection. "Posse comitatus has nothing to do with intelligence." The barriers to domestic intelligence collection are policy barriers not legal ones. When you go through the actual DoD regulations and guidelines there are no legal barriers to domestic intelligence collection. DoD answers to domestic intelligence collection are based on misperceptions vice actual regulations.
- Civilian authorities need to understand how the intelligence process works. We have to overcome the "green door" misperceptions of intelligence in Washington DC listed above. State and local officials need to understand no "green door" in Washington exists.
- Domestic CONUS intelligence centers do not exist. "Intelligence lies in St. Louis and the cities, not DC." The intelligence system must harness efforts throughout the country to develop an all-source fusion picture.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX G. AFTER ACTION REPORT FROM 26 SEPTEMBER 2002 TEW GROUP CONFERENCE

To: Distribution

Subject: TERRORIST EARLY WARNING WORKING GROUP CONFERENCE, LOS ANGELES, CA 26 SEP 02

Attachments:

1) Los Angeles Terrorism Early Warning (TEW) Group September meeting agenda
2) TEW September 2002 OSINTrep
3) TEW Phonebook (September 26, 2002)
4) LtCol Kempfer Consequence Management Intelligence briefing handout
5) Article by TEW members: "Homeland Security: Beyond Terrorism; Fourth Generation Warfare"

1. **Conference Summary:** LtCol Harold Kempfer (USMCR) invited me to attend the Terrorist Early Warning (TEW) working group conference in Los Angeles on September 26, 2002, to obtain inputs for my thesis (Developing NS3156 Intelligence Support to Homeland Security). The TEW provides a model and test case for understanding the intricacies of the interagency process occurring between organizations involved with Homeland Security concerns. The one-day conference was held at the Los Angeles County Emergency Operations Center in Los Angeles, CA. The Gilmore Commission sited the group as a model for interagency information sharing between several national entities (including executive and legislative actors). The monthly meeting allows members to interact and openly discuss and debate issues impacting regional TEW.

   Conference agenda included LtCol Kempfer's presentation on Consequence Management Intelligence and a roundtable discussion on recent OSINT trends and potentials, and threat issues. Participation included TEW permanent cadre, as well as representatives from local, state and federal public safety and health agencies (including National Guard and local military actors), several research institutions (e.g., RAND), and utilities (water and power). The briefing focused on intelligence indications and warnings. The roundtable session focused on building situational awareness for I&W and operational net assessment missions. A sampling of participating agencies included LASD, LAPD, FBI, NCIS, USMC I MEF, CNG/9th CST, OES, LAFD, LACOFD, LACODHS, INS, US Customs, USCG, USAF OSI, RAND, US Attorney, LA District Attorney, Australian Federal Police, and TEW representatives from Orange and San Bernardino Counties. Several national labs, and many other local and state agencies were also represented.

2. **Presentations:**

Copy of brief is available for further discussion. The following are highlights from LtCol Kempfer's presentation on Consequence Management Intelligence:

- Consequence Management is a critical part of the HLS intelligence tradecraft
- Most agencies do not have a designated intelligence officer (i.e. Does the Fire Dept have an intelligence officer? Probably not) therefore, how can agencies conduct consequence management intelligence?
- He talked about his role as J2 of Consequence Management JTF in Kuwait April-August 2002.
- Brief sought to teach people in TEW cadre of one of the skill sets needed for HLS intelligence tradecraft
- Consequence Management places a greater demand on intelligence: medical, CBW, logistics, etc.
- TEW cadre brings a lot of groups together to fuse knowledge piece together
- Emphasized the importance of incorporating first responders (ex: nuke suitcase bomb scenario)
- No one knows the national strategy for HLS…what are the benchmarks for agencies to follow? Who determines when resources are turned on/off?
- When in comes to HLS how do you get a common operational picture?
- LA Emergency Operations Center relies on the media for real-time intelligence. For example, news stations helicopters are like having UAVs on the battlefield.

3. **Roundtable Discussion Highlights:** Moderated by Deputy Mark Seibel, LA County Sheriff Department, the roundtable discussion focused on recent OSINT trends and potentials, and threat issues. Some of the highlights included:

- Representative from California Congressman's office was on hand to provide inputs from the state level
- Inputs provided from a wide range of agencies ranging from US Air Marshals to LAPD/LAFD to military reps from USAF OSI and National Guard.
- Participants went around the room and openly shared information from their respective agencies. For example, one rep from OSI shared recent indications and warnings about surveillance being done at local military installations.
- Role of citizen reporting brought up by several members as contributing to successful investigation and apprehensions of possible terrorists.
- Overwhelming amount of information sharing done on various HLS issues being dealt with in the region. For example, participants discussed modeling, systems incorporation, case studies, terrorist suspect databases, and even recent reporting on indications and warnings of terrorist activity.

4. **Conclusions:** This conference provided a great opportunity to conduct personal interviews with various representatives from the Intelligence Community as well as law enforcement. I was able to gain firsthand knowledge of the TEW concept and how it is becoming a model for interagency facilitation and cooperation regarding HLS. The fact I was personally invited by one of the guest speakers welcomed TEW cadre to share information with me that might not be obtained through secondary sources. The conference provided an education on how different agencies and levels of government are interacting on information sharing and mutual cooperation regarding threats to Homeland Security.

5. **Thesis Research Inputs:**

- TEW provides a model for how the HLS interagency process is working at the grassroots level. TEW efforts have been acknowledge federally by the Bush Administration's Foreign Intelligence Advisory Board, the Markle Center, and the Office of HLS. Discussion of the TEW working group's efforts should be incorporated into NS3156 module on the interagency process. Other cities and regions around the country like Las Vegas, Orange County, CA, and San Bernadino County, CA are incorporating TEW concept. With interest coming from the national-level the TEW is sure to be a model for HLS agencies to follow in the future. I have been added to the TEW phonebook directory in order to track future efforts by the TEW working group.
- Agencies involved in HLS are looking for national and federally mandated guidance from Washington D.C.
- TEW working group provides a successful example of organizations coming together to conduct all-source fusion analysis for intelligence and law enforcement purposes.
- TEW focuses on establishing an all-source fusion operations center for HLS
- TEW has experienced bureaucratic problems in working with agencies inside the Beltway. Consensus seems to be "Beltway talks about HLS but does not have an idea of what's going on at the grassroots level to succeed in HLS within the United States."
- Army National Guard representative I talked to provided insight and perspective regarding the demands being placed upon reservists participating in HLS efforts.
- TEW started by in 1996 to focus LA County efforts on terrorism and is now becoming a model for HLS interagency information sharing and intelligence dissemination.
- TEW is like bringing together a MAGTF or BATGRU to conduct; multiple assets being synchronized for a common strategic mission.
- I learned about how different agencies are getting around classification obstacles commonly hindering interagency information sharing. TEW focuses on declassifying information so all participants can tap into resources.

- I was able to establish several points of contact and given access to TEW resources for follow-on research.
- One question to tackle is how can the TEW model be incorporated at the state and federal levels. TEW is working at the regional level in Los Angeles County but with growing interests coming from the Office of HLS how can TEW concept be incorporated by larger bureaucratic organizations like the Office of HLS?
- From my interviews I learned about some of the current holes in the interagency process such as integration of Coast Guard assets, the lack of a centralized opintel center for HLS, the lack of a network-centric communication tool for intelligence and law enforcement agencies to share information, and the need for standardization from the Office of Homeland Security to guide information sharing efforts, unity of effort, and command and control responsibilities. These problem areas are good topics for NS3156 student briefs and policy papers.
- Recommend Dudley Knox Library folks and NS3156 contact Sgt John Sullivan to be added to TEW phonebook for further information sharing.

6. **Miscellaneous Notes:**

- POCs:
  LtCol Harold Kempfer, USMCR, J2 C/JTF-CM, (562)-984-2050)
  Sgt John Sullivan, TEW/Emergency Operations Bureau, 323-980-2292
  Deputy Mark Seibel, TEW Admin, 562-984-2050
  Capt Phillip Carter, Anti-Terrorism/FP Officer 40th Inf Div (Mech), (310)-428-8842
- TEW also publishes a monthly OSINTrep document for dissemination to TEW members. I obtained a copy if anyone is interested in reviewing.
- Also obtained a copy of LtCol Kempfer's brief if anyone is interested.

LIST OF REFERENCES

"America Still Unprepared—America Still in Danger." *Report of an Independent Task Force Sponsored by the Council on Foreign Relations.* By Gary Hart and Warren B. Rudman, Co-Chairs. New York: Council on Foreign Relations Publications Office, 2002.

ANSER Institute for Homeland Security: [http://www.homelandsecurity.org].

Army Center for Health Promotion and Preventive Medicine: [http://chppm-www.apgea.army.mil/HomelandSecurity].

Army Soldier and Biological Chemical Command: [http://hld.sbccom.army.mil/].

Bamford, James. "How to (De-) Centralize Intelligence." *New York Times*. 24 November 2002.

Basham, Don, US Department of Justice Official. Interview by Author, 13 August 2002. Interview Via E-Mail Correspondence.

Benesh, Peter. "Does U.S. Need New Agency To Spy On Its Own Citizens?" *Investor's Business Daily* (10 January 2003): A14.

Best, Richard A., Jr. *Homeland Security: Intelligence Support*. Washington, D.C.: Congressional Research Service Report for Congress, 18 November 2002. Library of Congress Congressional Research Service, Order Code RS21283.

Betts, Richard K. "Fixing Intelligence." *Foreign Affairs* 81, No. 1 (1 Jan 2002): 43-52.

Brown, John Seely, and Estee Solomon Gray. "The People Are the Company." *Fast Company Magazine*, No. 1, November 1995. Retrieved from Fast Company Website on 12 March 2003 at: [http://www.fastcompany.com/online/01/people.html].

"Bush to sign Homeland Dept. Bill." *New York Times*. 25 November 2002. Retrieved from NY Times Website on 25 November 2002 at: [http://www.nytimes.com/aponline/politics/AP-Bush-Homeland-Security.html?ex=1039242654&ei=1&en=9bbc98504ec515d7].

Carafano, James Jay. *Prospects for the Homeland Security Department: the 1947 Analogy*. Washington, D.C.: Center for Strategic and Budgetary Assessments, 12 September 2002. Retrieved from CSBA Website on 23 September 2002 at: [www.csbaonline.org].

Casella, Alexander. "Intelligent reform of US intelligence." *Asia Times*. 15 January 2003. Retrieved from *Asia Times* Website on 6 February 2003 at: [http://www.atimes.com/atimes/Front_Page/EA15Aa01.html].

Chambliss, Saxby. "Mind The Gap: We Were Caught Flat-Footed on September 11." *Washington Times*. 29 July 2002.

Channell, Ralph Norman. "Intelligence and the Department of Homeland Security." *Strategic Insights*. Monterey: Center for Contemporary Conflict, 09 August 2002. Database On-Line. Retrieved from Center for Contemporary Conflict Homepage on 10 August 2002 at: [http://www.ccc.nps.navy.mil/rsepResources/si/aug02/homeland2.asp].

Clausewitz, Carl Von. *On War*, Indexed Edition. Edited and Translated by Michael Howard and Peter Paret. New Jersey: Princeton University Press, 1984.

Coast Guard HLS: [http://www.uscg.mil/overview/Homeland%20Security2.htm].

Costarino, Thomas, SAIC consultant. Interview by Author, 13 August 2002. Interview Via E-Mail Correspondence.

"Degree of Danger: Now There's a Graduate Program in Homeland Security." *Newsweek*. 03 February Issue. Retrieved from MSNBC News Website on 31 January 2003 at: [http://www.msnbc.com/new.863870.asp].

Eggen, Dan and John Mintz. "Homeland Security Won't Have Diet of Raw Intelligence." *Washington Post*. 05 December 2002. Retrieved from Washington Post Website on 05 December 2002 at: [http://www.washingtonpost.com/wp-dyn/articles/A15908-2002Dec5.html].

"Fact Sheet: Strengthening Intelligence to Better Protect America." *Official White House News Release* (28 January 2003). Retrieved on 07 February 2003 from White House Official Website at: [http://www.whitehouse.gov/news/releases/2003/01/print/20030128-12.html].

Federal Bureau of Investigation: [http://www.fbi.gov/terrorinfo/terrorism.htm].

Franklin, Daniel. "Spooks vs. Suits: Why the FBI and CIA Don't Cooperate, and Why They Shouldn't." Slate Website, 14 October 2002. News Service On-Line. Available from Slate Website, msn.com, [http://slate.msn.com/?id=2072266].

"The Future of Homeland Security." Speech Given by MGEN Bruce Lawlor, Senior Director for Protection and Prevention, Office of Homeland Security. Naval Postgraduate School, Monterey, California, 05 November 2002.

Gertz, Bill. *Breakdown—How America's Intelligence Failures Led to September 11*. Washington, D.C.: Regnery Publishing, Inc., An Eagle Publishing Company, 2002.

Gorman Siobhan. "Cooperation Among Border Security Agencies Top Challenge for Department." *National Journal* August 10 Edition (09 August 2002).

Harris, Shane. "Homeland Security Cedes Intelligence Role." *Government Executive Magazine*, 26 February 2003. Retrieved from Government Executive Website on 28 February 2003 at: [http://govexec.com/dailyfed/0203/022603h1.htm].

_____. "Ridge Says Intelligence Czar Probably Unnecessary." *Government Executive Magazine*, 11 December 2002. Retrieved from Government Executive Website on 13 December 2002 at: [http://www.GovExec.com/dailyfed/1202/121102h1.htm].

"Homeland Security Agency a Reality." *MSNBC News.* 25 November 2002. News Service On-Line. Available from MSNBC News, [http://stacks.msnbc.com/news/833668.asp].

"Homeland Security: An Intelligence Oversight Perspective." *Military Intelligence Professional Bulletin* 28, No. 3 (July-September 2002): 5-8.

Howe, Kevin. "NPS Master's Program First in the U.S." *Monterey County (CA) Herald*. 06 January 2003.

"Intelligence and Law Enforcement Coordination: Overlapping Mission Dictates Need for Improved Liaison." *Military Intelligence Professional Bulletin* 28, No. 3 (July-September 2002): 22-23.

Isaacson, Jeffrey A. and Kevin M. O'Connell. "Beyond Sharing Intelligence, We Must Generate Knowledge." *Rand Review* 26, No. 2 (Summer 2002): 48-50. Retrieved from Rand Website on 29 January 2003 at: [http://www.rand.org/publications/randreview/issues/rr.08.02/intelligence.html].

Joint Publication 2-0: Doctrine for Intelligence Support to Operations. Washington, D.C: Joint Chiefs of Staff, 09 March 2000. Publications On-Line. Available from Joint Electronic Library, DTIC, [http://www.dtic.mil/doctrine/jpintelligenceseriespub.htm].

Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms. Washington, D.C.: Joint Chiefs of Staff, 12 April 2001 (as amended through 09 January 2003). Publications On-Line. Available from Joint Electronic Library, DTIC, [http://www.dtic.mil].

Lawlor, Bruce, MGEN, Senior Director for Protection and Prevention, Office of Homeland Security. Interview by Author, 03 November 2002, Naval Postgraduate School, Monterey, California. Typed Interview Notes.

Luikart, Kenneth A. "Homeland Security: Intelligence Indications and Warning." *Strategic Insights*. Monterey: Center for Contemporary Conflict, 02 December 2002. Database On-Line. Retrieved from Center for Contemporary Conflict homepage on 23 February 2003 at: [http://www.ccc.nps.navy.mil/rsepResources/si/dec02/homeland.asp].

Lowenthal, Mark M. *Intelligence: From Secrets to Policy.* Washington D.C.: Congressional Quarterly Press, 2000.

"Markle Foundation Task Force Says FBI Should Not be Lead Agency For Domestic Information to Prevent Terrorism; Report Calls for National Network of Information Sharing According to Guidelines." *Markle Foundation Task Force Press Release*. 07 October 2002. Retrieved from the Markle Foundation Task Force on National Security in the Information Age website on 18 October 2002 at: [http://www.markletaskforce.org/].

Mazzafro, Joe, Retired Navy Captain, Johns Hopkins Applied Physics Lab. Interview by Author, 02 March 2003. Interview Via E-Mail Correspondence.

Meeks, Brock N. "A Chink in the Infrastructure Armor?" *MSNBC News.* 06 February 2003. News Service On-Line. Available from MSNBC News On-Line, [http: www.msnbc.com/news/868116.asp?0cv=CB10].

National Defense University Library: [http://ndunet.ndu.edu/lib/homedefense.html].

*National Strategy for Homeland Security***.** Released by the Office of the Press Secretary. Washington, D.C.: Office of the President, July 2002. Retrieved from the White House Official Website on 17 July 2002 at: [http://www.whitehouse.gov/homeland/book/index.html].

Naval Doctrine Publication 2: Naval Intelligence. Washington, D.C.: Department of the Navy, 1994.

"New Homeland Security Department Would Identify, Assess Threats." *Armed Forces Press Service*. Armed Forces Information Service, 28 August 2002. Armed Forces Information Service On-Line. Available from US Department of Defense, DefenseLink, [http://www.defenselink.mil/news/Aug2002/n08282002_200208281.html].

New Master's Program: Executive Education for Tomorrow's Homeland Security. Monterey, California: Center for Contemporary Conflict, 28 January 2003. Database On-Line. Available from Center for Contemporary Conflict Website, Resources and Links, Homeland Security, [http://www.ccc.nps.navy.mil/nsa/homeSecurity.asp].

Pincus, Walter, and Mike Allen. "Terrorism Agency Planned: Center to Integrate Intelligence, Analysis." *Washington Post,* 29 January 2003.

"Protecting America's Freedom in the Information Age." *Report of the Markle Foundation Task Force on National Security in the Information Age.* By Zoe Baird and James L. Barksdale, co-chairmen. New York: The Markle Foundation, October 2002.

Reef Points 1997-1998. Annapolis, Maryland: United States Naval Academy Character Development Division, 1997.

Remarks by Governor Tom Ridge, Homeland Security-Designate in a Town Hall Meeting for Future Employees of the Department of Homeland Security, Ronald Reagan Building, Washington, D.C., [17 December 2002]. Retrieved from White House Official Website on 20 December 2002 at: [http://www.whitehouse.gov/news/releases/2002/12].

Report of the Homeland Security Practice Group. By James S. Gilmore, III, Chairman. Kelly Drye and Warren LLP Homeland Security Practice Group, 08 January 2003. *Homeland Security Weekly* 2, No. 4 (27 January 2003). Database On-Line. Available from Homeland Security Weekly, newsletter@twotigersonline.com.

Richelson, Jeffrey T. *The U.S. Intelligence Community*, 4th ed. Colorado: Westview Press, 1999.

Risen, James. "A Top Intelligence Post Goes to C.I.A. Officer In Spy Case." *New York Times*, 14 March 2003.

Rosenbaum, David E. "Spending Deadlock Will Delay Some Programs of New Security Department." *New York Times*. 21 November 2002. Retrieved from *New York Times* Website on 21 November 2002 at: [http://www.nytimes.com/2002/11/21/politics/21HOME.html].

Rothkopf, David J. "Bridging the Intelligence Gap." *Blueprint Magazine*, 29 July 2002.

Russell, James. "NORTHCOM to Coordinate DoD Role in Homeland Defense." *Strategic Insights*. Monterey: Center for Contemporary Conflict, 06 May 2002. Database On-Line. Retrieved from Center for Contemporary Conflict Homepage on 23 June 2002 at: [http://www.ccc.nps.navy.mil/rsepResources/si/may02/homeland.asp].

Russell James, and Iliana Bravo. "Homeland Defense: Ramping Up, But What's the Glide Path?" *Strategic Insights*. Monterey: Center for Contemporary Conflict, March 2002. Database On-Line. Retrieved from Center for Contemporary Conflict Homepage on 31 March 2002 at: [http://www.ccc.nps.navy.mil/rsepResources/si/mar02/homeDefense.asp].

Shenon, Philip. "Lack of Attack Readiness Laid to Financing Delay by U.S." *New York Times*. 13 February 2003. Retrieved from New York Times Website on 13 February 2003 at: [http://www.nytimes.com/2003/02/1/politics/13HOME.html].

_____. "Ridge Discovers Size of Home Security Task." *New York Times*. 02 March 2003. Retrieved from New York Times Website on 04 March 2003 at: [http://www.nytimes.com/2003/03/03/politics/03HOME.html].

Speech Given by Dr. Stephen Gale, Director of the Center for Organizational Dynamics, at the Government Symposium for Information Sharing and Homeland Security, Philadelphia, Pennsylvania, [20 August 2002].

Speech Given by Steven Cooper, Special Assistant to the President, Senior Director for Information Integration and Chief Information Officer, Office of Homeland Security, at the Government Symposium for Information Sharing and Homeland Security, Philadelphia, Pennsylvania, [19 August 2002].

State International Information Program: [http://usinfo.state.gov/topical/pol/terror/homeland.htm].

Steele, Robert David. *The New Craft of Intelligence: Personal, Public, and Political*. With a foreword by Senator Pat Roberts (R-KS). Oakton, Virginia: OSS International Press, 2002.

_____. *On Intelligence: Spies and Secrecy in an Open World.* Oakton, Virginia: OSS International Press, 2001.

_____. Interview by Author, 03 August 2002. Interview Via Email Correspondence.

_____. "Talking Points on Homeland Defense Intelligence." Memorandum Prepared for Brent Scowcroft, 03 December 2001. Email (Electronic Copy) to Author, 03 December 2002. Memorandum also retrieved at www.oss.net.

Stevenson, Richard W. "Signing Homeland Security Bill, Bush Appoints Ridge as Secretary." *New York Times,* 26 November 2002. Retrieved from NY Times Website on 29 November 2002 at: [www.nytimes.com].

Sullivan, John P., Sergeant, Los Angeles Terrorist Early Warning Working Group. Interview by Author, 26 September 2002, Los Angeles, California, Los Angeles Emergency Operations Center. Typed Interview Notes.

_____. "Integrated Threat and Net Assessment: The L.A. Terrorism Early Warning (TEW) Group Model." Los Angeles: Los Angeles TEW, Pre-Attack Panel: Prevention and Deterrence, 2002. Photocopied.

"Testing Intelligence." *The Economist*, 04 October 2001.

Tzu, Sun. *The Art of War*. Translated and Introduction by Samuel B. Griffith. With a Foreword by B. H. Liddell Hart. London: Oxford University Press, 1963.

Ullman, Harlan. *Unfinished Business: Afghanistan, The Middle East, and Beyond—Defusing the Dangers That Threaten America's Security*. With a Foreword by Senator John S. McCain. New York, New York: Citadel Press, Kensington Publishing Corp., 2002.

U.S. Congress. House. Permanent Select Committee on Intelligence. Subcommittee on Terrorism and Homeland Security. *Counterterrorism Intelligence Capabilities and Performance Prior to 9-11*. Report to the Speaker of the House of Representatives and the Minority Leader. July 2002.

US Department of Defense: [http://www.defenselink.mil/specials/homeland/].

US Department of Homeland Security Website. [http://www.dhs.gov/dhspublic.].

US Department of State: [http://usinfo.state.gov/topical/pol/terror/homeland.htm].

US Government Information: [http://www.firstgov.gov/Topics/Usgresponse.shtml].

Ward, Tom, Captain, USN, J2 of Joint Forces Headquarters JTF-HLS. Interview by Author, 20 August 2002, Philadelphia. Typed Interview Notes.

Wenger, Etienne, Richard McDermott, and William M. Snyder. *Cultivating Communities of Practice.* Boston: Harvard Business School Press, 2002.

White House Office of Homeland Security: [http://www.whitehouse.gov/homeland/].

White House Official Website. [http://www.whitehouse.gov].

Zulauf, Barry, Liaison Officer Drug Enforcement Agency Intelligence Division. Interview by Author, 04 December 2002. Interview Via E-Mail Correspondence.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Professor James Wirtz (NSWZ)
   Naval Postgraduate School
   Monterey, California

4. CAPT Robert Simeral
   Naval Postgraduate School
   Monterey, California

5. Professor Robert Looney
   Naval Postgraduate School
   Monterey, California

6. Dr. Barry Zulauf
   Liaison Officer
   Intelligence Division
   Drug Enforcement Administration
   Arlington, Virginia

7. CAPT (ret.) Joe Mazzafro
   Johns Hopkins Applied Physics Lab
   Baltimore, Maryland

8. Sandy Knowland
   Office of Naval Intelligence
   Suitland, Maryland

9. Steve Marrin
   University of Virginia
   Charlottesville, Virginia