2013-12

Employing the intelligence cycle process model within the Homeland Security Enterprise

Stokes, Roger L.

Monterey, California: Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

EMPLOYING THE INTELLIGENCE CYCLE PROCESS MODEL WITHIN THE HOMELAND SECURITY ENTERPRISE

by

Roger L. Stokes

December 2013

Thesis Co-Advisors: Kathleen Kiernan
John Rollins

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE December 2013	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE EMPLOYING THE INTELLIGENCE CYCLE PROCESS MODEL WITHIN THE HOMELAND SECURITY ENTERPRISE	5. FUNDING NUMBERS
6. AUTHOR(S) Roger L. Stokes	
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. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	12b. DISTRIBUTION CODE A

13. ABSTRACT (maximum 200 words)

The purpose of this thesis was to examine the employment and adherence of the intelligence cycle process model within the National Network of Fusion Centers and the greater Homeland Security Enterprise by exploring the customary intelligence cycle process model established by the United States Intelligence Community (USIC). This thesis revealed there are various intelligence cycle process models used by the USIC and taught to the National Network. Given the numerous different training entities and varied intelligence cycle process models, challenges exist with providing a well-defined training program that ensures consistent and clear intelligence cycle process model employment. Finally, this thesis offers an overview pertinent to researchers and/or practitioners regarding the viability of employing the intelligence cycle process model as the principle guide for domestic intelligence activities.

This thesis employed a qualitative research method that analyzed and interpreted publicly available academic and policy information gathered from government and nongovernment institutions regarding the conceptual and practical intelligence cycle process model narratives. A case study analysis was conducted of the April 15, 2013, Boston Marathon bombing as a platform to discuss the active and effective employment of the intelligence cycle process model by the National Network.

The principal conclusion offers while literature clearly agrees the intelligence cycle process model is a cyclical structure of actions, literature also finds there are common themes suggesting the intelligence cycle does not sufficiently describe how the intelligence process works at the operational stages of domestic intelligence activities within the National Network.

14. SUBJECT TERMS Domestic intelligence, intelligence cycle, intelligence, fusion centers, national network, homeland security enterprise, homeland security intelligence enterprise, US Intelligence Community, 28 CFR Part 23, national criminal information sharing plan, information sharing environment.	15. NUMBER OF PAGES 117
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

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

EMPLOYING THE INTELLIGENCE CYCLE PROCESS MODEL WITHIN THE HOMELAND SECURITY ENTERPRISE

Roger L. Stokes
Senior Intelligence Officer, U.S. Department of Homeland Security, Dallas, TX
B.S., Excelsior College, 2002
M.A., University of Oklahoma, 2003

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
December 2013

Author: Roger L. Stokes

Approved by: Kathleen Kiernan, PhD
Thesis Co-Advisor

John Rollins
Thesis Co-Advisor

Mohammad Hafez, PhD
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The purpose of this thesis was to examine the employment and adherence of the intelligence cycle process model within the National Network of Fusion Centers and the greater Homeland Security Enterprise by exploring the customary intelligence cycle process model established by the United States Intelligence Community (USIC). This thesis revealed there are various intelligence cycle process models used by the USIC and taught to the National Network. Given the numerous different training entities and varied intelligence cycle process models, challenges exist with providing a well-defined training program that ensures consistent and clear intelligence cycle process model employment. Finally, this thesis offers an overview pertinent to researchers and/or practitioners regarding the viability of employing the intelligence cycle process model as the principle guide for domestic intelligence activities.

This thesis employed a qualitative research method that analyzed and interpreted publicly available academic and policy information gathered from government and nongovernment institutions regarding the conceptual and practical intelligence cycle process model narratives. A case study analysis was conducted of the April 15, 2013, Boston Marathon bombing as a platform to discuss the active and effective employment of the intelligence cycle process model by the National Network.

The principal conclusion offers while literature clearly agrees the intelligence cycle process model is a cyclical structure of actions, literature also finds there are common themes suggesting the intelligence cycle does not sufficiently describe how the intelligence process works at the operational stages of domestic intelligence activities within the National Network.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACLU	American Civil Liberties Union
BUR	Bottom Up Review
CC	Community Coordinator
CFR	Code of Federal Regulation
CIA	Central Intelligence Agency
CINT	Chief Intelligence Officer
COC	Critical Operational Capability
COINTELPRO	Counterintelligence Program
D	Departmental
DHS	Department of Homeland Security
DNI	Office of the Director of National Intelligence
DoD	Department of Defense
DOJ	Department of Justice
EO	Executive Order
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
HSAC	Homeland Security Advisory Committee
HSE	Homeland Security Enterprise
HSEC SIN	Homeland Security Standing Information Needs
HSIE	Homeland Security Intelligence Enterprise
I&A	Office of Intelligence and Analysis
IACP	International Association of Chiefs' of Police
IALEIA	International Association of Law Enforcement Intelligence Analyst
ILP	Intelligence-Led Policing
IRTPA	Intelligence Reform and Terrorism Prevention Act
ISAC	Information Sharing and Analysis Center
ISE	Information Sharing Environment
JTTF	Joint Terrorism Task Force
MCCA	Major City Chiefs' Association

MCCCIE	Major City Chiefs' Criminal Intelligence Enterprise
NCISP	National Criminal Intelligence Sharing Plan
NSA	National Security Agency
USA PATRIOT	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism
PM	Program Manager
S	Service
SLTPS	State, Local, Tribal, and Private Sector
TCL	Target Capabilities List
USIC	United States Intelligence Community

EXECUTIVE SUMMARY

The United States Intelligence Community (USIC) was not designed to serve as a concept intended to detect significant national security threats originating or residing within our nation's borders, but it was focused on foreign intelligence activities. Little research has been done to study the post-9/11 Homeland Security Enterprise (HSE) counterterrorism efforts supporting domestic intelligence activities and its reliance on the intelligence cycle process model. This thesis evaluates whether the intelligence cycle process model supports the performance of domestic intelligence activities, specifically within the National Network of Fusion Centers (National Network) and the greater HSE.

The unprecedented September 11, 2001, terrorist attacks brought into question the USIC intelligence collection capabilities and served as the catalyst for state, local, tribal and private sector partners into the HSE. The DHS 2011 National Network of Fusion Centers Final Report defined the HSE as federal, state, local, tribal, nongovernmental, and private sector entities. The HSE serves organized complex organizations and their relationships through the National Network. The National Network allows for the integration of the HSE as nontraditional intelligence entities employing intelligence collection and analysis. The National Network and broader HSE have become essential elements providing support to the national intelligence architecture.

Originally, the 1947 USIC structure and the function of its intelligence cycle process model was designed to provide essential information to the president, policymakers, federal organizations, and military communities. The 1947 USIC structure has expanded to its current structure that includes 17 organizations charged with conducting intelligence activities – both foreign and domestic. Today, the growth of the USIC and its purpose has expanded beyond federal elements to include the National Network and the HSE in order to enhance domestic intelligence capabilities.

An assessment of the limited information made available that focuses on domestic intelligence and the intelligence cycle employment reveals information gaps concerning its effectiveness and appropriateness within the post-9/11 HSE. While literature clearly agrees the intelligence cycle process model is a cyclical structure of actions, literature also finds there are common themes suggesting the intelligence cycle does not sufficiently describe how the intelligence process works at the operational stages of domestic intelligence activities within the National Network.

This thesis offers an overview pertinent to researchers and/or practitioners regarding the viability of employing the intelligence cycle process model as the principle guide for domestic intelligence collection activities. Intelligence derived from analyzed information through the intelligence cycle process serves as a principle tool for supporting the nation's counterterrorism efforts and offers law enforcement and homeland security officials with insights and advantages over terrorists. However, there are multiple intelligence cycle concepts within the USIC and the HSE. The various intelligence cycle process models range from a four-step process to a seven-step process.

There are various intelligence cycle process models used by the USIC and now being taught to the National Network by federally funded entities. As an example, the DHS Office of Intelligence and Analysis (I&A), the National Counterterrorism Center, the Memorial Institute for the Prevention of Terrorism (MIPT), the Department of Justice State and Local Anti-terrorism Training Program, and the International Association of Law Enforcement Intelligence Analysts (IALEA) each deliver intelligence training opportunities enthusiastic of the intelligence cycle process model. Given the number of different training entities and varied intelligence cycle process models, challenges exist with providing a well-defined training program that ensures consistent and clear intelligence cycle process model employment within the National Network.

A case study analysis of the April 15, 2013, Boston Marathon bombing illuminates adherence to the intelligence cycle process model as a proactive approach that may have prevented the bombing. This case study was selected in an effort demonstrate the conceptual intelligence cycle process model, in action. Additionally, it

offers the challenges with employing the intelligence cycle process model as an element of the 2003 National Criminal Information Sharing Plan (NCISP) in efforts to prevent terrorism.

The literature provided no USIC or HSE doctrinal information on the adoption of the intelligence cycle as a formal process by USIC or HSE members. Providing comprehensive, consistent intelligence cycle process training to the National Network may serve to decrease privacy concerns while also verifying a concerted federal effort in the fitting execution of domestic intelligence activities. Drawing on publicly available information from government, academia, and national security consortiums, analysis revealed broad acceptance of the intelligence cycle process model philosophy. However, literature provided by academic and operational practitioners support claims that the intelligence cycle process model is flawed and not practical in the operational environment. This thesis may serve as a basis for recommending additional research necessary for studying the intelligence cycle process model implementation and employment within the post-9/11 HSE and its effectiveness in preventing terrorist attacks and enhancing national security intelligence.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Jeremiah 33:3 – “Call unto Me and I will answer you, and tell you great and hidden things that you have not known.” (ESV)

I would like to thank my wonderful wife, Nikkia, and children, Xavier and Isaiah, for their support and sacrifices during the time spent away doing my academic work. May they forever live in the blessings of God.

Finally, I would like to thank my thesis advisors, Dr. Kathleen Kiernan and Mr. John Rollins, as their steady guidance throughout the thesis process was both insightful and encouraging. Thank you for your words of support and direction.

To the senior leadership, Mr. Scott McAllister and Mr. Robin Taylor, of the DHS Office of Intelligence and Analysis, State and Local Program Office for their support in making this endeavor a reality.

Moreover, to the men and women of the United States Intelligence Community, the United States Military, Federal and Domestic Law Enforcement, the Fire Service, Emergency Management and Emergency Medical Services who protect this nation on a daily basis. May God watch over and protect you.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The topic discussed in this thesis is important to the author, and as such, presents a degree of theoretical sensitivities. This thesis runs the risk of slight bias towards the intelligence cycle process model from the federal level and national security intelligence perspective; juxtapose the nontraditional criminal intelligence perspective at the state and local level. The author's own professional experiences as a retired intelligence collector with the U.S. Army Military Intelligence Corps/Defense Intelligence Agency, former Federal Bureau of Investigation Supervisory Intelligence Analyst and current DHS Senior Intelligence Officer have been useful in understanding the policy and practical challenges related to employing the intelligence cycle process model.

However, the intent of this research is to serve as an introduction and description of the issues necessary to explore employing the customary intelligence cycle process model established by the United States Intelligence Community (USIC) within the National Network of Fusion Centers (National Network) and the greater Homeland Security Enterprise (HSE). The information offered delivers an overview pertinent to researchers and/or practitioners regarding the viability of employing the intelligence cycle process model as the principle guide for domestic intelligence collection activities.

On September 11, 2001, the unthinkable happened. International terrorists residing in the US brought into question the USIC intelligence collection capabilities and served as the catalyst for state, local, tribal and private sector partners into the HSE. Immediately following the devastating strike, the nation focused all of its intelligence collection efforts on the prevention of future terrorist attacks from abroad and from within. Nine separate national strategies were written to address elements of homeland security. They include, in part, a National Intelligence Strategy published by the Office of the Director of National Intelligence (DNI) in 2005; a National Strategy for Homeland Security published by the White House in 2007; a National Counterintelligence Strategy published by the DNI in 2009; a National Security Strategy of the United States published by the White House in 2010; a National Counterterrorism Strategy published by the White House in 2011, and most recently a National Strategy for Information

Sharing and Safeguarding published by the White House in 2012. The lack of any national level guidance or strategy related to the collection of domestic intelligence within the HSE other than organizational relationships, classified, or otherwise appears to be a glaring oversight.

The DHS *2011 National Network of Fusion Centers Final Report* defined the HSE as federal, state, local, tribal, nongovernmental, and private sector entities.[1] The HSE serves organized complex organizations, and their relationships with the national intelligence architecture through the National Network. Collecting and analyzing information through the National Network combines state and local criminal intelligence and national intelligence to address transnational threats.[2] The National Network in partnership with the HSE provides an essential information collection and analysis function in efforts to prevent terrorist attacks within the homeland.

Within this complex HSE, there are several USIC intelligence cycle process models being taught. Given today's transnational threat environment, this thesis is intended to inform readers regarding the adaptation and adherence to the intelligence cycle process model within the HSE. The adherence to a consistent intelligence cycle process model within the National Network, as an internal entity of the complex HSE, is critical to producing common operating threat pictures at all levels of government.

The National Network is the integration of nontraditional intelligence entities into the practice of intelligence collection and analysis essential for supporting the national intelligence architecture. In order to examine the National Network's adeptness to adapt to the intelligence cycle process model, it is fitting to review the history of the USIC germane to the intelligence process. The USIC serves as a coalition of agencies and organizations that work both independently and collaboratively with the primary mission

[1] U.S. Department of Homeland Security, *2011 National Network of Fusion Centers Final Report*, May 2012, 2.

[2] 50 U.S. Code Section 402(i)(5) defines transnational threats as any transnational activity (including international terrorism, narcotics trafficking, the proliferation of weapons of mass destruction and the delivery systems for such weapons, and organized crime) that threatens the national security of the United States that includes any individual or group that engages in such activity.

to collect and produce intelligence. The USIC has evolved tremendously in size, structure, and scope since its creation more than 60 years ago following World War II and the 1947 National Security Act. However, the conceptual intelligence cycle process has essentially gone unchanged since its inception. Notwithstanding, the intelligence cycle process phases or steps have increased over the years.

Over the 60 years the USIC has existed, domestic intelligence activities have raised serious concerns regarding privacy, civil rights and civil liberties as a result of abuses of authority and illegal behavior by federal and local law enforcement intelligence entities. Providing federally funded training to the National Network that supports employing the intelligence cycle process model is once again raising concerns among privacy advocates and American citizens. Providing comprehensive, consistent intelligence cycle process training to the National Network may serve to decrease privacy concerns while also verifying a concerted federal effort in the proper execution of the intelligence process. Literature reveals even the best analysis will do nothing to affect national security and crime rates at the state and local level, if it does not influence practices within the National Network.

Chapter II offers a literature review essential for identifying critical premises, as well as contributions necessary for exploring the adherence to the intelligence cycle process model within the National Network. The main goal of the literature review is to understand intelligence cycle process models and to provide context for homeland security and intelligence professionals. Fundamental to this chapter is defining the USIC, the Homeland Security Intelligence Enterprise (HSIE), the HSE, and key intelligence terms. As important is the identification and illumination of the various intelligence cycle process models being used within the HSE.

The 1947 USIC structure has expanded to its current structure that includes 17 organizations charged with conducting intelligence activities both foreign and domestic. The 17-member USIC is composed of a community coordinator, six program managers, five departmental elements, and five services. The Office of the Director of National Intelligence serves as the USIC community coordinator. The six USIC entities that serve as intelligence program managers are the Central Intelligence Agency, the Defense

Intelligence Agency, the National Security Agency, the National Reconnaissance Office, Federal Bureau of Investigation (National Security Branch), and the National Geospatial-Intelligence Agency. The five departmental elements identified as USIC members within specific organizations are the Department of Energy's Office of Intelligence and Counterintelligence, the Drug Enforcement Administration's Office of National Security Intelligence, the Department of Homeland Security's Office of Intelligence and Analysis, the Department of State's Bureau of Intelligence and Research, and the Department of the Treasury's Office of Intelligence and Research. The five services identified as USIC members are US Air Force Intelligence, US Army Intelligence, US Coast Guard Intelligence, US Marine Corps Intelligence, and US Navy Intelligence.[3]

Originally, the 1947 USIC structure and the function of its intelligence cycle process model were designed to provide essential information to the president, policymakers, federal organizations, and military communities. Today, the growth of the USIC and its purpose has expanded beyond federal elements to include state, local, tribal, nongovernmental, and private sector entities necessary to enhance domestic intelligence capabilities.

Chapter III is intended to offer illustrations relevant to the challenges of executing domestic intelligence activities. The central points are identifying the national security focus of domestic intelligence policies, the exploitation of domestic intelligence authorities and cultural differences between the USIC and elements of the HSE that affect the employment of the intelligence cycle process model.

Chapter IV presents a case study of the April 15, 2013, Boston Marathon bombing in the context of the intelligence cycle process model adherence necessary to detect the threat and provide intelligence to policy and decision makers with information in order to prevent the bombing. This case study was selected in an effort demonstrate the conceptual intelligence cycle process model, in action, within the context of the National Network and the broader HSE. Additionally, the case study offers the challenges with employing the intelligence cycle process model within the National Network at the state

[3] "About the Intelligence Community," Intelligence.gov, accessed July 12, 2013, http://www.intelligence.gov/about-the-intelligence-community/.

and local level and supporting the 2003 National Criminal Information Sharing Plan (NCISP) efforts to prevent terrorism.

Chapter V is intended to offer a reading on the intelligence cycle process model and the HSE relevant to intelligence cycle model training and national integration of state and local law enforcement, the private sector, and implementation challenges given the complex HSE.

A. PROBLEM STATEMENT

The USIC was not designed to serve as a concept intended to detect significant national security threats originating or residing within our nation's borders[4] but was focused on foreign intelligence activities. This thesis evaluates if the intelligence cycle process model supports the performance of domestic intelligence activities within the National Network that serve as focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information between the federal government and state, local, tribal, territorial and private sector partners.[5] Research provided little has been done to study the weaving together of local, state, and federal counterterrorism efforts[6] that support domestic intelligence activities and the reliance on the intelligence cycle process model.

The National Network has been in development since 2003 and was established to serve as intelligence and analytical hubs[7] at the state, local, tribal, and territorial level. The National Network is supported by training and technical assistance in employing the intelligence cycle process model from DHS, the Department of Justice (DOJ), and other

[4] Intelligence and National Security Alliance, *Intelligence to Protect the Homeland: Taking Stock Ten Years Later and Looking Ahead*. White paper, Arlington: Homeland Security Intelligence Council, 2011.

[5] U.S. Department of Homeland Security, accessed June 7, 2013, http://www.dhs.gov/state-and-major-urban-area-fusion-centers.

[6] Frank J. Cilluffo, Joseph R. Clark, and Michael P. Downing, *Counterterrorism Intelligence: Law Enforcement Perspectives*, Counterterrorism Intelligence Survey Research, Homeland Security Policy Institute, George Washington University, September 2011.

[7] U.S. Department of Homeland Security, *Role of Fusion Centers in Countering Violent Extremism*, October 2012.

institutions. Providing federally funded training to the National Network on intelligence cycle process model variations, and their employment philosophies, serve as limitations to establishing fusion center baseline capabilities and their integration into national intelligence. Annual assessments are conducted on the National Network by DHS in efforts to evaluate baseline capabilities and their integration into national intelligence. The National Network completes an Online Self Assessment Tool that includes numerous multiple-choice and "yes/no" questions focused on the critical operational capabilities (COC) in support of the 2011 and 2012 DHS-led fusion center assessments.[8] While the COC questions focus on distinct aspects of the intelligence cycle process model, the 2011 and 2012 assessments do not evaluate the adherence to or wholly employing the intelligence cycle process model. A publication written by noted author and academic David Carter, who developed a local intelligence guide titled *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, affirms, "the need for a different approach to the intelligence cycle exists for the federal level compared to state, local, tribal and territorial elements because of different intelligence demands."[9]

The July 2010 DHS Bottom Up Review (BUR) that provides the results of a department-wide assessment reported, "there had been no systematic effort to ensure that these centers establish and maintain a baseline level of capability so that they are able to become fully integrated into national efforts to gather, analyze, and share information needed to protect our communities."[10] The 2010 BUR was addressed by the subsequent annual DHS-led National Network assessments. Notwithstanding, elements external to the National Network observed continued challenges with integrating local elements within the national intelligence architecture. A 2011 report by The Homeland Security

[8] U.S. Department of Homeland Security, *2012 National Network of Fusion Centers Final Report*, accessed October 8, 2013, http://www.dhs.gov/sites/default/files/publications/2012%20National%20Network%20of%20Fusion%20Centers%20Final%20Report.pdf.

[9] David Carter, U.S. Department of Justice, Office of Community Oriented Policing Services, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, 2nd ed., January 2009, 14.

[10] U.S. Department of Homeland Security, *Bottom-Up Review Report*, July 2010.

Policy Institute's Counterterrorism Intelligence Survey Research indicated 62 percent of the intelligence chiefs representing major metropolitan police departments in the U.S. believed the "national [federal] intelligence enterprise was such that it left them unable to develop a complete understanding of their local threat environment"[11] — an intended product of the intelligence cycle process model.

B. OVERVIEW

Intelligence derived from analyzed information through the intelligence cycle process serves as a principle tool for supporting the nation's counterterrorism efforts and offers law enforcement and homeland security officials with insights and advantages over terrorists. However, there are multiple intelligence cycle concepts within the USIC and the HSE. The various intelligence cycle process models range from a four-step process to a seven-step process.

The first depicted model of an intelligence cycle process was documented in 1944 and titled the *Production of Military Intelligence, a Continuous Process*.[12] Moreover, in 1948, Robert Rigby Glass published a book titled *Intelligence for Commanders* becoming the first known academic reference to an intelligence cycle process.[13] Subsequently there have been numerous books about the USIC and the intelligence cycle process. Author Leo D. Carl refers to the intelligence cycle as a five-step process in his 1990 book titled *The International Dictionary of Intelligence*.[14] Author Robert M. Clark in his 2004 *Intelligence Analysis: A Target-Centric Approach* refers to the traditional intelligence cycle as a six-step process.[15] The Naval Postgraduate School's Center for Homeland

[11] Frank J. Cilluffo, Joseph R. Clark, and Michael P. Downing, *Counterterrorism Intelligence: Law Enforcement Perspectives*. Counterterrorism Intelligence Survey Research. Homeland Security Policy Institute. George Washington University, September 2011.

[12] Michael E. Bigelow, "A Short History of Army Intelligence," *Military Intelligence*, July-September 2012, 31.

[13] Sources and Methods: Part 4 – *The Traditional Intelligence Cycle and Its History*, accessed December 1, 2011, http://sourceandmethods.blogspot.com/2011/05/part-4-traditional-intelligence-cycle.html.

[14] Leo d. Carl, *The International Dictionary of Intelligence* (McLean, VA. International Defense Consulting Service, 1990), 183.

[15] Robert M. Clark, *Intelligence Analysis: A Target-Centric Approach* (Washington, D.C.: CQ Press, 2004), 14.

Defense and Security Course NS4146 titled *Intelligence for Homeland Security*, by Dr. William Lahneman, refers to a seven-step process. The aforementioned noting of intelligence cycle process models reveals the diverse number of models and aids in identifying the potential challenges with providing consistent training and adherence to the National Network and the greater HSE. The DHS Homeland Security Advisory Council (HSAC), which provides advice and recommendations to the DHS Secretary on matters related to homeland security, noted effective intelligence and information fusion requires reliance on existing traditional USIC analytic processes. The HSAC defined "fusion" as a cyclic process that includes elements of a five-step intelligence cycle process.[16] This provides yet another version of the intelligence cycle process model. Table 1 provides a depiction of different intelligence cycle process models of USIC members, academia, and a state and local law enforcement element.

[16] U.S. Department of Homeland Security, *Intelligence and Information Sharing Initiative: Homeland Security Intelligence and Information Fusion*. Homeland Security Advisory Council. April 28, 2005, 5–7.

Table 1. The Various Types of Organizational Intelligence Cycle Models and Attributes

	Requirements	Planning & Direction	Collection	Processing & Exploitation	Analysis & Production	Dissemination	Consumption	Evaluation & Feedback
CIA		X	X	X	X	X		
FBI	X	X	X	X	X	X		
U.S. Air Force		X	X	X	X (Production)	X (Integration)		
U.S. Army		X	X	X		X		
U.S. Marine Corps		X	X	X	X (Production)	X	X (Utilization)	
U.S. Navy		X	X	X (Processing)	X (Production)	X		
DoD Joint Pub		X	X	X	X	X (Integration)		X
HSAC		X (Requirements Development)	X		X (Analysis)	X (Tasking, Archiving)		X (Reevaluation)
	Requirements	Planning & Direction	Collection	Processing & Exploitation	Analysis & Production	Dissemination	Consumption	Evaluation & Feedback
IOWA DPS		X	X	X (Processing)	X	X		
NPS-CHDS	X		X	X	X	X	X	X
PENN STATE		X (Planning, Direction, Needs, Requirements)	X	X	X (Analysis)	X		

The single intelligence cycle attribute used by all within the various intelligence cycle models is the “collection” phase. There are various intelligence cycle process models used by the USIC and now being taught to the National Network by federally funded entities. As an example, the DHS Office of Intelligence and Analysis (I&A), the

National Counterterrorism Center, the Memorial Institute for the Prevention of Terrorism (MIPT), the Department of Justice State and Local Anti-terrorism Training Program, and the International Association of Law Enforcement Intelligence Analysts (IALEA) each deliver intelligence training opportunities on intelligence cycle process model. The complexities of HSE are intensified when observed through the lens of different training entities and varied intelligence cycle process models. Consistent and clear intelligence cycle process employment within the National Network presents challenges with integration into the national intelligence architecture without a uniform training.

C. RESEARCH OBJECTIVES AND METHODOLOGY

The research process applies the basic program evaluation principles to gather information on the intelligence cycle process model adherence within the National Network and greater HSE. The research objective seeks to evaluate whether the National Network and HSE members adhere to the intelligence cycle process model when performing public safety and homeland security related missions.

This thesis employs a qualitative research method that analyzes and interprets publicly available academic and policy information gathered from government and nongovernment institutions regarding the conceptual and practical writings relevant to the intelligence cycle process model. In addition to the academic and policy data gathered, the writer provides a case study analysis of the April 15, 2013, Boston Marathon bombing focused on practical adherence to the phases of a general intelligence cycle process model. The applied research method is intended to provide the framework for exploring the employment of the intelligence cycle process model within the current HSE. A case study approach was chosen in an effort to explore adherence to the intelligence cycle process within the National Network in context to its origin and intended purpose. It is in this setting that the writer explores the National Network's adherence to the intelligence cycle process model considering their integration as a critical state and local asset within the broader national intelligence architecture.

Employing the intelligence cycle process model within the National Network and the greater HSE presents privacy concerns. Literature reveals these privacy concerns are

focused on the collection of information on Americans who have not violated the rule of law. Privacy concerns among policymakers also exist regarding the proper collection of information in support of domestic intelligence activities engagement by public and private HSE entities. Lastly, scholars and practitioners present concerns questioning whether the intelligence cycle process model serves as effective analytic tradecraft in reducing strategic surprises associated with a threat while simultaneously enhancing operational law enforcement and intelligence elements.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

The significance of examining the intelligence cycle process model within the HSE is well intentioned given it was not originally designed or intended to detect significant national security threats originating or residing within our nation's borders.[17] The literature examined provided a spectrum of knowledge about the intelligence cycle process model within the pre- and post-9/11 domestic intelligence environment. The evaluation of intelligence literature provided by academic, organizational and nongovernment consulting institutions revealed minimal discourse concerning the intelligence cycle process employment to support domestic intelligence activities.

The research literature includes publications from within and outside the government by high-level policy organizations and academia. The concentration of government publications reviewed were congressional legislation associated with homeland security and intelligence, as well as homeland security intelligence reports and information sharing related products of the Government Accountability Office and Congressional Research Service. A review of public and nonprofit organizations serving as consultants to the intelligence community and homeland security provided intelligence journals and articles, as well as academic intelligence publications by the Department of Defense (DoD) and public institutions. Finally, as appropriate, USIC organizational and National Network documents were reviewed specifically relating to intelligence cycle process model training and policies.

The literature review provided no USIC or HSE doctrinal information on the adoption of the intelligence cycle as a formal process by USIC or HSE members. Additionally, there are no specific standards concerning intelligence processes for domestic intelligence collection, whether at the federal level or the state and local level. However, there are documents that provide guiding principles regarding domestic intelligence collection and the use of the intelligence cycle process. The principle document governing the USIC (federal-level) role relevant to domestic intelligence

[17] Intelligence and National Security Alliance, *Intelligence to Protect the Homeland: Taking Stock Ten Years Later and Looking Ahead*. White paper, Arlington: Homeland Security Intelligence Council, 2011.

activities is Presidential Executive Order (EO) 12333. The DHS/DOJ endorsed guidelines for introducing the intelligence cycle process model into the National Network are the 2006 Fusion Center Guidelines[18] and the TCL[19] for state and local partners operating externally to the National Network. In March 2002, during an Intelligence Summit, the International Association of Chiefs of Police (IACP), an organization established in 1893 to serve as the professional voice of law enforcement, adopted the intelligence-led policing philosophy.[20] In 2011, the Major City Chief's Association (MCCA) initiated the Major City Chiefs' Criminal Intelligence Enterprise (MCCCIE) to better integrate state and local criminal intelligence and counterterrorism operations and address the deficiencies of standardizing integration and intelligence collection practices.[21] These guiding principles focus on the administration and management of the collection process, not necessarily a standardized employment of an intelligence cycle process model. An assessment of the limited information made available that focuses on domestic intelligence and the intelligence cycle employment reveals information gaps concerning its effectiveness and appropriateness within the post-9/11 HSE. This thesis attempts to explore whether the intelligence cycle is the best process model for domestic intelligence.

This literature review includes defining key intelligence enterprises, the term "intelligence" within the USIC and law enforcement, intelligence cycle process models, and training the intelligence cycle process to the HSE and National Network. The key intelligence enterprises discussed are the USIC, the Homeland Security Intelligence Enterprise (HSIE), and the HSE.

---

[18] U.S. Department of Homeland Security, *Fusion Center Guidelines Developing and Sharing Information and Intelligence in a New Era; Guidelines for Establishing and Operating Fusion Centers at the Local, State, and Federal Levels; Law Enforcement Intelligence, Public Safety, and the Private Sector*, accessed July 16, 2013, http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf.

[19] U.S. Department of Homeland Security, *Target Capabilities List: A companion to the National Preparedness Guidelines*, September 2007, accessed July 16, 2013, http://www.fema.gov/pdf/government/training/tcl.pdf.

[20] International Association of Chiefs of Police, *Criminal Intelligence Sharing: A National Plan for Intelligence-Led Policing at the Local, State and Federal Levels*. Alexandria, VA, 2002.

[21] Major Cities Chiefs Criminal Intelligence Enterprise, accessed August 25, 2013, https://www.majorcitieschiefs.com/pdf/news/mcca_criminal_intelligence_enterprise_initiative_20120329.pdf.

A. DEFINING KEY INTELLIGENCE ENTERPRISES AND THE TERM "INTELLIGENCE"

The USIC is formally defined in EO 12333 titled *United States Intelligence Activities*. An EO serves as an official document to manage the operations of the federal government.[22] The EO 12333 is an extremely complex order that sets forth the foundation of the USIC and the administration's directions regarding "timely and accurate information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons and their agents."[23] Its support of national security consists of three key parts: Part 1) defines each intelligence community member and the particular roles and responsibilities; Part 2) focuses on the protection of civil liberties and privacy rights; and Part 3) provides relevant definitions. The 17-members consisting of the USIC are primarily concerned with foreign intelligence and counterintelligence, as prescribed in EO 12333, with the only agencies focusing on domestic intelligence are the

FBI and the newly created DHS.[24] EO 12333 was originally signed in 1981 under the Reagan Administration and since amended in 2008 under the Bush Administration because of the 9/11 terrorist attacks. EO 12333 provides the goals, direction, and responsibilities of USIC members performing intelligence activities within the U.S. There have been several amendments to EO 12333 since the original signing: in 2003 by EO 13284, in 2004 by EO 13355, and lastly in 2008 by EO 13470. The 2003 amendment by EO 13284 provided for the inclusion of the DHS Office of Intelligence and Analysis. The 2004 amendment by EO 13355 was designed to strengthen the management of the intelligence community. Lastly, the 2008 amendment by EO 13470 made administrative changes, to include language focused on state, local, and tribal governments as well as the private sector:

> State, local, and tribal governments are critical partners in securing and defending the United States from terrorism and other threats to the United

[22] National Archives, accessed July 27, 2013, www.archives.gov/federal-register/executive-orders/about.html.

[23] Ibid.

[24] Sephan J. Flanagen, *Managing the Intelligence Community*, International Security, vol. 10, no. 1, (Summer 1985), MIT Press, accessed June 13, 2012, http://www.jstor.org/stable/2538790.

> States and its interests. Our national intelligence effort should take into account the responsibilities and requirements of state, local and tribal governments and, as appropriate, private sector entities, when undertaking the collection and dissemination of information and intelligence to protect the United States.[25]

While every USIC member has the authority and responsibility for implementing EO 12333 within their respective organizations, the two chief organizations responsible for ensuring successful implementing and providing direction is the DNI and DOJ/FBI.

The DHS HSIE consists of three DHS headquarter elements that have an intelligence function: The Office of Intelligence and Analysis, the Homeland Infrastructure Threat and Risk Analysis Center, and the Intelligence Division of the Office of Operations Coordination and Planning. It also consists of the intelligence element of six operational components: U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, U.S. Citizenship and Immigration Services, Transportation Security Administration, U.S. Coast Guard, and U.S. Secret Service.[26] While there is a described HSIE, the term *homeland security intelligence* has yet to be defined or codified in law.[27] Noted author Frances Townsend, the former Homeland Security Advisor under President Bush and former Chairwoman of the nonprofit, public-private organization Intelligence and National Security Alliance, defined *homeland security intelligence* as a discipline that depends on the successful fusion of foreign and domestic intelligence to produce the kind of actionable intelligence necessary to protect the homeland.[28]

The DHS Undersecretary for Intelligence and Analysis serves as the Department's Chief Intelligence Officer (CINT) responsible for leading the HSIE. The DHS' Management Directive Number 8110 titled *Intelligence Integration and Management*

---

[25] Executive Order 13470, *Further Amendments to Executive Order 12333, United States Intelligence Activities*, Part 1 1.1(f), accessed July 27, 2013, www.fas.org/irp/offdocs/eo/eo-13470.htm.

[26] Congressional Research Service, *The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress*, R40602, May 27, 2009, 3.

[27] Congressional Research Service, *Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches*, RL33616, January 14, 2009, 9.

[28] Frances Townsend, *Intelligence to Protect the Homeland - Taking Stock Ten Years Later*. Intelligence and National Security Alliance 1 2011, 3.

established the CINT position to effectively integrate and manage DHS intelligence programs, as well as serve as the principle for leading, governing, integrating, and managing intelligence functions throughout DHS.[29] The DHS CINT is tasked with being the primary connection between DHS and the USIC, as well as the primary source of information for state, local, tribal, and private sector partners. To date, there has only been two Senate confirmed DHS CINTs. The first CINT was the Honorable Charles Allen, a 40-year senior Central Intelligence Agency official who served as the first DHS CINT from 2005–2009 and was responsible for developing the department's intelligence architecture.[30] The second CINT was the Honorable Caryn Wagner, a 30-year DoD official who served as the DHS CINT from 2010 to 2012[31] and during her tenure provided a focus of "creating a true homeland security information-sharing enterprise through a greater focus on state, local, and major urban area fusion centers," as well as "unify and sustain the DHS intelligence enterprise."[32]

The HSE was defined by a DHS report on the National Network as federal, state, local, tribal, nongovernmental, and private sector entities.[33] Integration of the HSE into the national intelligence architecture was intended to occur through the National Network. Other than the 2011 DHS report, the examination of literature does not provide any other formal HSE definition, although the term is frequently used in government and academic articles. Similar to the term *homeland security intelligence*, the failure to provide a unified and accepted definition among stakeholders encumbers the ability to assess the effectiveness of the intelligence cycle process model.

---

[29] U.S. Department of Homeland Security, Management Directive 8110, *Intelligence Integration and Management*, accessed August 4, 2013, http://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_8110_intelligence_integration_and_management.pdf.

[30] Chertoff Group, accessed August 4, 2013, http://chertoffgroup.com/bios/charles-allen.php.

[31] U.S. Department of Homeland Security, accessed August 4, 2013, http://www.dhs.gov/caryn-wagner.

[32] Anthony L. Kimery, *Homeland Security Today*, "DHS I&A Chief Outlines New Vision," May 13, 2010, accessed August 7, 2013, http://www.hstoday.us.

[33] U.S. Department of Homeland Security, *2011 National Network of Fusion Centers Final Report*, May 2012, 2.

Intelligence is a term that has multiple meanings dependent upon the literary contribution whether it has a USIC or law enforcement origin. An examination of literature commonly discussed what "intelligence" means or at least how an author intended to use the term. Prior to the terrorist attacks of September 11, 2011, academic and federal government literature largely referred to intelligence within the context of issues related to national security associated with defense, foreign policy, and internal (domestic) security.[34] However, the term "intelligence" within the context of law enforcement often refers to significant information that is relevant to an impending event and that will be a contribution to the positive outcome of a specific case.[35] Lowenthal subscribes that intelligence can be defined from three different perspectives: 1) "Intelligence as a product – intelligence that can be thought of as a product of the [process]," 2) "Intelligence as a process – intelligence [that] can be thought of as the means by which certain types of information are required and requested, collected, analyzed, and disseminated…," and 3) "Intelligence as an organization – intelligence…thought of as the units that carry out its various functions."[36]

In the post-9/11 environment, intelligence began to be more widely accepted and used among state, local, tribal, territorial, and private sector elements as key partners within the HSE. For the purpose of this thesis, "intelligence" is defined as the collective "functions [and] activities…which are involved in the [intelligence] process [model] of planning, gathering, and analyzing information of potential value to decision makers."[37]

[34] U.S. Department of Homeland Security, *2011 National Network of Fusion Centers Final Report*, May 2012, 4.

[35] Roger G. Dunham, Geoffrey P., Alpert, Jennifer E. Davis, and Robert W. Taylor, *Intelligence-Led Policing and Fusion Centers, Critical Issues in Policing: Contemporary Readings* (6th ed., Waveland Press, 2010), 225.

[36] Mark M. Lowenthal, *Intelligence: From Secrets to Policy* (Washington, D.C., CQ Press, 2012). 9.

[37] Leo D. Carl, *The International Dictionary of Intelligence* (McLean, VA. International Defense Consulting Service, 1990), 178.

B. INTELLIGENCE CYCLE PROCESS MODELS

A review of journals and scholarly publications provided descriptions of intelligence cycle process models. However, it was difficult uncovering its origination and the policies associated with its formal adoption within the USIC. According to the International Journal of Information Management, an international peer-reviewed journal, the use of the intelligence cycle was first derived from the U.S. Army.[38] In 1920, the Army's Chief of Staff attempted to establish the first Army-wide intelligence doctrine via the distribution of *Intelligence Regulations.*[39] Author Michael Bigelow, Command Historian with the U.S. Army Intelligence and Security Command, contends the first depicted model of the intelligence process was documented in 1944, under the title the *Production of Military Intelligence, a Continuous Process.*[40]

In 1952, intelligence collection, the single most common intelligence cycle attribute was defined as the procuring, assembling and organizing of information and served as the first step in the processing of intelligence information. It is now considered the third step or phase in the intelligence cycle process model and "…officially defined as 'the exploitation of sources of information by collection agencies and delivery of information to the proper intelligence-processing unit for use in the production of intelligence.'"[41] The 1952 definition focused on intelligence collection targeted against communist nation-states and not the domestic intelligence environment of today.

The intelligence cycle process model in simple discourse involves structured steps necessary for gathering required data in order to create knowledge. The created knowledge (intelligence) in the early years served executive and congressional policymakers primarily focused on Cold War adversaries in an attempt to uncover foreign intelligence activities and assist with supporting global national security interests.

---

[38] "Targeting Intelligence Gathering in a Dynamic Competitive Environment," *International Journal of Information Management*, 20, iss. 3, 2000: 184.

[39] Michael E. Bigelow, "A Short History of Army Intelligence." *Military Intelligence*, July-September 2012, 21.

[40] Ibid., 31.

[41] Leo D. Carl, *The International Dictionary of Intelligence* (McLean, VA. International Defense Consulting Service, 1990), 59.

Prior to the September 11 terrorist attacks, the FBI served as the principle federal agency responsible for domestic intelligence. In response to criticism by Congress following the attacks, the FBI initiated reforms to increase their collection and analysis of domestic intelligence. Nonetheless, critics contend FBI intelligence collection play a secondary role to their law enforcement mission.[42] Because of the September 11, 2001, Al-Qaida terrorist attacks that emphasized intelligence failures, the stated integration of the intelligence cycle process model became a common theme among public safety officials at the state, local, tribal, territorial and private sector levels. The new intelligence mission has by both necessity and practice expanded beyond the federal-level originally identified in the 1947 National Security Act and is now based on the principle of shared responsibility and partnership with state and local governments, the private sector, and the American people in a concerted national effort to prevent future terrorist attacks within the U.S.[43]

There are multiple intelligence cycle process model versions within the USIC, the HSIE and the HSE, which range from four-step process to a seven-step process. Many authors indicated that the intelligence cycle process model is more or less a common practice of how intelligence professionals perform the functions of intelligence. For the purpose of this thesis, the intelligence cycle is defined according to the official USIC definition as "the steps by which information is acquired and converted into intelligence and made available to consumers."[44] Similarly to the many academic descriptions of the intelligence cycle process models, USIC organizational models depend on the organization and its mission-space. The diverse number of intelligence cycle models stresses the need for an HSE-wide accepted intelligence cycle process doctrine.

[42] Eric Rosenbach, *Confrontation or Collaboration? Congress and the Intelligence Community*. Belfere Center for Science and International Affairs. The Intelligence and Policy Project. Background Memorandum for the 111th Congress. July 2009, 44–49.

[43] Office of Homeland Security, *National Strategy for Homeland Security*, July 2002, 2.

[44] Leo D. Carl, *The International Dictionary of Intelligence* (McLean, VA. International Defense Consulting Service, 1990), 183.

C. CORE ISSUE

The intelligence cycle process model continually strives to better understand the threat environment or a threat issue. Understanding is accomplished and supported by relying on past and present information necessary to deliver a probabilistic view of the future. The basic intelligence cycle process model involves sequenced steps necessary for gathering the information in order to create the desired understanding. While literature plainly reveals the cyclical structure of intelligence cycle process model, literature also suggests the intelligence cycle process model does not sufficiently describe how the intelligence process works at the operational stages of domestic intelligence activities within the National Network. Within the USIC, however, the intelligence cycle process model appears to be an academic process conducted primarily by analysts and not operational intelligence collectors. As an example, in a doctoral dissertation written by Ms. Bridget Nolen on USIC information sharing and collaboration she noted "An analyst will sometimes write a paper on a self-generated topic, but much of the time the analyst is responding to a 'tasking,' which means that a policymaker has a specific question that he or she wants a subject matter expert to answer. The analyst drafts a response as quickly as possible by putting together the available information from a variety of classified and open sources, and must then begin the arduous coordination process to ensure that other analysts in the Intelligence Community concur with the assessment. After the paper is coordinated, it must then go through many more layers of editing through management, and then a final edit for style, structure, and formatting before it can be published—that is, delivered to policymakers."[45]

A critical juncture in the process identified by Nolen is coordination. This corresponds with the independent phase "production" or the joint phase "analysis and production" dependent on which intelligence cycle process model is being used. During this phase, it is noted "...each paper an analyst writes is considered a 'community' product...,so it is important that other experts vet an analyst's work before the policy

[45] Bridget Rose Nolen, *Information Sharing and Collaboration in the United States Intelligence Community: An Ethnographic Study of the National Counterterrorism Center* (PhD diss., University of Pennsylvania, 2013), 90.

maker reads it. At this theoretical level, coordination makes sense. In practice, however, the coordination process frequently transforms into a battle over turf, a venue for blatant backstabbing, and a practice rooted in nitpicking and meaningless editing...."[46] Another cogent example identifying the challenges of finished intelligence—the theoretical end result of a perfectly functioning intelligence cycle process model—is provided from an interview excerpt "NCTC has to coordinate with everyone. It is difficult when DHS thinks they can call the editors personally and hold your piece because they think it interferes with their business project. Like with terrorist documents—we might write about how terrorists exploit student visas, and well, State issues the student visas and they do not like the fact that we are criticizing the loopholes in their system. So they'll hold the piece or try to kill it."[47] These issues point out the practical challenges with employing the intelligence cycle process model within the USIC established in 1947, accordingly, similar challenges are present within the complex National Network and the HSE.

Author Leo D. Carl reference to the intelligence cycle as a five-step process in his 1990 *The International Dictionary of Intelligence* includes: 1) Planning and Direction, 2) Collection, 3) Processing, 4) Production, and 5) Dissemination.[48] Author Robert M. Clark in his 2004 *Intelligence Analysis: A Target-Centric Approach* describes the traditional intelligence cycle as a six-step process: 1) Requirements, needs, 2) Planning, direction, 3) Collection, 4) Processing, 5) Analysis, and 6) Dissemination.[49] Lastly, the Naval Postgraduate School Center for Homeland Defense and Security's Course NS4146 titled *Intelligence for Homeland Security*, by Dr. William Lahneman offers to a seven-step process: 1) Requirements, 2) Collection, 3) Process and Exploitation, 4) Analysis and Production, 5) Dissemination, 6) Consumption and 7) Feedback. The aforementioned

[46] Bridget Rose Nolen, *Information Sharing and Collaboration in the United States Intelligence Community: An Ethnographic Study of the National Counterterrorism Center* (PhD diss., University of Pennsylvania, 2013), 90–91.

[47] Ibid., 98–99.

[48] Leo D. Carl, *The International Dictionary of Intelligence* (McLean, VA. International Defense Consulting Service, 1990), 183.

[49] Robert M. Clark, *Intelligence Analysis: A Target-Centric Approach* (Washington, D.C.: CQ Press, 2004), 14.

noting of intelligence cycle process models reveals the diverse number of models and aids in identifying the potential challenges with providing consistent training and adherence to the National Network and broader HSE.

The DHS HSAC cyclic process included a five-step intelligence cycle process: 1) Planning and Requirements Development, 2) Collection, 3) Analysis, 4) Dissemination, Tasking, and Archiving, and 5) Reevaluation.[50] This provides yet another version of the intelligence cycle process model.

The four figures below serve as diagrams illustrating the diversity of intelligence cycle process models, similar to the table provided in Chapter I. While there are minor but important differences, not one of the four is exactly alike, although each element is a member of the national intelligence architecture.

[50] U.S. Department of Homeland Security, *Intelligence and Information Sharing Initiative: Homeland Security Intelligence and Information Fusion*. Homeland Security Advisory Council. April 28, 2005, 5–7.

Figure 1. FBI Intelligence Cycle[51]

Figure 2. The Iowa State Police Intelligence Cycle[52]

[51] Federal Bureau of Investigation, accessed September 4, 2013, http://www.fbi.gov/about-us/intelligence/intelligence-cycle.

[52] Iowa Department of Public Safety, accessed September 4, 2013, http://www.dps.state.ia.us/intell/intellcycle.shtml.

Figure 3. CIA Intelligence Cycle[53]

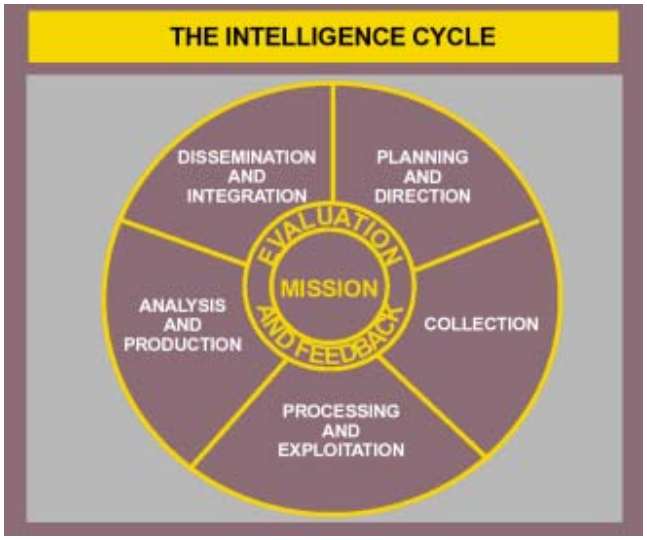

Figure 4. DoD Joint Publication Intelligence Cycle[54]

The integration of state, local, tribal, territorial and private sector elements as nontraditional intelligence partners of the HSE has shepherded the need to fundamentally change the requirement to provide intelligence not just to the federal level organizations, the president and Congress, but also to state and local policymakers and operational

[53] U.S. Central Intelligence Agency, accessed September 4, 2013, http://vmc.cia-dia.50megs.com/fboi/facttell/intcycle.htm.

[54] U.S. Department of Defense, accessed September 4, 2013, http://www.dodccrp.org/events/9th_ICCRTS/CD/papers/044.pdf.

entities. It involves evaluating the profound differences between providing classified information to policymakers, such as during the Cold War, and providing homeland security intelligence and threat information to the private sector, public organizations and U.S. Citizens in a post-9/11 domestic intelligence environment.[55]

The 9/11 Commission Act, Section 511 provides DHS shall establish a DHS State, Local, and Regional Fusion Center Initiative necessary for establishing partnerships with state, local, and regional fusion centers; specifically Section (b) (11) mandates providing training to state, local, and regional fusion centers.[56] The DHS I&A concurred with the responsibility per Section 511 to develop training curricula on the intelligence cycle process for state and local officials.[57] In satisfying this mandate, DHS deployed intelligence officers charged with managing the intelligence cycle in their areas of responsibility.[58] While fusion center personnel receive DHS sponsored intelligence cycle training from a variety of federally funded institutions, this is not the case for a majority of public safety officials operating outside the National Network such as the MCCCIE initiative.

The Major Cities Chiefs Association, an organization comprised of police chiefs and sheriffs from 63 of the largest law enforcement agencies in the U.S., initiated the MCCCIE in 2011. Serving as a significant representative of the state and local criminal intelligence community, the MCCCIE's aim is to better integrate state and local criminal intelligence and counterterrorism operations in support of the National Network by addressing the deficiencies of standardizing integration and intelligence collection

[55] Elaine C. Kamarck, *Transforming the Intelligence Community: Improving the Collection and Management of Information*. John F. Kennedy School of Government, Harvard University, IBM Center for The Business of Government, October 2005, 11.

[56] 110th Congress Public Law, Public Law 110–53, *Implementing Recommendations of the 9/11 Commission Act of 2007*.

[57] U.S. Department of Homeland Security, *DHS' Role in State and Local Fusion Centers is Evolving*. Office of Inspector General Report – OIG-09–12. October 2008. 16.

[58] U.S. Department of Homeland Security, *Responsibilities of Intelligence Officers*, accessed March 7, 2013, http://www.dhs.gov/deployed-intelligence-officers-and-protective-security-advisors.

practices within the state and local environment.[59] Figure 5 depicts a four-step Prediction-Led Policing Business Process Model that may be viewed in the context of the intelligence cycle process model. The Prediction-Led Policing Business Process Model is based on a concept established by the Center for Problem-Oriented Policing with the first two phases focusing on collecting and analyzing criminal information necessary for establishing predictions and the last two phases focus on response to the predictions.[60] The parallels between the intelligence cycle process model and the prediction-led policing process model is the critical need for information collection and analysis.

This critical segment of the HSE receives considerably less training on the intelligence cycle process model, although it oversees far more personnel than the National Network. There are questions law enforcement intelligence analysts use to ascertain a threat or the threat situation using the intelligence cycle process model that are not readily obvious to law enforcement investigators.[61] The contrasting perspectives associated with the intelligence cycle process model between law enforcement intelligence analysts and law enforcement investigators parallel the environmental setting within the USIC between intelligence analysts and operational intelligence collectors.

[59] Major Cities Chiefs Criminal Intelligence Enterprise, accessed August 25, 2013, https://www.majorcitieschiefs.com/pdf/news/mcca_criminal_intelligence_enterprise_initiative_20120329.pdf.

[60] RAND, *Predictive Policing – The Role of Crime Forecasting in Law Enforcement Operations*, Prediction-Led Policing Business Process Model, accessed October 3, 2013, http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf.

[61] Timothy Connors, and John Rollins, Center for Policing Terrorism at the Manhattan Institute. *State Fusion Center Processes and Procedures: Best Practices and Recommendations* (Policing Terrorism Report, No. 2, September 2007), 3.

Figure 5. The Prediction-Led Policing Business Process Model, RAND RR233–1.1[62]

The terrorist events of 9/11 vastly transformed law enforcement communities across the U.S. and the approach to preventing and combating terrorism that focused on proactive posturing versus reactive engagement.[63] New transnational enemies possibly operating within the homeland in the form of international terrorists and transnational issues, such as narcotics and money laundering have risen in importance becoming more urgent than the previous Cold War era geopolitical concerns. As the intelligence and law enforcement communities have both become increasingly involved in the international aspects of terrorism, drug trafficking, and international organized crime, the National Network is positioned to access the USIC's considerable wealth of information on these subjects. However, in considering the fulfillment of these capabilities by the HSE, this issue has been the most difficult to resolve.[64]

[62] RAND, accessed October 3, 2013, http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf.

[63] Roger G. Dunham, Geoffrey P. Alpert, Jennifer E. Davis, and Robert W. Taylor, *Intelligence-Led Policing and Fusion Centers, Critical Issues in Policing: Contemporary Readings*, 6th ed, Waveland Press, 2010, 224.

[64] *The Intelligence Community in the 21st Century*: Staff Study - Permanent Select Committee on Intelligence House of Representatives 104th Congress, accessed March 5, 2013, http://www.gpo.gov/fdsys/pkg/GPO-IC21/html/GPO-IC21–13.html.

The HSIE, through DHS I&A, authorizes intelligence collection activities that serve to support the National Network and the HSE in efforts to identify emerging homeland security threats. The DHS I&A intelligence collection efforts of DHS Intelligence Officers supporting the National Network was detailed in a July 29, 2008 DHS Memorandum. On April 3, 2008, DHS CINT Honorable Charles Allen under DHS Intelligence Oversight procedures defined homeland security threats to include "all threats or hazards, regardless of origin, that relate to: critical infrastructure or key resources; a significant public safety, public health or environmental impact; political, societal and economic infrastructure; border security; the proliferation or use of weapons of mass destruction; or other potential catastrophic events including man-made and natural disasters."[65]

An examination of literature provides general knowledge and reveals minimal discourse concerning the intelligence cycle process model employment within the context of domestic intelligence collection activities, specifically within the National Network. DHS and other entities continue to provide training and instruction on various intelligence cycle process models to the 78 state and major urban area fusion centers that embody the National Network.

Lowenthal proclaims one of the stated goals of the U.S. intelligence process (intelligence cycle) is to have "analysis-driven collection." A short hand way of recognizing that collection priorities should reflect the intelligence needs required to produce analysis.[66]

There are disagreements in literature as writer Arthur S. Hulnick, a professor at Boston University who served seven years as an U.S. Air Force Intelligence Officer and 28 years with the Central Intelligence Agency (CIA), claims the intelligence cycle is really not a very good description of the ways in which the intelligence process works and "the notion that policymakers or intelligence consumers provide guidance to

[65] U.S. Department of Homeland Security, *Roles and Function*, Office of Intelligence and Analysis General Counsel Memorandum, July 29, 2008.

[66] Mark M. Lowenthal, *Intelligence: From Secrets to Policy*. (Washington, D.C.: CQ Press, 2003), 60–61.

intelligence managers to begin the intelligence process is incorrect."[67] Robert Clark, a 42-year Intelligence Analyst, faculty member of the Intelligence and Security Academy and a professor of intelligence studies at the University of Maryland University College, likewise challenges the intelligence cycle process model's effectiveness and contends "intelligence is organized around the flawed concept of an intelligence cycle"[68] and "over the years the intelligence cycle has become somewhat of a theoretical concept…[and] when pressed many intelligence officers admit that the intelligence process 'really doesn't work like that.'"[69]

The evaluation of the intelligence cycle process model, based on the writers' presentation, suggest the theoretical intelligence cycle is a simple process beginning with customer needs and ending with providing a product that satisfies those needs. Inconsistencies with employing the intelligence cycle process model surface because of existing conflicts among intelligence and law enforcement analytic and operational components. With the inclusion of DHS into the USIC, along with state and local entities as key HSE elements, there exists an essential challenge—what intelligence process training should be provided to the National Network and HSE? In addition, is current intelligence cycle process training provided to the National Network and HSE appropriate and effective? Given literature overlooks a standardized intelligence cycle process model that does not exist. Furthermore, literature reflects significant historical abuses along with current events that illustrate challenges with domestic intelligence activities specifically collection.

Unlike at the federal-level within the USIC, the National Network made up of mainly law enforcement centric elements view the intelligence process from a different perspective. Prior to using the intelligence cycle as a business practice, state and local law enforcement integrated intelligence-led policing as the standard business practice for "analysis-driven collection." Law enforcement's acceptance of intelligence-led policing

[67] Arthur S. Hulnick, *What's Wrong with the Intelligence Cycle*. Intelligence and National Security 21. No. 6. December 2006. 959.

[68] Robert M. Clark, *Intelligence Analysis: A Target-Centric Approach* (Washington, D.C.: CQ Press), 2004. 12.

[69] Ibid., 15.

advanced the goal of developing a universal process that would integrate both law enforcement and national security intelligence agendas. The result was the intelligence cycle process model[70] although some have affirmed there are fundamental differences between national security and local law enforcement intelligence. The fundamental differences that exist between the law enforcement perspective and traditional intelligence community perspective, regarding intelligence collection, results in a less than effective intelligence platform within the homeland.[71]

In a September 2011 publication by the Intelligence and National Security Alliance titled *Intelligence to Protect the Homeland: Taking Stock Ten Years Later and Looking Ahead*, former FBI Executive Assistant Director for Intelligence Maureen Baginski, a former NSA senior intelligence official who headed the FBI Directorate of Intelligence created in 2005, claims that many federal intelligence and law enforcement professionals do not recognize the homeland security implications and intricacies of criminal information.[72] Jennifer Sims, a Senior Fellow for National Security at the Chicago Council on Global Affairs and a Visiting Professor in the Security Studies Program at Georgetown University along with Burton Gerber, a CIA Distinguished Intelligence Medal recipient and former 39-year CIA employee acknowledges, "[a] critical difference between law enforcement and traditional intelligence collection is that law enforcement gathers hard truth in the form of evidence; prosecutors and courts require this."

The intelligence collection phase under the intelligence cycle process model covers the gray area and makes estimations, which is what the consumer demands. The "gray area" centers on how to effectively perform domestic intelligence activities while employing the intelligence cycle process model among HSE members concurrently protecting privacy, civil liberties, and civil rights. Chapter III offers the historical and

[70] Roger G. Dunham, Geoffrey P. Alpert, Jennifer E. Davis, and Robert W. Taylor, *Intelligence-Led Policing and Fusion Centers, Critical Issues in Policing: Contemporary Readings*, 6th ed, Waveland Press, 2010, 232.

[71] Jennifer E. Sims, and Burton Gerber, *Transforming U.S. Intelligence* (Washington, D.C., Georgetown University Press, 2005), 208–209.

[72] Intelligence and National Security Alliance, *Intelligence to Protect the Homeland: Taking Stock Ten Years Later and Looking Ahead*. White paper, Arlington: Homeland Security Intelligence Council, 2011.

post-9/11 challenges of domestic intelligence activities, specifically the collection phase of the intelligence cycle process model.

The HSE receives intelligence training from many organizations, such as DHS I&A, DOJ Bureau of Justice Assistance, MIPT, the Institute for Intergovernmental Research, as well as many academic institutions. When combining the many versions of the intelligence cycle process model and the various organizations providing intelligence training on one of its many versions to the HSE, the question surfaces as to its effective adherence.

D. HOMELAND SECURITY ENTERPRISE AND NATIONAL NETWORK INTELLIGENCE CYCLE TRAINING

The previous section of the literature review focused on defining key intelligence enterprises, the term "intelligence" within the USIC and law enforcement, and the intelligence cycle process and its many variations. This section of the literature review will focus on training the intelligence cycle within the HSE and National Network.

The analysis of limited information made available regarding HSE and National Network intelligence cycle employment reveals gaps concerning its effectiveness and appropriateness within the post-9/11 environment. The HSE and National Network receive training from federal, government sponsored and academic institutions on the intelligence cycle process model with an emphasis on enhancing domestic intelligence capabilities to prevent future terrorist attacks.

Providing structured training on the intelligence cycle process model should make the most of the HSE and National Network efforts to detect, neutralize, and exploit terrorist strategies and tactics. Well-trained analysts within the National Network are critical to efficient intelligence analysis. However, even with pristine data, a lack of strong analytics may result in less-than-desirable intelligence products and operational outcomes.

Additionally, employing the intelligence cycle process model within the National Network and the greater HSE have presented several concerns. Among privacy advocates, there are privacy concerns regarding collection of information on Americans

who have not violated the rule of law. Among policy makers, there are concerns regarding the proper collection of information in support of domestic intelligence activities among public and private HSE entities. Lastly, among scholars and practitioners, there are concerns the intelligence cycle process model may not serve as an effective analytic tradecraft competency in reducing strategic surprises associated with a threat, while simultaneously enhancing operational law enforcement and intelligence elements. The literature review did not provide standardized doctrinal information on the adoption of the intelligence cycle as a formal process by USIC, HSIE or HSE members. However, guiding principles such as EO 12333 (as amended), the 2006 Fusion Center Guidelines, and the TCL provided a common framework to introduce the intelligence cycle process model.

The DHS State and Local Program Office, in conjunction with the DHS Federal Emergency Management Agency (FEMA) and DOJ provides intelligence cycle training opportunities to the National Network and HSE via the DHS/DOJ Fusion Process Technical Assistance Program and Services, the FEMA sponsored MIPT. There are a number of academic institutions that also provide intelligence cycle training, most notably the Naval Postgraduate School's Center for Homeland Defense and Security and the Michigan State University. The author and academic David Carter with Michigan State University developed a local intelligence guide titled *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies* highlighting the need for a different approach to the intelligence cycle at federal level when compared to state, local, tribal and territorial level based on different intelligence demands.[73]

Literature clearly agrees that the intelligence cycle is used as the traditional intelligence process at the federal level within the USIC. Because of the federal government's support to the state and local environment via the National Network, DHS provides instruction on the intelligence cycle process to state and local officials within

[73] David L. Carter, U.S. Department of Justice, Office of Community Oriented Policing Services, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, 2nd ed., January 2009, 14.

the National Network and limited HSE elements. As highlighted by author David Carter, there is a cultural contradiction that exists in traditional law enforcement notwithstanding the recent focus on the intelligence-led policing (ILP) model that focuses on identifying criminal behavior, reporting criminal activity and preventing future crimes based on trends and patterns.

Mr. Carter acknowledges the private sector is often a legitimate consumer of law enforcement intelligence meeting the "right to know" and "need to know" in support of information sharing standards. Similar to the majority 18,000 U.S. law enforcement agencies, the private sector as a significant element of the HSE that owns an estimated 85 percent of the nation's critical infrastructure is generally not slated to receive federally funded intelligence cycle process training. Moreover, the private sector has a large personnel force who, if given the proper information, can significantly increase the "eyes and ears" on the street to observe individuals and behaviors that pose threats. However, there are information sharing issues that need to be resolved. For example, certain types of personal information may be inappropriate for law enforcement to release to the private sector. Conversely, proprietary information related to corporate products may also be restricted. Despite these limitations, there is a legitimate intelligence role for the private sector.[74]

Mr. David Cid, MIPT Executive Director, similarly recognizes the law enforcement cultural contradiction to intelligence and asserts avoiding strategic surprise is a principle function of intelligence that allows law enforcement to be anticipatory and proactive in efforts to prevent potential terrorist attacks. However, traditional measures of success in law enforcement, such as arrests, indictments, and seizures of property are secondary to prevention.[75]

Common themes within the literature advances intelligence cycle models as a key element of the USIC. The literature also reveals disagreements about its effectiveness at

[74] David L. Carter, White paper, *The Intelligence Fusion Process for State, Local and Tribal Law Enforcement*, Michigan State University, May 2006, accessed March 3, 2013, http://www.ncirc.gov/documents/public/intelligence_fusion_process.pdf, 7.

[75] David Cid, *Understanding Counterterrorism: A Guide for Law Enforcement Policy Makers and Media*, 2012, 264, 268.

the practitioner level, as well as its many variations based on organizational mission space. Finally, the literature overlooks or perhaps shortchanges the question of whether the intelligence cycle process model is effective or appropriate within the HSE and the National Network, while revealing the challenges of domestic intelligence collection, which will be focus of the following chapter.

THIS PAGE INTENTIONALLY LEFT BLANK

III. DOMESTIC INTELLIGENCE AND EMPLOYING THE INTELLIGENCE CYCLE PROCESS MODEL

> We also have no official with sole and comprehensive responsibility for domestic intelligence. It is no surprise that gaps in domestic intelligence are being filled by ad hoc initiatives.
>
> – Judge Richard Posner, U.S. Court of Appeals

The focus of this thesis provides an academic inquiry into the intelligence cycle process adherence within the National Network and the greater HSE. The information contained in this publication may reflect the intelligence cycle process as an idealistic model while highlighting the challenges of adopting a standardized intelligence cycle process acceptable among homeland security professionals. Chapter III is intended to offer illustrations relevant to the challenges of executing domestic intelligence activities. The central points are identifying the national security focus of domestic intelligence policies, the exploitation of domestic intelligence authorities, and cultural differences between the USIC and elements of the HSE that effect the employment of the intelligence cycle process model.

A. DOMESTIC INTELLIGENCE ACTIVITIES – NATIONAL SECURITY FOCUS

The USIC, established by the 1947 National Security Act because of World War II, differs in many ways from its present structure. The 1947 National Security Act established a national effort to protect the U.S. from foreign actors in response to the Japanese attack on Pearl Harbor and the subsequent Cold War with the Soviet Union. As a result of the terrorist acts committed on September 11, 2001, the USIC changed to introduce two new members of the USIC; the DNI; and DHS I&A. The 9/11 attacks on the U.S. served as a motivator for yet another national effort to protect the U.S. from both foreign terrorists operating abroad and within U.S. borders. A national policy or doctrine

regarding a standard intelligence process is critical, since professional intelligence officers often think of their primary mission of information collection and analysis in terms of an "intelligence cycle."[76]

Historically, America has responded to the need for domestic intelligence in four ways. First, avoid it. There was less than a page-sized narrative devoted to intelligence in the 2002 National Strategy for Homeland Security. Second, construct ad-hoc arrangements without clear oversight and authority, which led to political abuse in the 1975 Church Commission Report. Third, allow the FBI and CIA to perform limited and highly scrutinized overt domestic intelligence collection activities per EO 12333. Fourth, assume the law enforcement community can substitute for intelligence.[77]

The National Network assumed a key role to address counterterrorism threat information sharing and intelligence analysis at the state and local level. The annual Fusion Center Assessments, a critical component of a broader Fusion Center Performance Program, is designed to measure pre-determined baseline capabilities and holistic performance of the National Network[78] fulfilling the shortcomings identified in the 2010 DHS BUR.

The DHS, in coordination with interagency partners, Fusion Center Directors, and other fusion center stakeholders, manages the annual assessment process that focuses primarily on measuring four COCs,[79] which contain elements of the intelligence cycle process model – collection, analysis, production, and dissemination. The 78 fusion centers that constitute the National Network completed the 2011 and 2012 Fusion Center Assessments allowing DHS to collect data necessary for measuring their progress in achieving baseline capabilities that include the COCs as key performance objectives within the National Network.

---

[76] Loch K. Johnson, and James J. Wirtz, *Intelligence and National Security: The Secret World of Spies-An Anthology* (Oxford, NY: Oxford University Press, 2008). 49.

[77] Henry A. Crumpton, *Intelligence and Homeland Defense. In Transforming U.S. Intelligence*, edited by Jennifer E Sims and Burton Gerber, 198–219. Washington, D.C: Georgetown University Press, 2005, 206–207.

[78] U.S. Department of Homeland Security, *2011 National Network of Fusion Centers Final Report*, accessed June 7, 2013, http://www.dhs.gov/2011-fusion-center-assessment.

[79] Ibid.

The first COC-1 is *receive*; the ability to receive classified and unclassified information from federal partners.[80] The second COC-2 is *analyze*; the ability to assess local implications of threat information using a formal risk assessment process.[81] The third COC-3 is *disseminate*; the ability to further disseminate threat information to other state, local, tribal, and territorial entities within their jurisdictions.[82] And lastly, the fourth COC-4 is *gather*; the ability to gather locally generated information, aggregate it, analyze it, and share it with federal partners as appropriate.[83] The COCs 1 and 4 are viewed in context of the intelligence cycle process model pertaining to "collection" and places emphasis on the vertical flow of information among federal agencies and state, local, tribal, territorial, and private sector partners. As previously mentioned and reflected in Figure 1, the single common attribute within the various intelligence cycle models is the "collection" phase. Chapter III of this thesis offers noted historical and current challenges to executing domestic intelligence activities under the collection phase of the intelligence cycle process model, a continuing concern for privacy advocates. The COCs 2 and 3 are logical sequenced actions of the intelligence cycle process model that are utterly contingent on the National Network's ability to fully execute the complete intelligence cycle process.

External to the National Network, DHS in close partnership with state and local partners developed the Target Capabilities List for general public safety officials, excluding law enforcement. The TCL describes the preparedness capabilities related to the four homeland security mission areas: Prevent, Protect, Respond, and Recover. The TCL identified critical elements of the intelligence cycle process model involved with gathering [collection], analysis, production and dissemination that states and localities should possess in order to prevent, protect, respond and recover from a terrorist incident. It defines and provides the basis for assessing preparedness of which include information gathering (collection), intelligence analysis and production as elements of the Prevent

[80] U.S. Department of Homeland Security, *2011 National Network of Fusion Centers Final Report*, accessed June 7, 2013, http://www.dhs.gov/2011-fusion-center-assessment.

[81] Ibid., 14.

[82] Ibid., 17.

[83] Ibid., 19.

Mission Capabilities. In 2009, the Heritage Foundation,[84] which is a conservative think tank whose mission is to formulate and promote conservative public policy, emphasized the significance of state and local capabilities in understanding the threat environment reported in a article titled *Effective Counterterrorism: State and Local Capabilities Trump Federal Policy*.

B. DOMESTIC INTELLIGENCE POLICY

The 2002 Homeland Security Act established DHS I&A, which was later amended by the 2007 Implementing Recommendations of the 911 Commission Act that established the DHS I&A State and Local Program Office. Both pieces of legislation created an organization designed to address the issues of information sharing to protect the homeland and partnering with state, local, tribal, territorial and private sector elements to ensure not only horizontal and vertical information sharing but also to leverage the HSE as contributors to the national intelligence architecture. Effective information sharing and the expansion of USIC capabilities is intended serve a more comprehensive approach in supporting the national efforts to protect the U.S. from future terrorist attacks.

The 2004 Intelligence Reform and Terrorism Prevention Act (IRTPA), signed into law by President Bush made major amendments to the 1947 National Security Act and reintroduced the "…idea of a Director of National Intelligence (DNI) [that] dates to 1955 when a blue-ribbon study [was] commissioned by Congress. It was the attacks of September 11, however, that finally moved forward the longstanding call for major intelligence reform and the creation of a Director of National Intelligence."[85] As noted in Chapter II, EO 12333 sets forth the foundation of the USIC and the Administration's

[84] The Heritage Foundation, accessed June 7, 2013, http://www.heritage.org/about.

[85] Office of the Director of National Intelligence, accessed August 5, 2013, http://www.dni.gov/index.php/about/history.

directions regarding "timely and accurate information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons and their agents"[86] in support of national security.

An EO serves as an official document to manage the operations of the federal government.[87] However, when EO 13470 in 2008 amended EO 12333, it included language focused on the responsibility of state, local and tribal governments, as well as the private sector to support U.S. intelligence activities. In order to support state, local and tribal governments, as well as the private sector integration into the HSE and support U.S. intelligence activities, DHS I&A, as well as other federal and academic elements, began delivering intelligence cycle process model training to the National Network and HSE.

The single common attribute used by various USIC intelligence cycle models is the "collection" phase. Nonetheless, the intelligence collection phase under the intelligence cycle process model within the post-9/11 HSE is considered a gray area because information is often required or expected from activities that are not necessarily violations of law, yet the information may be collected for the purpose of predictive analytic assessments for law enforcement and homeland security professionals. In 1952, intelligence "collection" was defined as the procuring, assembling and organizing of information and served as the first step in the processing of intelligence information according to *The International Dictionary of Intelligence* published by author Leo D. Carl. Today, it is considered the third step or phase in the intelligence cycle and "officially defined as 'the exploitation of sources of information by collection agencies and delivery of information to the proper intelligence-processing unit for use in the production of intelligence.'"[88] The 1952 definition was geared toward intelligence collection targeted against communist nation-states of the former Soviet Union and not the domestic intelligence environment of today.

---

[86] U.S. National Archives, accessed July 27, 2013, www.archives.gov/federal-register/executive-orders/12333.html.

[87] Ibid.

[88] Leo D. Carl, *The International Dictionary of Intelligence* (McLean, VA. International Defense Consulting Service, 1990). 59.

The September 11 terrorist attacks raised serious concerns regarding the sufficiency of the USIC intelligence collection capabilities and facilitated state, local, tribal and private sector partner assimilation into the newly established homeland security enterprise. The nation began focusing its intelligence collection efforts in order to prevent future attacks through the development of multiple national strategies between the White House and the DNI with minimal attention to domestic intelligence collection. The White House produced the 2002 National Security Strategy, the 2007 National Strategy for Homeland Security, and the 2010 National Security Strategy of the United States, the 2011 National Counterterrorism Strategy, and most recently the 2012 National Strategy for Information Sharing and Safeguarding. The DNI produced the 2005 National Intelligence Strategy and the 2009 National Counterintelligence Strategy. The first National Homeland Security Strategy published by the Bush administration in 2002 documented "Homeland security is based on the principle of shared responsibility and partnership with "state and local governments, the private sector, and the American people."[89] However, within the 2002 national strategy, there is no specific mention of domestic intelligence collection,[90] which remains consistent among the other referenced strategies.

Executive Order (EO) 12333 provides guidance for U.S. intelligence activities among USIC members, but it lacks a specific doctrine or "how to" concerning domestic intelligence collection to prevent repeating the law enforcement and intelligence mishaps of the past. The lack of doctrine may accelerate intelligence mishaps given the explicit language of Part 1.4 of EO 12333 that integrates state, local, and tribal governments, as well as private sector entities.

> [T]he Intelligence Community shall collect and provide information in accordance with priorities set by the President concerning activities to protect against international terrorism, proliferation of weapons of mass destruction, intelligence activities directed against the United States, international criminal drug activities, and other hostile activities directed against the United States by foreign powers, organizations, persons, and

[89] Office of Homeland Security, *National Strategy for Homeland Security*, July 2002, 2.

[90] Jennifer E. Sims, and Burton Gerber, *Transforming U.S. Intelligence*. Washington, D.C., Georgetown University Press. 2005. 206.

> their agents as well as take into account information needs relating to national and homeland security provided by state, local, and tribal governments and private sector entities.[91]

The federal government concentrates its support to nontraditional intelligence collectors (state, local, and tribal governments, as well as private sector entities) via the National Network. The National Network is a far-reaching change from the USIC that existed originally as part of a massive response to the challenge from the Axis powers in World War II and charged with responding to the challenges associated with the spread of Communism and the military might of the Soviet Union.

Most fusion centers within the National Network are law enforcement centric and recently integrated the Intelligence-Led Policing (ILP) model as the standard intelligence business practice. The term "Intelligence-led Policing" was coined in Great Britain to focus on key criminal activities[92] and its general philosophy was adopted by IACP in the March 2002 Intelligence Summit.[93] Author and academic David Carter, stated the emergence of ILP significantly enhances the law enforcement intelligence function.[94] However, as law enforcement agencies wrestle with the understanding of their new role in collecting and analyzing intelligence in support of the national intelligence architecture while at the same time managing crime in their jurisdictions, some authors judge introduction of ILP in the U.S. has been problematic.[95] Few agencies engage in proper intelligence-led techniques and ILP cannot be implemented effectively, if officers and analysts are not trained in the intelligence cycle process model in order to prevent crime

---

[91] Executive Order 12333, *United States Intelligence Activities* (As amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008).

[92] U.S. Bureau of Justice Assistance, *Intelligence-Led Policing: The New Intelligence Architecture*, September 2005, 9.

[93] International Association of Chiefs of Police, *Criminal Intelligence Sharing: A National Plan for Intelligence-Led Policing at the Local, State and Federal Levels*. Alexandria, VA, 2002.

[94] David L. Carter, *The Law Enforcement Intelligence Function: State, Local, and Tribal Agencies*, accessed March 3, 2013, http://www.hsdl.org/?view&did=469588.

[95] Roger, G. Dunham, Geoffrey P. Alpert, Jennifer E. Davis, and Robert W. Taylor, *Intelligence-Led Policing and Fusion Centers, Critical Issues in Policing: Contemporary Readings*, 6th ed, Waveland Press, 2010, 232.

and terrorism.[96] According to the 2012 National Network of Fusion Centers Final Report, 100 percent of the National Network reported conducting or contributing to threat assessments, primarily focused on consequence, risk or vulnerability analysis[97] juxtapose proactively identifying threats supporting intelligence-led law enforcement activities necessary for preventing crime and terrorism. Purportedly, only 41 of 78 fusion centers (53.2 percent) contributed to national-level assessments, a statistic unchanged from the 2011 Assessment.

The International Association of Law Enforcement Intelligence Analyst (IALEIA), an organization established in 1980 to advance law enforcement intelligence analytic standards, defines ILP as "executive implementation of the intelligence cycle to support proactive decision making for resources allocation and crime prevention."[98] A consensus on the interpretation of the ILP philosophy between IACP and IALEIA has not been reached relative to standard employment of the intelligence cycle process model.

C. EXPLOITING DOMESTIC INTELLIGENCE AUTHORITIES – ABUSES

Expanding domestic intelligence capabilities initially began in the early part of the 20th century under President Theodore Roosevelt's administration.[99] Thirty-plus years prior to 9/11, challenges with domestic intelligence collection were uncovered during the 1970s Watergate, Rockefeller, Church, and Pike Investigations. The investigations involved overreach into U.S. domestic intelligence by the USIC and

[96] Roger, G. Dunham, Geoffrey P. Alpert, Jennifer E. Davis, and Robert W. Taylor, *Intelligence-Led Policing and Fusion Centers, Critical Issues in Policing: Contemporary Readings,* 6th ed. (Waveland Press, 2010), 243.

[97] U.S. Department of Homeland Security, *2012 National Network of Fusion Centers Final Report*, accessed October 8, 2013, http://www.dhs.gov/sites/default/files/publications/2012%20National%20Network%20of%20Fusion%20Centers%20Final%20Report.pdf, 15.

[98] Lisa M. Palmieri, *Challenges Facing law Enforcement Intelligence*, 316.

[99] Loch K. Johnson, and James J. Wirtz, *Intelligence and National Security: The Secret World of Spies-An Anthology*. Oxford, NY. Oxford University Press. 2008, 6.

improper domestic intelligence activities by the Law Enforcement Community.[100] However, September 11, 2001, once again initiated the demand for increased domestic intelligence collection.

Domestic intelligence abuses may be viewed from two perspectives, political and multicultural. During the 1970s, the main topic of interest underlying the perceived threat to U.S. social structures centered on preventing the spread of communism by addressing perceived Soviet Union influence of social issues. In the post-9/11 environment, the topic centers on identifying the terrorist threat residing within the U.S. from groups or individuals aligned with radical violent and extremist ideology.

D. USIC MEMBERS – FBI, CIA, AND DOD/NSA

Members of the USIC, most notably the FBI and the CIA, as well as local law enforcement, conducted improper domestic intelligence collection activities under two programs. The FBI Counterintelligence Program known as COINTELPRO is well known for its domestic intelligence collection overreaches. The Center for National Security Studies,[101] a civil liberties think-tank founded in 1974 to prevent violations of civil liberties in the U.S., published several articles on COINTELPRO. Another grim domestic intelligence overreach involved the CIA's Operation CHAOS.[102]

Seymour Hersh in the New York Times first exposed the CIA's domestic operations on December 22, 1974. As a result, President Ford established the Rockefeller Commission to look into the CIA's domestic intelligence activities. The Rockefeller Commission detailed the CIA's mail intercept program described a separate domestic spying program run by the CIA's Office of Security called Project Resistance and

[100] *The Intelligence Community in the 21st Century: Staff Study* - Permanent Select Committee on Intelligence House of Representatives 104th Congress, accessed March 5, 2013, http://www.gpo.gov/fdsys/pkg/GPO-IC21/html/GPO-IC21–13.html.

[101] The Center for National Security Studies serves as a watchdog in defense of civil liberties, human rights and constitutional limits on government power. Policymakers, opinion leaders and journalists regularly seek the Center's expertise on both substantive and strategic issues, accessed August 5, 2013, http://www.cnss.org/pages/mission.html.

[102] Verne Lyon, *Domestic Surveillance: The History of Operation CHAOS*, accessed March 5, 2013, http://www.serendipity.li/cia/lyon.html.

mentioned an Office of Security program that gave seminars and training on lock-picking and surveillance to a number of local police departments.

The CIA's Operation CHAOS was designed to infiltrate American student organizations opposed to the Vietnam War to determine if there were foreign links.[103] The CIA Operation CHAOS existed for 5 years beginning in 1967 and ending in 1972, according to the Rockefeller report that revealed a compilation of some 13,000 different files, including files on 7,200 American citizens. However, the numbers may be on the low side; Operation CHAOS was tightly compartmented within the CIA and free from periodic internal review. For example, later reports of the number of state, local, and county police departments assisted by the CIA were put at 44, which is far more than the handful mentioned in the Rockefeller report.

The problems of collection guidance were the subject of a number of special studies to include the CIA's Inspector General in 1966 (known as the Cunningham Report).[104] In wake of revelations that the CIA had violated its charter by spying on U.S. citizens, a series of congressional investigations concluded there were violations of the law, as well as discovery of much wider range of intelligence investigation abuses.[105]

During the same period as CIA's Operation CHAOS, the FBI's COINTELPRO levied intelligence requirements on the CIA to collect information on U.S. citizens traveling abroad.[106] The FBI, established in 1908, was initially designated primarily as a law enforcement agency. However, under President Roosevelt's administration and because of World War II, the FBI's responsibilities expanded to include centralizing the authority for domestic intelligence.[107] Although originally created to investigate specific federal crimes, the FBI expanded into the notorious Hoover-era domestic intelligence

[103] Loch K. Johnson, and James J. Wirtz, *Intelligence and National Security: The Secret World of Spies-An Anthology*. Oxford, NY. Oxford University Press. 2008, 368.

[104] Scott D. Breckenridge, *The CIA and the U.S. Intelligence System* (Boulder, CO.: Westview Press. 1986), 56.

[105] Mark M. Lowenthal, *Intelligence: From Secrets to Policy* (Washington, D.C.: CQ Press, 2003), 21.

[106] Scott D. Breckenridge, *The CIA and the U.S. Intelligence System* (Boulder, CO.: Westview Press, 1986), 201.

[107] Ibid., 112.

agency that was famous for excess and overreach. Revelations of Hoover-era abuses prompted the FBI to refocus for a time on crime solving and a season of robust oversight and operational limitations on intelligence gathering followed. These limits were set forth in an internal set of rules, known since their creation as the "Attorney General's Guidelines."[108] The organizational setback is still a concern with the American public and civil liberties organizations. Because of 9/11, the Attorney General's Guidelines have once again undergone changes and currently it is titled the *Domestic Intelligence Operations Guide*. Thus, while the FBI has conducted investigations for both law enforcement and intelligence purposes throughout its history, their intelligence-collection activities prompt the most frequent calls for reform.[109]

During combat operations in Vietnam, U.S. Army intelligence agents gathered information on anti-war activists in support of the potential use of federal troops in the case of civil disturbances or urban riots. When the U.S. Army's domestic intelligence program became public knowledge in 1970 the public and political backlash caused a sever reduction at the end of the Vietnam War at perceived abuses.[110] The NSA, a DoD element recently came under public scrutiny concerning domestic intelligence collection activities. In the wake of leaks by former NSA contractor Edward Snowden, U.S. officials have faced growing questions about the kinds of information they are collecting about Americans, at what scale and under what authority. Intelligence officials reported collection efforts are important counterterrorism measures. Similar to the current privacy concerns regarding domestic intelligence collection activities by the FBI and the National Network, NSA has ties to past domestic intelligence collection abuses. The NSA created Project MINARET in 1969 to spy on peace groups and black power organizations. Federal agencies requested NSA to survey international communications of certain U.S. citizens traveling to Cuba. Beginning in 1967, requesting agencies provided names of U.S. persons in an effort to determine foreign influence on civil disturbances occurring

[108] Emily Berman, *Domestic Intelligence: New Powers, New Risks*. Brennan Center for Justice at New York University School of Law. 2011, 5.

[109] Ibid., 7.

[110] Michael E. Bigelow, "A Short History of Army Intelligence." *Military Intelligence*, July-September 2012, 45.

throughout the Nation and later, the widespread national concern over criminal activity such as drug trafficking and acts of terrorism, both domestic and international.[111]

The activities were likely a result of the lack of specific legislative and organizational guidance or doctrine regarding domestic intelligence collection. The U.S. intelligence collection array was largely built to respond to the difficulties of penetrating the Soviet target.[112] However, as the literature review highlights, when the collection phase on the USIC intelligence cycle is directed to support domestic intelligence, it has proved to be a detriment to civil rights without sound doctrine.

E. LOCAL LAW ENFORCEMENT

As early as the 1920s, law enforcement intelligence units maintained "dossier" files on individuals thought to be involved in some form with criminal activity, and in the 1950s, such files were maintained on individuals due to their political expressions or their placement on the fringes of mainstream society. Because of these files, the U.S. Supreme Court under Chief Justice Earl Warren ruled state or local law enforcement might be subject to civil liability.

This ruling commonly referred to as the "1983 suits" relied on a provision of the 1871 Civil Rights Act, codified as U.S. Code Title 42, Section 1983 – Civil Action for Deprivation of Rights. In the 1960s and early 1970s, lawsuits under the "1983 suits" targeting police intelligence units provided an individual could hold state and local law enforcement departments and their officers liable for maintaining records on individuals with no evidence of a crime.[113] Given a history in the 1960s and 1970s in which police

[111] U.S. Senate, Select Committee to Study Governmental Operations with Respect to Intelligence Activities, Intelligence Activities – National Security Agency and Fourth Amendment Rights, October 29, 1975, accessed October 8, 2013, http://www.aarclibrary.org/publib/church/reports/vol5/pdf/ChurchV5_1_Allen.pdf.

[112] Mark M. Lowenthal, *Intelligence: From Secrets to Policy*. Washington, D.C.. CQ Press. 2012, 83.

[113] David L. Carter, *Law Enforcement Intelligence: A Guide for State, Local and Tribal law Enforcement Agencies*, 2nd ed, 2009, 33.

intelligence units all too often violated citizen groups' First Amendment rights, there was a widespread movement to dismantle such capabilities.[114]

The NCISP drafted by the Global Justice Information Sharing Initiative Intelligence Working Group served to provide a model for intelligence process principles and policies by law enforcement elements. A key element of the NCISP supports policies that will protect privacy and constitutional rights while not hindering the intelligence process. As an example, the NCISP states a "privacy policy should stress the need for and importance of planning and direction (the first stage of the intelligence process). Although it is only one phase of the intelligence cycle, planning and direction guides the overall activities of the criminal intelligence function."[115]

F. NATIONAL NETWORK OF FUSION CENTERS

The National Network is susceptible to encountering like challenges with executing domestic intelligence activities. In December 2007, the American Civil Liberties Union (ACLU) published an article titled *What's Wrong With Fusion Centers?*" in which authors Michael German, ACLU Senior Policy Counsel and former FBI Supervisory Special Agent and Jay Stanley, an ACLU Senior Policy Analyst claims there has not been adequate public discourse regarding the National Network establishment prior to opening a state or major urban area fusion center charged with collection and sharing of intelligence information, specifically about American citizens and other residents. The article emphasizes civil rights abuses of the past by federal and local law enforcement and intelligence organizations while concluding like actions could potentially occur again without the proper legislative oversight and adequate checks and balances to monitor their operations.

The ACLU provided examples of a number of troubling intelligence products produced by fusion centers that were leaked to the public, such as a Texas fusion center

[114] Timothy Connors, and John Rollins, Center for Policing Terrorism at the Manhattan Institute. *State Fusion Center Processes and Procedures: Best Practices and Recommendations*. Policing Terrorism Report, No. 2, September 2007, 3.

[115] U.S. Department of Justice, Global Justice Information Sharing Initiative, *National Criminal Intelligence Sharing Plan*, October 2003, 12.

that released an intelligence bulletin describing a purported conspiracy between Muslim civil rights organizations, lobbying groups, the Iraq anti-war movement, a former U.S. Congresswoman, the U.S. Treasury Department and hip hop bands to spread Sharia law in the U.S. A Virginia Fusion Center reportedly issued a terrorism threat assessment describing the state's universities and colleges as "nodes for radicalization" and characterized the "diversity" surrounding a Virginia military base and the state's "historically black" colleges as possible threats.[116]

G. DOMESTIC INTELLIGENCE - CULTURE

As a result of the September 11 terrorist attacks, the 2001 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act also known as the USA PATRIOT Act, allowed greater latitude in domestic intelligence/law enforcement collection activities.[117] The USA PATRIOT Act represents a decision on the part of the president and Congress that the nation expects its defenders to be proactive against terrorism of all kinds.[118] In support of the proactive nature to defend the nation, DHS I&A has the responsibility per Section 503 of the 9/11 Commission Act to develop training curricula on the intelligence cycle process model for state and local officials[119] via the National Network in an effort to predict emerging threats.

In order to fully execute the USIC intelligence cycle process model, information fusion as an immediate and long-term strategic capability must be continually built upon to perform carefully informed analysis and assessments of homeland security information. In order to achieve such a capability, government agencies and organizations must have timely and appropriate access to information that supports the "collection" phase of the intelligence cycle process model. This remains a challenge

[116] American Civil Liberties Union, accessed August 7, 2013, http://www.aclu.org/spy-files/more-about-fusion-centers.

[117] Mark M. Lowenthal, *Intelligence: From Secrets to Policy*. Washington, D.C., CQ Press. 2003, 23.

[118] Loch K. Johnson and James J. Wirtz, *Intelligence and National Security: The Secret World of Spies-An Anthology*. Oxford, NY. Oxford University Press. 2008, 369.

[119] U.S. Department of Homeland Security, *DHS' Role in State and Local Fusion Centers is Evolving*. Office of Inspector General Report – OIG-09–12. October 2008, 16.

within the HSIE, specifically DHS I&A, as reflected in the DOJ Opinion of 28 Code of Federal Regulations, Part 23 specifically pertaining to DHS I&A. The opinion revealed;

> It has been brought to [DOJ] attention that some elements of the law intelligence information (which may include 'law enforcement sensitive' information) with the Department of Homeland Security (DHS), based upon a concern that it is not a 'law enforcement activity.' DOJ has consistently advised that the term does not require that an agency have law enforcement or investigative authority in order to qualify under an intelligence project's 'need to know' and 'right to know' criteria. Based on the description above, it appears that DHS, in performing its function of gathering information needed to protect the nation from foreign or domestic terrorist activity, is engaged in a 'law enforcement activity' and accordingly may be given access to criminal intelligence information that may be needed to properly carry out that function.[120]

The challenges with fusing information have been identified within HSIE as well as the HSE. The 2007 National Strategy for Homeland Security reported under the heading *Challenges in Homeland Security and Beyond* "although we have substantially improved our cooperation and partnership among all levels of government, private and nonprofit sectors, communities, and individual citizens, we must continue to strengthen efforts to achieve full unity of effort through a stronger and further integrated national approach to homeland security. Our information sharing capabilities have improved significantly, but substantial obstacles remain. We must continue to break down information barriers among federal, state, local and tribal partners and the private sector."[121]

In early August 2010, President Obama signed EO 13549 titled *Classified National Security Information Programs for State, Local, Tribal, and Private Sector (SLTPS) Entities*. This represented a significant step forward to facilitate classified intelligence and homeland security-related information sharing with SLTPS partners; to include putting in place a governance and oversight structure that would serve to ensure the uniform application of security standards within the executive branch and SLTPS

[120] U.S. Department of Justice Memorandum, *28 Code of Federal Regulations, Part 23*, March 31, 2005.

[121] The White House, *National Strategy for Homeland Security*, Washington: The White House, October 2007.

communities while maintaining consistency with existing policy and standards. This action now allowed classified information originating outside of DHS, and not otherwise covered by specific memorandum of understandings, to be disseminated by DHS to appropriately cleared nonfederal recipients in the National Network.

However, the policy and associated information sharing strategies often set forth by Washington are not readily accepted as they promulgate outside Washington, DC. In a professional environment, the writer observed and experienced unsuccessful intelligence and information sharing between SLTPS nontraditional intelligence recipients and federal HSIE and USIC entities because of differing organizational cultures. Due to the typical law enforcement culture and "lead-agency" law enforcement concept, the sharing of information with nontraditional law enforcement partners and the private sector remains a challenge. The October 2010 DHS Office of Inspector General Report emphasized this premise when it reported, "despite the overall improvements, DHS continues to face several information sharing challenges. Specifically, DHS component collaboration in the information sharing process needs improvement. In addition, unfinished intelligence products have not always been timely, and the production process for finished intelligence products should allow for more fusion center collaboration."[122]

The intelligence cycle process model collection phase depends on effective information sharing in order to produce value-added finished intelligence products for HSE policy and decision makers. With the expansion of USIC capabilities via SLTPS partners in support of the national intelligence effort, it is difficult to evaluate its effectiveness of the intelligence cycle process model in context of the lack of consistent intelligence cycle training and employment. Ms. Lisa Palmieri, a current DHS I&A Senior Intelligence Officer and former President of the International Association of Law Enforcement Intelligence Analysts, suggests the analysis phase of the intelligence cycle process model is problematic given the confusion between the terms intelligence and information among law enforcement officials as well as "…agencies employment of so-

[122] U.S. Department of Homeland Security, *Information Sharing with Fusion Centers Has Improved, but Information System Challenges Remain*, Office of Inspector General Report 11–04, October 2010.

called analysts who were either unaware of or untrained in analysis and who were merely collecting and disseminating raw data."[123]

Mr. Matt Mayer, counselor to the Secretary and Acting Executive Director for the Office of Grants and Training in DHS, visiting fellow at The Heritage Foundation, and President of the Buckeye Institute for Public Policy Solutions in Columbus, Ohio and Mr. Scott Erickson, who has studied and written on the proliferation of homegrown terrorism and the response by domestic law enforcement have specifically addressed the need for reform within the law enforcement culture in order to properly support their new counterterrorism role. Both assert that "uniformity of training must be a central aspect of any comprehensive shift in the domestic law enforcement culture" and "maintaining a mixed counterterrorism training regime [that includes the application of intelligence analysis] across the nation's 18,000 law enforcement agencies will inhibit the adoption of consistent and uniform standards for counterterrorism recognition and awareness." Symmetrical and uniform training standards would benefit the broader law enforcement community, as well as the public at large, by ensuring a consistent understanding of the threat of terrorism.[124]

[123] Lisa M. Palmieri, International Association of Chiefs of Police, "Information Vs. Intelligence: What Police Executives Need to Know," *The Police Chief*, vol. 72, no. 6, Alexandria, VA, June 2005.

[124] Matt A. Mayer, and Scott G. Erickson, *Changing Today's Law Enforcement Culture to Face 21st-Century Threats*. The Heritage Foundation. June 23, 2011.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. INTELLIGENCE CYCLE PROCESS MODEL CASE STUDY – BOSTON MARATHON BOMBING

> No one can comprehend what goes on under the sun. Despite all their efforts to search it out, no one can discover its meaning. Even if the wise claim they know, they cannot really comprehend it. Ecclesiastes 8:17

A. INTRODUCTION

In an evaluation of performance metrics known as COCs for the National Network, the TCL for non-law enforcement elements, such as emergency managers, and the MCCCIE for the law enforcement community, this thesis intends to ascertain adherence to the intelligence cycle process model. To better understand the intelligence cycle process model's general effectiveness, the thesis examines existing public data made available to the author of the 2013 Boston Marathon bombing with respect to the National Network and HSE. Information made available regarding the 2013 Boston Marathon bombing will attempt to illuminate whether the National Network or the HSE adhered to the intelligence cycle process model in order to forecast or prevent the terrorist act.

The Boston Marathon bombing once again raised similar questions that surfaced after the September 11, 2001 terrorist attacks regarding law enforcement officials and intelligence analysts' ability to identify a potential terrorist attack. The Boston Marathon bombing serves as a platform to discuss the effective employment of the intelligence cycle process model by the National Network, and why it did not prevent the Boston bombing. This associated case study is intended to underscore key issues associated with employing the intelligence cycle process model at the state and local level by demonstrating its effectiveness prior to, during, and after the April 15, 2013, Boston Marathon bombing as an appropriate HSE intelligence process model. It is not focused on identifying possible solutions and providing potential courses of action. The case study framework and lessons learned from the Boston Marathon bombing may be useful to HSE agencies in developing and supporting intelligence processes suitable for the National Network. The information sources gathered for this case study were acquired

from public discussion of the issue in Congress, court documents, the press media and statements of senior state and local officials.

This case study uses the April 15, 2013, Boston Marathon bombing in the context of the intelligence cycle process model adherence necessary to detect the threat and provide intelligence to policy and decision makers with information in order to prevent the bombing. Additionally, the case study highlights the challenges with implementing the intelligence cycle process model within the National Network while ensuring security and safety from both domestic and international terrorism. Literature has highlighted the challenges with the intelligence cycle process model within the U.S. intelligence community, as well as the HSIE and HSE, and how difficult it is to lead a successful intelligence process to the point that a value-added intelligence product is produced with sufficient content and consensus to be useful to the organizations tasked to develop it. This is especially true in a National Network that lack the mature culture and uniform repeatable processes generally employed by organizations like those that comprise the 17-member USIC. Nonetheless, intelligence as an entity, process, and product within the HSE has the critical mission of preventing future terrorist attacks.

Using the intelligence cycle process model domestically to support the HSE in an attempt to think ahead and to understand what is going to happen in the future has reopened old wounds associated with abuse of power by law enforcement and intelligence entities. Instead of having to focus on domestic intelligence collection in an effort to identify state actors of foreign intelligence and security services as a result of Cold War labors, it is now necessary that intelligence collection must expand beyond the traditional USIC members in order to defeat terrorism and transnational criminal organization threats in a post-9/11 environment.

The National Network was another safeguard developed across the country since 9/11 to support the national intelligence architecture and prevent future terrorist attacks. They were expressly created to make sure law-enforcement agencies shared terrorist-related information developed by federal, state, and local law enforcement agencies. “It highlights a concern that we have and the need for agencies to share data on the subjects that they are investigating,” said Mike Sena, president of the National Fusion Center

Association.[125] DHS estimates it has pumped $1.4 billion into state and local fusion centers in their effort to support the National Network and assist with sharing intelligence and treat information necessary to prevent terror attacks across the country.[126]

The implementation of the intelligence cycle process model within the USIC, HSIE and HSE in order to determine its effectiveness has received mixed reviews. Given these interpretations, the Boston Marathon bombing will be used to assess the effectiveness of a six-step intelligence cycle process that embraces *Intelligence Analysis: A Target-Centric Approach* published in 2004 by author Robert M. Clark: 1) Requirements, needs, 2) Planning, direction, 3) Collection, 4) Processing, 5) Analysis, and 6) Dissemination.[127]

B. SCENARIO

On April 15, 2013, at 2:49 p.m. Eastern Standard Time, two pressure cooker bombs exploded during the Boston Marathon killing three people and injuring 264 others.

The suspects were identified later that day as Dzhokar and Tamerlan Tsarnaev.[128] Tamerlan Tsarnaev was subsequently killed by law enforcement, but Dzhokhar Tsarnaev while injured was able to escape. On April 19, 2013, during an unprecedented manhunt by thousands of law enforcement officers, Dzhokhar Tsarnaev was later captured and arrested.

C. PHASE 1 – REQUIREMENTS/NEEDS

The beginning of the intelligence cycle process model is identifying information needs/requirements from a defined customer base with the intent of providing the right

---

[125] Boston Globe, *FBI Did not Alert State's Anti-terror Unit to its Probe of Suspected Bomber in 2011*, accessed June 10, 2013, http://www.boston.com/politicalintelligence/2013/04/25/fbi-did-not-alert-state-anti-terror-unit-its-probe-suspected-bomber/RLHZM6GHRotZ6ciIYxmiKP/story.html.

[126] The Boston Channel, *Effectiveness of Fusion Centers Questioned*, accessed June 20, 2013, http://www.wcvb.com/news/investigative/effectiveness-of-fusion-centers-questioned/-/12520878/20358362/-/bkveudz/-/index.html#ixzz2aHaeHk5x.

[127] Robert M. Clark, *Intelligence Analysis: A Target-Centric Approach*. Washington, D.C., CQ Press. 2004, 14.

[128] U.S. District Court for the District of Massachusetts, Criminal Complaint, *USA v. Dzhokar Tsarnev*, Case No. 13–2106-MBB, April 21, 2013.

intelligence product to the right end user to prevent future terrorist attacks. Homeland Security Standing Information Needs (HSEC SINs) form the foundation for information collection activities within the National Network to focus their collection, analytic, and reporting assets in support of the homeland security mission.[129]

There existed HSEC SINs made available to the National Network and the HSIE to identify and document information needs designed to prevent the Boston Marathon bombing. Additionally, in 2004 DHS issued a warning regarding explosive devices hidden in pressure cookers.[130] Likewise, according to a July 2007 National Intelligence Estimate entitled *The Terrorist Threat to the U.S. Homeland* an attack like the Boston bombing has been a concern for the U.S. government for years.[131] The DHS warning indicated pressure cooker bombs was as "a technique commonly taught in Afghan terrorist training camps."[132]

The Boston Regional Intelligence Center and the Commonwealth Fusion Center in Maynard,[133] which were designed to serve as clearinghouses for information about potential threats, were unaware that the FBI interviewed Tsarnaev as part of a three-month investigation after Russian agents alerted U.S. officials to his increasing radicalization, officials said.[134] Nor was information about Tsarnaev shared at the quarterly meetings the FBI had with local law enforcement leaders because according to

[129] U.S. Department of Homeland Security, accessed June 10, 2013, http://www.dhs.gov/more-about-office-intelligence-and-analysis-mission.

[130] CNN, *Boston Marathon Terror Attack Fast Facts*, accessed August 14, 2013, http://www.cnn.com/2013/06/03/us/boston-marathon-terror-attack-fast-facts.

[131] Statement for the Record Senator Joe Lieberman (Ret) House Committee on Homeland Security, *The Boston Bombings: A First Look*, accessed July 27, 2013, http://docs.house.gov/meetings/HM/HM00/20130509/100785/HHRG-113-HM00-Wstate-SchwartzK-20130509.pdf.

[132] Newsdesk, *Israel Homeland Security*, "A "Pressure Cooker" Warning was Given a Few Times in Recent Years," accessed April 21, 2013, http://i-hls.com/2013/04/a-pressure-cooker-warning-was-given-in-2004/.

[133] The Boston Regional Intelligence Center and the Commonwealth Fusion Center of Maynard are elements of the National Network of Fusion Centers (National Network).

[134] Boston Globe, *FBI did not alert state's anti-terror unit to its probe of suspected bomber in 2011*, accessed June 10, 2013, http://www.boston.com/politicalintelligence/2013/04/25/fbi-did-not-alert-state-anti-terror-unit-its-probe-suspected-bomber/RLHZM6GHRotZ6ciIYxmiKP/story.html.

the FBI, it did not rise to a specific level of concern.[135] "We were not privy to the tip,'' said David Procopio, the spokesman for the Massachusetts State Police, which oversees the Fusion Center, "They didn't share that information with us."[136]

The numbers of HSE nontraditional intelligence recipients are vast, including the 78 fusion centers that make up the National Network. Due to the enormous number of executives charged with establishing and implementing intelligence policy, two challenges are immediately discovered; who determines the requirement to have access to intelligence and information together with identifying who shoulders the responsibility of approving and establishing the priorities for satisfying documented intelligence needs. The National Network is unlike the USIC that can be task members to collect, analyze and produce national intelligence products by Intelligence Community Directives and Intelligence Community Policy Guidance.

Within Phase 1 of the intelligence cycle process model, it appears clear that the DHS HSEC SINs provided the necessary information needs (requirements) to the National Network in an effort to focus their assets on reporting potential terrorist activity in support of the homeland security mission. Nevertheless, the National Network does not have an executive body capable of issuing directives to state and local owned fusion centers that serve their respective jurisdictions.

D. PHASE 2 – PLANNING/DIRECTION

In an April 2009 statement by John E. Bateman, Assistant Commander, Texas Department of Public Safety to the Committee on House Homeland Security Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment, he commented that the National Network was designed to be a network of multi-agency intelligence centers, sharing and analyzing information, and then passing that information on to decision makers and first line personnel in the field, allowing these groups to make

[135] The Boston Channel, *Effectiveness of Fusion Centers Questioned*, accessed June 20, 2013, http://www.wcvb.com/news/investigative/effectiveness-of-fusion-centers-questioned/-/12520878/20358362/-/bkveudz/-/index.html#ixzz2aHaeHk5x.

[136] Boston Globe, *FBI Did Not Alert State's Anti-terror Unit to its Probe of Suspected Bomber in 2011*, accessed June 10, 2013, http://www.boston.com/politicalintelligence/2013/04/25/fbi-did-not-alert-state-anti-terror-unit-its-probe-suspected-bomber/RLHZM6GHRotZ6ciIYxmiKP/story.html.

better, more informed decisions as they work to thwart the individuals and groups intended to harm the U.S. While there have been, in the past, multi-agency taskforce operations on the enforcement side designed to address problems relating to crime and terrorism, the National Network is the first true comprehensive nationwide program to combine the analytical and informational capabilities of federal, state, county, local, and tribal agencies.[137]

The planning/direction phase of the intelligence cycle process model at the federal level is generally administered by the DNI and the respective USIC organization. However, within the National Network, there does not exist a centralized element to oversee the administration of this process. Although there existed HSEC SINs focused on preventing terrorist attacks, Senator Joseph Lieberman asked, "did the FBI enlist the help of state and local law enforcement, either on or off the JTTF to continue to watch the brothers, engage with their friends, associates and community leaders or monitor their Internet activities – including Tamerlan Tsarnaev's YouTube account, which openly recommended a collection of jihadist videos – for the purpose of assessing if either or both of the brothers were radicalizing"? Senator Lieberman commented the FBI does not have the resources or personnel to monitor all potential terrorist threats in this country and must rely on state and local law enforcement.[138]

The cultural and legal barriers to effective partnerships among national intelligence elements and the National Network prevent effective planning/direction within the HSE and the new national intelligence structure. The final report of the National Commission on Terrorist Attacks Upon the United States (9/11 Commission) described many instances in which, in the period leading up to September 11, 2001 potentially useful information was available but no one knew to ask for it, information was distributed only in compartmented channels, or information was requested but

[137] *CQ Homeland Security*, "Fusion Center Hearing," accessed August 22, 2012, http://homeland.cq.com/hs/.

[138] Statement for the Record Senator Joe Lieberman (Ret) House Committee on Homeland Security, *The Boston Bombings: A First Look*, accessed July 27, 2013,, http://docs.house.gov/meetings/HM/HM00/20130509/100785/HHRG-113-HM00-Wstate-SchwartzK-20130509.pdf, 2013.

withheld on the basis of a determination that it could not be shared. Twelve years later, Congressional House and Senate members have identified similar challenges remain with threat notification, access to information, and database management of information that may have contributed the 2013 Boston Marathon bombing.

E. PHASE 3 – COLLECTION

The National Strategy for Homeland Security supports the collection of information resulting in actionable intelligence for law enforcement agencies to prevent terrorist attacks. The collection of this information combines state and local criminal intelligence and national intelligence. Historically, domestic intelligence collection is viewed as problematic for law enforcement criminal intelligence when American law enforcement agencies have three primary roles: 1) Solving crimes committed in the past, 2) Preventing crimes that are imminent, and 3) Collecting criminal intelligence to stop future crimes.

Law enforcement criminal intelligence collection is guided by 28 CFR Part 23. 28 CFR Part 23 requires the collection and maintenance of criminal intelligence information concerning an individual, only if there is reasonable suspicion or criminal predicate that the individual is involved in criminal conduct or activity, and only if the information is relevant to that criminal conduct or activity. Because the "reasonable suspicion or criminal predicate" thresholds may be both conjectural and subjective in nature, criminal intelligence information cannot be accessed by criminal suspects to verify that the information is accurate and complete. The protections and limitations set forth in 28 CFR Part 23 are necessary to protect the privacy interests of the subjects and potential subjects of a criminal intelligence system.[139]

The FBI said it took a number of investigative steps to check on the request, including looking at his travel history, checking databases for derogatory information and searching for Web postings. Agents also interviewed Tsarnaev's family members, the

[139] Institute for Intergovernmental Research, *Criminal Intelligence Systems Operating Policies (28 CFR Part 23) Training and Technical Assistance Program*, accessed July 27, 2013, http://www.iir.com/WhatWeDo/Criminal_Justice_Training/28CFR/.

FBI said, but did not detect terrorist activity.[140] Richard Falkenrath, an adjunct Senior Fellow for Counterterrorism and Homeland Security, claim the U.S. authorities support broadminded foreign intelligence-gathering techniques abroad while, "we're instead reliant on more restricted domestic intelligence techniques to identify terrorist before they attack."[141]

Although the FBI and CIA as USIC members conducted a collection of information to determine the threat, a spokeswoman for the Boston Police Department said the Boston Regional Intelligence Center also was never notified about the FBI investigation[142] that may have resulted in the ability to leverage state and local unique capabilities to collect valuable data. In the FBI's final analysis, it concluded there was little it could have done to prevent the Boston Marathon bombing due to constraints provided in federal law and Justice Department protocols.[143] Although federal-level protocols disallowed the FBI from further inquiry, the National Network was also prevented from serving as a force-multiplier in an effort to collect as much information as possible in determining the threat.

While collection is the common variable among various intelligence cycle process models, it is also the most challenging to accomplish given the history of domestic intelligence collection activities by federal agencies and local law enforcement. Within the National Network, collection is implied to address "all-threats," but state and local organizational policies are generally unclear on what information is to be collected and what collection techniques is to be used, notwithstanding explicit statements to protect privacy, civil liberties, and civil rights.

---

[140] CNN, *FBI Agent Interviewed Bombing Suspect in 2011*, accessed April 21, 2013, http://www.cnn.com/2013/04/19/us/boston-suspects-no-links/index.html.

[141] Council on Foreign Relations, *Domestic Intelligence and the Boston Bombings*, accessed August 7, 2013, http://www.cfr.org/counterterrorism/domestic-intelligence-boston-bombings/p30557.

[142] Boston Globe, *FBI Did Not Alert State's Anti-terror Unit to Its Probe of Suspected Bomber in 2011*, accessed June 10, 2013, http://www.boston.com/politicalintelligence/2013/04/25/fbi-did-not-alert-state-anti-terror-unit-its-probe-suspected-bomber/RLHZM6GHRotZ6ciIYxmiKP/story.html.

[143] New York Times, *FBI Said to Find It Could Not Have Averted Boston Attack*, accessed August 6, 2013, http://www.nytimes.com/2013/08/02/us/fbi-said-to-conclude-it-could-not-have-averted-boston-attack.html?_r=0.

F. PHASE 4 – PROCESSING

The processing of information associated with the Boston Marathon bombing in the context of the intelligence cycle process model proved ineffective because of information sharing challenges and data overload. A FBI Supervisory Agent provided an emailed statement suggesting that state and local officials had ample access to information about the Tsarnaev investigation in 2011, through their participation on the FBI Boston JTTF[144] that include detectives and detective supervisors from the Boston Regional Intelligence Center. Additionally, the Boston Police Department maintains a close and ongoing working relationship with both the FBI and DHS through the intelligence personnel both agencies have assigned to work within the fusion center.[145] While fusion center (National Network) personnel are employed on the FBI Boston JTTF, what has surfaced is that the information was compartmentalized to a point it provided a barrier and prevented a timely notification of potential threat information and intelligence to senior state and local decision makers.

An added challenge to processing information for determining an intelligence value is data overload. Richard DesLauriers, head of FBI Boston stated the FBI's assessment of Tsarnaev was "…one of about 1,000 such assessments conducted by the Boston task force…"[146] leading up to the Boston Marathon bombing. In relation to the processing of information associated with the Boston Marathon bombing, congressional members evoke many of the same themes associated with September 11, 2001. Representative Michael McCaul, Chairman of the House Homeland Security Committee, declared "My fear is that the Boston bombers may have succeeded because our system

[144] Boston Globe, *FBI Did Not Alert State's Anti-terror Unit to Its Probe of Suspected Bomber in 2011*, accessed June 10, 2013, http://www.boston.com/politicalintelligence/2013/04/25/fbi-did-not-alert-state-anti-terror-unit-its-probe-suspected-bomber/RLHZM6GHRotZ6ciIYxmiKP/story.html.

[145] *Congressional Testimony of Boston Police Commissioner Edward F. Davis, III before the House Committee on Homeland Security*, accessed July 27, 2013, http://docs.house.gov/meetings/HM/HM00/20130509/100785/HHRG-113-HM00-Wstate-SchwartzK-20130509.pdf, 2013.

[146] Wall Street Journal, *Boston Hearings Delve into FBI Alerts*, accessed August 14, 2013, https://www.online.wsj.com/article.

failed,"[147] and Representative Bernie Thompson announced "We cannot ignore that once again it has taken a tragedy to reveal problems in our vast, varied and numerous federal databases."[148]

G. PHASE 5 – ANALYSIS

Analysis in many respects is as difficult to attain as the collection aspect. One critical challenge is the intergroup dynamics between law enforcement investigators and intelligence analysts. Ms. Lisa Palmeiri, noted law enforcement is undergoing a real transformation and recognizing that intelligence is different from simple information as police executives have recognized only a clear comprehension of the analytic process will support public safety officials in protecting the nation.[149] Boston's Commissioner Edward Davis stated his detectives may have concluded the same findings as the FBI in that there was no information (back then) that would have caused further investigation of the Tsarnaev's.[150] What is not stressed in both the FBI findings and the Boston Commissioner's statement is the skill-set and analytic tradecraft employed by supporting analysts. This issue is compounded when dealing with the associated challenges of intelligence management, as well as interagency intelligence collaboration. As an example, how do you effectively balance the demands of current real-time crime intelligence needs and the competing demands for longer-range predictive analysis?

A 2011 The Homeland Security Policy Institute's Counterterrorism Intelligence Survey Research report, indicated 62 percent of the intelligence chiefs representing major metropolitan police departments in the U.S. believed the "national [federal] intelligence enterprise was such that it left them unable to develop a complete understanding of their

[147] Wall Street Journal, *Boston Hearings Delve into FBI Alerts*, accessed August 14, 2013, https://www.online.wsj.com/article.

[148] Ibid.

[149] Lisa M. Palmieri, International Association of Chiefs of Police, "Information Vs. Intelligence: What Police Executives Need to Know," *The Police Chief*, vol. 72, no. 6, Alexandria, VA, June 2005.

[150] Wall Street Journal, *Boston Hearings Delve into FBI Alerts*, accessed August 14, 2013, https://www.online.wsj.com/article.

local threat environment."[151] Likewise, in the September 2011 Intelligence and National Security Alliance publication, experts agree that many federal intelligence and law enforcement professionals do not recognize the homeland security implications and intricacies of criminal information.[152]

Without the information possessed by FBI Boston, the Boston Regional Intelligence Center analysts were never in a position to help federal authorities connect the dots on a potentially dangerous person. They could not evaluate the relevance of Tsarnaev's six-month trip to Russia in 2012; assess whether his potentially extremist views may have further hardened after he returned to his home in Cambridge; or decide whether authorities needed to interview him again.[153]

In hindsight to the Boston Marathon bombings, the DNI as part of a full interagency review ordered a review and assessment now under way by the U.S. intelligence and law enforcement community. The initial intelligence review had focused largely on regional militant connections the men had in Russia or Central Asia. Initially, before the FBI identified the men, the review was looking at any indications of a threat emerging from overseas against the U.S. Once the identities of the men became known, with their possible ethnic Chechen background, the focus shifted. The USIC is tasked under the review with checking any intelligence gathered overseas while the FBI will focus on what is known inside the United States.[154] As part of the great HSE, the National Network has not been revealed as an element of the review, or the significant role it may have played in preventing the bombing.

---

[151] Frank J. Cilluffo, Joseph R. Clark, and Michael P. Downing, *Counterterrorism Intelligence: Law Enforcement Perspectives*. Counterterrorism Intelligence Survey Research. Homeland Security Policy Institute. George Washington University. September 2011.

[152] Intelligence and National Security Alliance, White paper, *Intelligence to Protect the Homeland: Taking Stock Ten Years Later and Looking Ahead*. Arlington: Homeland Security Intelligence Council, 2011.

[153] Boston Globe, *FBI did not alert state's anti-terror unit to its probe of suspected bomber in 2011*, accessed June 10, 2013, http://www.boston.com/politicalintelligence/2013/04/25/fbi-did-not-alert-state-anti-terror-unit-its-probe-suspected-bomber/RLHZM6GHRotZ6ciIYxmiKP/story.html.

[154] CNN, *FBI Agents Interviewed Bombing Suspect in 2011*, accessed April 21, 2013, http://www.cnn.com/2013/04/19/us/boston-suspects-no-links/index.html.

H. PHASE 6 – DISSEMINATION

The dissemination of a possible intelligence product may have centered on the differences in the understanding of what was identified as "intelligence" necessary for sharing information associated with the Boston Marathon bombing. The general inclination among law enforcement practitioners is that intelligence is information that leads to successful law enforcement activities. Within this context, the FBI Boston JTTF may have arrived at the conclusion there was no need to share information regarding the bombers. The USIC however, describes intelligence as information that has undergone a formal process, typically using a variation of the intelligence cycle process model. According to a U.S. official familiar with intelligence information on the Boston Marathon bombings, initial indications were that the two suspects do not have direct links to any major al Qaeda group or affiliates, or to a new significant terrorist threat to the U.S.[155] Equally within the context of statement of the U.S. official, the intelligence information referenced was not provided to the National Network, specifically the Boston Regional Intelligence Center.

The National Network, specifically the Boston Regional Intelligence Center, was not in a position to publish an intelligence product identifying concerns and issuing a warning regarding explosive devices hidden in pressure cookers. There is no available public literature or empirical data supporting the use of the intelligence cycle process model associated with information processing was used in respect to producing indications, watch and warnings intelligence in an effort to prevent the Boston Marathon bombing. The issues associated with the adherence of the intelligence cycle process model underscore the challenges that remain within the National Network relative to the effectiveness of the intelligence cycle process model.

I. CONCLUSION

The writer's analysis of the 2013 Boston Marathon bombing offers the National Network nor the HSE adhered entirely to the intelligence cycle process model in order to

[155] CNN, *FBI Agents Interviewed Bombing Suspect in 2011*, accessed April 21, 2013, http://www.cnn.com/2013/04/19/us/boston-suspects-no-links/index.html.

forecast or prevent the terrorist act. This type of event was forecasted nine years earlier in 2004 when DHS issued a issued a warning regarding explosive devices hidden in pressure cookers, also there existed HSEC SINs to identify and document relevant information needs. In addition, a National Intelligence Estimate entitled *The Terrorist Threat to the U.S. Homeland* was issued in July 2007 designating an attack like the Boston bombing was a concern for the U.S. government.[156]

The writer identified several key issues underscored in the April 15, 2013, Boston Marathon bombing associated with employing the intelligence cycle process model at the state and local level as an appropriate HSE intelligence cycle process model. Adherence to the intelligence cycle process model revealed its ineffectiveness due to delays in access to relevant information between the FBI and local law enforcement. Recognizing that successful counterterrorism efforts require effective information sharing, Section 1016 of the 2004 IRTPA (Public Law 108–458), building on the August 27, 2004, EO 13356, "*Strengthening the Sharing of Terrorism Information to Protect Americans*," required the creation of the Information Sharing Environment (ISE) for terrorism information. What also emerges is the challenge of identifying and prioritizing to whom and what information is to be shared by agencies within the HSE that supports the requirements/needs process.

The 9/11 Commission Report that described instances leading up to September 11, 2001, clearly reflected that potentially useful information was available, but no one knew to ask for it; information was distributed only in compartmented channels, or information was requested but withheld on the basis of a determination that it could not be shared. Each challenge is linked to effective adherence of the intelligence cycle process model, specifically planning and direction (Phase 2), collection (Phase 3), processing (Phase 4) and analysis (Phase 5) within the National Network and in this case similar to the Boston Marathon bombing. This exposes the continued need to address the

[156] Statement for the Record Senator Joe Lieberman (Ret) House Committee on Homeland Security, *The Boston Bombings: A First Look*, accessed July 27, 2013, http://docs.house.gov/meetings/HM/HM00/20130509/100785/HHRG-113-HM00-Wstate-SchwartzK-20130509.pdf.

ISE designed to support sharing and access to terrorism information, including information from the intelligence, law enforcement, military, homeland security, and other communities.

Individual departments and agencies have their own policies and procedures for information sharing, but there is no single government-wide agreement on what constitutes appropriate information sharing. Different standards exist among agencies (and even within agencies) for the designation and dissemination of terrorism information, resulting in different views on who requires the information and when and how the information is needed and processed. Because information protection standards vary, decisions on reconciling the need to protect information and the need to share information have been inconsistent and have contributed to the creation of cultures that support information segregation. A fundamental change must occur so that, in the dynamic setting of the new ISE, the right information is available to the right people at the right time.[157]

Consistent with the work of the Information Systems Council under Section 5 of EO 13356, one of the ISE's goals is to remove technology as a barrier to improved information sharing. For the most part, the technology needed to improve interoperability and information sharing is available today; and it should be an enabler rather than a barrier. While it is true that users face a vast and confusing array of systems, databases, networks and tools, in most cases this vast and confusing array is caused not by technological barriers, but by the policies, protocols, and sometimes security and legal concerns that prevent us from connecting the systems and sharing information in an optimal way.[158]

An area that remains to be developed is an appropriate identity-based screening system, to include biometrics and an improved visa threat analysis system. Law enforcement agencies have had to rely more on traditional investigative techniques to

[157] Office of the Director of National Intelligence, *Preliminary Report on the Creation of the Information Sharing Environment*, accessed August 8, 2011, http://www.ise.gov/sites/default/files/preliminaryreport.pdf.

[158] Ibid.

detect terrorist travel concerns, which resulted in the arrest of two U.S. citizens in New York after allegations they planned to travel to Somalia to join al-Shabaab.[159] The lack of a direct mechanism to share terrorism-related information between law enforcement agencies, along with the sheer amount of data that a JTTF in a major city has to sort through, are two issues that should be addressed in light of these attacks.

[159] Stephanie Hanson, *Al-Shabaab*, August 10, 2011, accessed August 24, 2011, http://www.cfr.org/somalia/al-shabaab/p18650.

THIS PAGE INTENTIONALLY LEFT BLANK

V. INTELLIGENCE CYCLE PROCESS MODEL AND THE HOMELAND SECURITY ENTERPRISE

A. HOMELAND SECURITY ENTERPRISE AND EMPLOYING THE INTELLIGENCE CYCLE PROCESS MODEL

Intelligence can no longer be defined in the context of ascertaining the capabilities and intentions of other nation-states abroad while systemically providing access to such intelligence to only an elite community of federal level intelligence analyst and collectors. The 9/11 terrorist attacks brought the intelligence function and the associated intelligence cycle process model to the forefront of the HSE. The post-9/11 HSE requires an intelligence cycle process model with the capability to operationalize intelligence gaps necessary for preventing terrorist acts from international terrorist groups operating abroad and within U.S. borders, domestic terrorist groups and homegrown violent extremists. It also requires providing timely results of intelligence cycle process model information (intelligence) to federal, state, and local customers. It is essential that officials responsible for the various aspects of homeland security fully realize the robust capacity of the national intelligence architecture. The U.S. government has the responsibility to dutifully and deliberately consider the Nation's approach and actions given the complexity and uniqueness of operating within the domestic intelligence realm.[160]

In order to maximize the capabilities of the HSE, the intelligence cycle process should address both a dynamic "top-down" and "bottom-up" approach as a contributor to the national intelligence architecture. The USIC traditional intelligence cycle process model is a "top-down" approach that was originally constructed to addresses military and national policy maker information needs. National policymakers requested information and assessments concerning foreign capabilities and threats and their potential to affect U.S. interests abroad, as well as U.S. preparations for defeating military foreign threats. A "bottom-up" approach to the intelligence cycle process model provides state and local decision makers, public safety officials and the private sector the ability to influence and

[160] The White House, *Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the U.S.*, December 2011, 3.

shape national interest through fusion centers operating within the National Network at the state and local level. There exists a credible need for a new intelligence process model that integrates the post-9/11 HSE and with it a need to train these diverse groups. Developing an intelligence process that integrates both, a "top-down" and "bottom-up" approach provides a comprehensive evaluation of the threats to homeland security that affect all levels of government and engages multiple public safety disciplines.

B. INTELLIGENCE CYCLE PROCESS MODEL TRAINING

Members of the USIC have developed organizational institutions to train its intelligence elements on the intelligence cycle process model most fitting their organization. The CIA has the Sherman Kent School for Intelligence Analysis that provides specialized training in the craft of intelligence analysis.[161] In 2005, the FBI established the Intelligence Career Service comprised of intelligence analysts, language specialists and surveillance specialists personnel with intelligence training at the College of Analytical Studies. It was later changed to the Center for Intelligence Training to provided basic and advanced training for FBI analysts and agents.[162] The Department of Defense provides intelligence training via individual service institutions and jointly through the National Intelligence University located within the Defense Intelligence Analysis Center that focuses on the profession of intelligence and offers an in-depth curriculum intended to enhance the analytical skills and competencies of intelligence analysis.[163] The DHS I&A Training Branch established the Homeland Security Intelligence Training Center to strengthen DHS intelligence enterprise capabilities, enhance collaboration among the intelligence offices of the department's components, and provide specialized intelligence training to state and local officials.[164]

---

[161] U.S. Central Intelligence Agency, *Training Resources*, accessed August 10, 2013, https://www/cia/goc/offices-of-cia/intelligence-analysis/training-resources.html.

[162] U.S. Department of Justice, Federal Bureau of Investigation, *National Security Branch*, September 2006, accessed August 10, 2013, http://www.hsdl.org/?view&did=480684.

[163] U.S. Defense Intelligence Agency, accessed August 10, 2013, http://www.dia.mil/university/.

[164] U.S. Department of Homeland Security, *The Department Develops its Own Professional Intelligence Workforce*, January 14, 2009, accessed August 10, 2013, http://ipv6.dhs.gov/journal/leadership/labels/Intelligence%20and%20Analysis%20Directorate.html.

The DHS also supports formal degree granting opportunities with tailored intelligence instruction through the Naval Postgraduate School – Center for Homeland Defense and Security.

In October 2007, the DOJ Global Justice Information Sharing Initiative commonly referred to as Global, published the *Minimal Criminal Intelligence Training Standards for Law Enforcement and Other Criminal Justice Agencies in the United States*. Global serves as a federal advisory committee to the U.S. Attorney General on critical justice information sharing initiatives.[165] The Global training philosophy is intended to "…develop a culture of information analysis and information sharing within the law enforcement communities…"[166] Global defines the intelligence cycle as "an organized process by which information is gathered, assessed and distributed in order to fulfill the goals of the intelligence function. It is a method of performing analytic activities and placing the analysis in a usable form."[167]

Global identified objectives for law enforcement intelligence analyst, intelligence managers/commanders, executives, and officers. Within these objectives is a standard for training the intelligence process/cycle that includes topics to be considered: Collection, analysis, dissemination, production, collation, evaluation, and assessment within a three-hour block of instruction for law enforcement analysts and managers.[168] The law enforcement officer basic criminal intelligence officer provides for 40-minutes of training to include the officer's role and responsibilities in the intelligence process/cycle.[169] Global does not identify sequential steps common within the USIC nor provide illustrations of the intelligence cycle.

Though HSE partners, specifically state and local officials, have limited opportunities to attend in-residence training opportunities at the USIC member

[165] U.S. Department of Justice, Global Justice Information Sharing Initiative, Findings and Recommendations, *Minimal Criminal Intelligence Training Standards for Law Enforcement and Other Criminal Justice Agencies in the United States*, Version 2, October 2007.

[166] Ibid., 1.

[167] Ibid., 41.

[168] Ibid., 4, 8.

[169] Ibid., 18.

institutions, there are far more intelligence focused training opportunities presented to state and local officials through on-site mobile training events sponsored by a number of elements. Through the DHS/DOJ Fusion Process Technical Assistance Program and Services, DHS FEMA sponsored MIPT and the Institute of Intergovernmental Research delivers on-site mobile training opportunities to the National Network, as well as the state and local members of the HSE. In order to effect the required change, some have opined the need to establish as national center for intelligence training in conjunction with a national intelligence strategy. Although a national center has not been established, the Governor of Texas designated the Texas Department of Public Safety, Intelligence and Counter-Terrorism Division (DPS-ICT) as the proponent for intelligence for the State of Texas. The DPS-ICT, in concert with criminal justice professors at Texas State University, has initiated a project intended to create a certification program providing statewide training and an education baseline for all analysts in Texas.[170] While many have echoed the sentiment regarding specific intelligence training to state and local law enforcement, there has been little realization of the kind of training that state, local, and tribal law enforcement communities need to be truly effective homeland security partners.[171]

The need for integration of the state and local environment into nation's intelligence effort was a principal finding of the USIC assessments in the wake of the 9/11 attacks and desired goals of subsequent national strategies. In addition to the USA PATRIOT Act, the 2004 IRTPA provided the DNI and is responsible for establishing intelligence community-wide policies. Yet, there remain challenges and practical implementation with the intelligence cycle process model and domestic intelligence collection by the HSE, as noted in the previous chapter. It is critical to recognize and define how the USIC intelligence cycle process model is to be employed within the HSE at the state and local level. Equally significant is ascertaining if a standardized

[170] Texas Department of Public Safety, *IDP's for Intelligence Analysts at the Texas Department of Public Safety PowerPoint*, accessed October 7, 2013, www.iafie.org/resource/resmgr/2012_conference/mullins.pptx.

[171] Law Enforcement Assistance And Partnership, *A Law Enforcement Assistance and Partnership Strategy, Improving Information Sharing Between the Intelligence Community and State, Local, and Tribal Law Enforcement*, 5.

intelligence cycle process model exists that is capable of being employed effectively within the USIC, the HSIE, as well as the HSE. As noted in previous chapters, there are many versions of the intelligence cycle process model that is generally aligned to an organizations' mission space and numerous intelligence training venues theoretically serving to provide some aspect of training on the intelligence cycle.

C. STATE AND LOCAL LAW ENFORCEMENT COMMUNITY

A key element of the HSE is the state and local law enforcement community. Intelligence in law enforcement has historically been misunderstood, underutilized, and even misapplied. With 18,000 local and state law enforcement agencies in the U.S., there is a critical need to provide and coordinate education, training, and professional services related to domestic intelligence collection activities and the employment of a standardized intelligence cycle process model. There are many misconceptions about the meaning and application of intelligence within law enforcement, although the IACP Criminal Intelligence Sharing Plan provides "intelligence is the combination of credible information with quality analysis - information that has been evaluated and from which conclusions can be drawn.[172]

Ms. Lisa Palmieri suggests the intelligence cycle process model is not fully explored in the law enforcement community within the context of criminal investigations because case information collected during an investigation is often considered "peripheral to proving the elements of the crime." Additionally, Ms. Palmeiri claims the training of law enforcement officials and intelligence analysts has not been institutionalized necessary for incorporating "intelligence as an element of policing culture [that] would address the challenge of evaluating intelligence analysts in police agencies."[173]

Various reports identify more than 800,00 law enforcement officials nationwide responsible for public safety. Being able to provide intelligence products that support

[172] David L. Carter, U.S. Department of Justice, Office of Community Oriented Policing Services, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, 2nd ed., January 2009, 10, 13.

[173] Lisa M. Palmieri, Law Enforcement Intelligence Units and International Association of Law Enforcement Intelligence Analysts, *Challenges Facing Law Enforcement Intelligence*, 2011, 313.

more than 800,000 state and local law enforcement officials and the private sector requires a new approach to the intelligence cycle process model. Given the 18,000 state and local law enforcement agencies operating within the HSE, and the misconceptions about intelligence, the type of products disseminated generally fails to satisfy varied and numerous customer needs.

In the 1970s, standards were introduced requiring police departments to articulate "criminal predicate" before beginning intelligence operations on members of the community. In the 1980s, the Regional Information Sharing System was established and implemented through the Criminal Intelligence Operating Policies at the federal level - 28 CFR Part 23.[174] A noticeable distinction exposes the current USIC intelligence cycle process model in that it does not require criminal predicate, on the other hand, 28 CFR Part 23 does not address the collection of information for policymakers, yet both are in use within the HSE in support of domestic intelligence collection activities.

Police officers' and sheriff's believe that in order to be effective in preventing terrorism and related criminal activity; it is essential that they fully participate in the intelligence cycle process at both the federal and nonfederal levels. Additionally, they must become advocates for law enforcement intelligence products that meet their information needs and ensure law enforcement intelligence and other information is shared with their communities.[175] The current USIC intelligence cycle process model paradigm fosters aggressive, active intelligence gathering. It anticipates the threat before it arises and plans preventive action against suspected targets. In contrast, the law enforcement paradigm fosters reactions to information provided voluntarily, uses ex post

[174] Roger G. Dunham, Geoffrey P. Alpert, Jennifer E. Davis, and Robert W. Taylor, *Intelligence-Led Policing and Fusion Centers, Critical Issues in Policing: Contemporary Readings*, 6th ed. (Waveland Press, 2010), 226–227.

[175] Law Enforcement Assistance And Partnership, *A Law Enforcement Assistance and Partnership Strategy, Improving Information Sharing Between the Intelligence Community and State, Local, and Tribal Law Enforcement*, 1.

facto arrests and trials governed by the rule of law, rules of evidence, and the protection of the rights of American citizens.[176]

Although law enforcement agencies need background information or "strategic intelligence" regarding patterns of criminal activity (e.g., analysis indicating that increasing quantities of cocaine are flowing through harbors in southern Florida), they tend to give higher priority to tactical information (e.g., a tip that a specific cargo vessel is scheduled to off-load a shipment of cocaine at a specific dock in Miami on the night of August 4). However, national policymakers require a continuous stream of information about countries, groups, and individuals working against U.S. interests. There is no end-point to these requirements; even a favorable evolution of events does not mean the end of the need for up-to-date information. In many cases at the federal level, the need for intelligence is more important than the need for dealing with a particular incident.

D. PRIVATE SECTOR

In addition to the National Network, primarily supported by state and local law enforcement, there is a philosophy to integrate and maintain relationships with the private sector to support the needs of the national intelligence architecture. The are 15 private sectors Information Sharing and Analysis Centers (ISAC) considered operational organizations that collect, analyze, and share threat and vulnerability information to protect critical infrastructure.[177] These private sector elements with specialized capabilities can and are being used to address national security concerns and homeland security threat issues. These ISACs[178] are: the Communications ISAC; the Electric Sector ISAC; the Emergency Services ISAC; the Financial Services ISAC; the National Health ISAC; the Information Technology ISAC; the Multi-State ISAC; the Maritime Security ISAC; the Nuclear Energy Institute; the Public Transportation ISAC; the Surface Transportation ISAC; the Real Estate ISAC; the Research and Education ISAC; the

[176] Richard A. Best Jr., Congressional Research Service, *Intelligence and Law Enforcement: Countering Transnational Threats to the U.S.*, RL30252, December 3, 2001, 9.

[177] Mark A. Randol, Congressional Research Service, *Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches*, RL33616, January 14, 2009, 14.

[178] National Council of Information Sharing and Analysis Centers, accessed August 10, 2013, http://www.isaccouncil.org/memberisacs.html.

Supply Chain ISAC; and the Water ISAC, all of which enhance information sharing and serve as analytic centers within the private sector.

With the integration of private sector elements into the HSE and their value-added to information sharing, questions arise as to the intelligence cycle process model being trained by the elements mentioned previously. The success of U.S. intelligence at home will increasingly depend on a new form of domestic intelligence collection against specific threats and on the forging of a deep partnership with the American nation, from local law enforcement to the private sector.[179]

Within the governance structure of the National Network, the *Baseline Capabilities for State and Major Urban Area Fusion Centers* provides fusion centers "shall have a governance structure that provides appropriate representation for the jurisdictions and disciplines in the center's area of responsibility," and as an example it reflects "including representatives from…the Information Sharing and Analysis Centers…" in support of Fusion Center Guidelines 3, 4, and 5.[180] In highlighting the role of fusion centers in national security, DHS posits "The national security enterprise must reach beyond the capabilities of the federal government and national intelligence community to identify and warn about impending plots that could impact the homeland, particularly when the individuals responsible for the threats operate within the United States and do not travel or communicate with others overseas."[181] Given DHS I&A's responsibilities as a USIC member, it has the largest customer set than any other intelligence community member.

This thesis summarizes there are no fewer than an estimated 175 federal, state, local law enforcement, and private sector establishments contributing to the responsibility for sharing homeland security information through the conduct of collecting, analyzing

[179] Jennifer E. Sims, and Burton Gerber, *Transforming U.S. Intelligence* (Washington, D.C.: Georgetown University Press, 2005), 198.

[180] U.S. Department of Homeland Security and U.S. Department of Justice, *Baseline Capabilities for State and Major Urban Area Fusion Centers: A Supplement to the Fusion Center Guidelines***,** September 2008, 23.

[181] U.S. Department of Homeland Security, *State and Major Urban Area Fusion Centers*, accessed February 24, 2012, http://www.dhs.gov/files/programs/gc_1156877184684.shtm.

and disseminating threat information based on the number of USIC member organizations, HSIE elements, fusion centers, FBI Field Intelligence Groups, and private sector ISACs. At the federal level, there are 17 members of the USIC; within the USIC there are 56 FBI Field Intelligence Groups as elements of the FBI National Security Branch; three (3) DHS headquarters elements and six (6) operational component intelligence elements that make up the HSIE for a total of (9); at the state and local level there are 78 DHS/DOJ recognized fusion centers; and at the private sector level 15 ISACs. These 175 entities that make up the HSE has received or may receive some form of training on the varied intelligence cycle process models from various federal level, federally sponsored or academic institutions.

The number of intelligence cycle process models, as well as the amount of intelligence consumers, is as varied as the number of intelligence producing entities. Policymakers exist at all levels of government, law enforcement elements operate at all levels of government and other public safety officials provide prevention, protection, recovery, and response resources at all levels of government. Additionally, the private sector, likewise, supports the prevention, protection, recover, and response mission spaces that integrates the business community yet another intelligence consumer. Because of the post-9/11 HSE, these entities now serve as key partners in the first phase of the intelligence cycle – planning and direction. However, a vital question surfaces; who is responsible for determining the planning and direction, as well as prioritizing, what should be collected in order to ensure appropriate finished intelligence is produced and disseminated as an end-result of the intelligence cycle process model? Can the National Network serve as an effective analytic element at the state and local level for such an enormous customer base?

Additionally, with the diverse numbers of intelligence cycle process models and the assorted training venues another question remains; is it appropriate to employ the intelligence cycle process model in an effort to detect significant national security and homeland security threats originating or residing within our nation's borders provide it was not designed and intended to serve as such? Further, is it possible to evaluate the

USIC intelligence cycle process model in the performance of domestic intelligence collection activities at the state and local level in support of the HSE?

A new intelligence cycle process model would provide an opportunity for a more cohesive community of stakeholders who could both exploit training and educational opportunities to the benefit of the collective whole.

E. PRACTICAL CHALLENGES TO EMPLOYING THE INTELLIGENCE CYCLE PROCESS MODEL

Two key challenges to employing the USIC intelligence cycle process model is defining the term *homeland security intelligence* and the lack of access to information necessary to provide a comprehensive threat picture. A challenge to adopting a standardized intelligence cycle process model within the HSE may be associated with the fact the term *homeland security intelligence* has not been defined or codified in law.[182] The closest definition provided by law is the term *homeland security information* provided in the 2002 Homeland Security Act that states it is;

> any information possessed by a federal, state or local agency that (a) related to the threat of terrorist activity, (b) relates to the ability to prevent, interdict or disrupt terrorist activity, (c) would improve the identification or investigation of a suspected terrorist or terrorist organization, or (d) would improve the response to a terrorist act.

There are clear challenges associated with effectively employing initial phases of the intelligence cycle process model - planning and direction, as well as collection - at the state and local level given the independent nature of stakeholders. What element serves as the compromising authoritative body for determining planning and direction for the National Network and broader HSE? What element ensures access to information when it is incomplete due to information sharing disputes between agencies (whether cultural or procedural)? What element shoulders the responsibility to address the lack of standardized training given the various forms of intelligence cycle process models? As argued previously, proper planning and direction, as well as efficient information

[182] Mark A. Randol, Congressional Research Service, *Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches*, RL33616, January 14, 2009, 9.

collection within the HSE, increases the performance of the final intelligence product aimed at providing situational awareness and a common threat picture for all stakeholders.

The U.S. counterterrorism strategy and its implementation have seen little progress since the terrorist attacks of 9/11. The "shared responsibility" proposition has not been fully realized in the sharing of intelligence and threat information at all levels of government or the "whole of government" approach to counterterrorism investigations. This concern directly affects DHS' ability to share intelligence and threat information with state, local, and private sector partners as mandated by the 9/11 Commission Act, particularly given that the DHS State and Local Program Office has a mandated role to support the National Network as state and local intelligence collection and analytical centers.

F. CONCLUSION

Within this thesis, the writer identified several critical moments in U.S. history that initiated major intelligence reform at the federal level, as well as the state and local levels of government. The attack of Pearl Harbor in 1947 and the subsequent involvement in World War II, initiated the creation of the USIC per the 1947 National Security Act. In 1981, President Ronald Reagan issued EO 12333 *United States Intelligence Activities* in order to address domestic intelligence collection abuses by federal level government agencies. During the same general period, the "1983-suits" were legal actions brought against local police intelligence units in the 1960s and 1970s for violating citizen groups' First Amendment rights. This period facilitated the establishment of IALEA and the establishment of 28 CFR Part 23 that provides guidance for criminal intelligence. The tragic and horrible attack on the U.S. by international terrorist on September 11, 2001, initiated the creation of DHS, and subsequently, the DHS I&A State and Local Program Office charged with providing federal level support to the National Network and HSE. After 9/11, the IACP endorsed ILP and the Major City Chiefs' initiated the MCC Criminal Intelligence Enterprise.

Table 2, constructed by the author, provides a visual snapshot of the gaps in synchronizing federal level intelligence initiatives and integration. While the post-9/11 National Network was not established until 2003, history reveals a pattern of addressing domestic intelligence collection issues. Based on the information reflected, one can deduce the timeframe gaps between federal level intelligence doctrine and intelligence cycle process employment and the establishment of local level intelligence guidance and intelligence process endorsement. As an example, there was 24 years from the initiation of the first U.S. Army-wide intelligence doctrine to the first documented intelligence cycle process model [1920–1944] and 27 years until the creation of the USIC [1920–1947]. There was 33 years from the creation of the USIC to the establishment of the IALEA, formalizing efforts to professionalize law enforcement analysts and the establishment of the Regional Information Sharing System operating under 28 CFR Part 23 [1947–1980]. The IACP, which was established in 1893, did not endorse intelligence-led policing until 19 years later in 2002, the same period in which DHS was created under the 2002 Homeland Security Act. In 2007, the 9/11 Commission Act established the DHS I&A State and Local Program Office for the specific purpose of providing federal level intelligence support to the National Network created in 2003. Establishing intelligence training guidance at the state and local level, external to the National Network occurred in 2007 with the Major City Chiefs' establishment of the Major City Chiefs' Criminal Intelligence Enterprise four years later in 2011. The White House supported the intelligence progress at the state and local level and issued EO 13470 in 2008 that amended EO 12333 to include the state and local environment within the U.S. Intelligence Activities guidance, as well as establishing EO 13594 two years later in 2010 that provided guidance for state and local access to national security information. The intent of the aforementioned chronology of intelligence initiatives is to provide a visual snapshot of the gaps between time in the synchronizing of federal level intelligence initiatives and integration of the National Network and the broader HSE.

Table 2. Timeline Reflecting Intelligence Policy Engagement among Federal and Local Environment

Date	Organization	Intelligence Initiative
1920	U.S. Army	U.S. Army-wide intelligence doctrine
1944	U.S. Army	First documented intelligence cycle process model
1947	White House & Congress	Established U.S. Intelligence Community
1980	International Association of Law Enforcement Analyst	Professionalize law enforcement analytic cadre and increase capabilities
1980	Regional Information Sharing System	RISS established and implemented through the Criminal Intelligence Operating Policies at the federal level - 28 CFR Part 23
1981	White House	Established Executive Order 12333 - U.S. Intelligence Activities; provides guidance for U.S. intelligence activities among USIC members
2002	International Association of Chiefs' of Police	Established in 1893; endorsed intelligence-led policing
2003	National Network of Fusion Centers	Established state & local intelligence and information sharing network
2007	DHS I&A	Establish a DHS State, Local, and Regional Fusion Center Initiative necessary for establishing partnerships with state, local, and regional fusion centers; specifically section (b) (11) mandates providing training to state, local, and regional fusion centers
2007	DOJ Global Justice Information Sharing Initiative	Published the minimal criminal intelligence training standards for law enforcement and other criminal justice agencies in the U.S.
2008	White House	Amended EO 12333 via EO 13470 to include state & local environment
2010	White House	Established EO 13549; provided state & local access to classified national security information
2011	Major City Chiefs'	Established Major City Chiefs' Criminal Intelligence Enterprise

In theory, the intelligence production cycle, otherwise known as the intelligence cycle, is the process by which information is acquired and converted into an assessment or estimate begins and ends with the policy maker. Ideally, policymakers advise the managers of the USIC collection and production organization of their informational needs. In practice, it is often up to intelligence managers to gauge and anticipate policy maker's needs because policy makers have never been particularly diligent or effective in articulating their informational needs. Yet, today DHS I&A field deployed personnel not only provide training on the intelligence cycle process model, but they are also requested to manage the intelligence cycle in their area of responsibility to include the sharing of threat-related information between SLTPS partners and the federal government. Throughout the literature review and case study, the writer offered the intelligence cycle process model serves as a theoretical concept allowing academic comprehension by nonintelligence individuals. The writer also reasoned, based on the interpretation of literature, case study to include professional experience and observation, the practical employment of the intelligence cycle process model at the strategic and operational levels within the post-9/11 HSE has not fully been studied in order to evaluate its effectiveness or appropriateness.

This document was intended to provide awareness of employing the intelligence cycle process model and initiate dialogue regarding standardizing an intelligence cycle process within the HSE. The writer acknowledges there are possible challenges with attempting to standardize the intelligence cycle process model. The obvious challenges to the enormous task of standardizing a domestic intelligence cycle process given the numerous and varied stakeholders at the federal, state and local level are identifying who would serve as the principle oversight and/executive agency for standardizing such a training program. While the DNI is the executive agency for the USIC, additional thought would have to be given to integrating the state and local level, as well as the private sector. At the state and local level, the National Fusion Center Association represents the National Network, and they are in an executive position to provide influence for the training requirements. Similarly, the IACP, the MCCIE, and IALEIA serve as influencing bodies for elements external to the National Network. The private sector as critical

elements of the HSE may prove as the most challenging when integrating key elements into discussions of standardizing the intelligence cycle process model.

Another challenge deals with building consensus among the numerous and varied HSE stakeholders regarding the design of an intelligence cycle process model that appropriately addresses USIC intelligence requirements and the intelligence information needs for nontraditional intelligence elements. In proposing and developing a new intelligence cycle process model, considerations must be given to the varying analytic and operational paces of the intelligence, law enforcement, and private sector environments. The timeframe provided for pure USIC analytic and operational differ significantly from the analytic and operational environments of the National Network, the great law enforcement and private sector communities.

In conclusion, drawing on publicly available information from government, academia, and national security consortiums, analysis revealed broad acceptance of the intelligence cycle process model philosophy. However, literature provided by academic and operational practitioners support claims that the intelligence cycle process model is flawed and not practical in the operational environment. This thesis may serve as a basis for recommending additional research necessary for studying the intelligence cycle process model implementation and employment within the HSE and its effectiveness in preventing terrorist attacks and enhancing national security intelligence.

THIS PAGE INTENTIONALLY LEFT BLANK

BIBLIOGRAPHY

A Complex Organization United Under a Single Goal: National Security. http://www.intelligence.gov/about-the-intelligence-community/.

American Civil Liberties Union. "More About Fusion Centers." http://www.aclu.org/spy-files/more-about-fusion-centers.

Berman, Emily. *Domestic Intelligence: New Powers, New Risks*. Brennan Center for Justice at New York University School of Law, 2011.

Best, Jr., Richard A. Congressional Research Service, *Intelligence and Law Enforcement: Countering Transnational Threats to the U.S.*, RL30252, December 3, 2001.

Bigelow, Michael E. "A Short History of Army Intelligence," *Military Intelligence*, July-September 2012.

The Boston Channel. *Effectiveness of Fusion Centers Questioned*, http://www.wcvb.com/news/investigative/effectiveness-of-fusion-centers-questioned/-/12520878/20358362/-/bkveudz/-/index.html#ixzz2aHaeHk5x.

Boston Globe. *FBI Did not Alert State's Anti-terror Unit to Its Probe of Suspected Bomber in 2011*, http://www.boston.com/politicalintelligence/2013/04/25/fbi-did-not-alert-state-anti-terror-unit-its-probe-suspected-bomber/RLHZM6GHRotZ6ciIYxmiKP/story.html.

Breckinridge, Scott D. *The CIA and the U.S. Intelligence System*. Boulder, CO.: Westview Press, 1986.

Carl, Leo D. *The International Dictionary of Intelligence*. McLean, VA. International Defense Consulting Service, 1990.

Carter, David L. U.S. Department of Justice, Office of Community Oriented Policing Services, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, 2nd ed., January 2009.

———. White paper, *The Intelligence Fusion Process for State, Local and Tribal Law Enforcement*, Michigan State University, May 2006. http://www.ncirc.gov/documents/public/intelligence_fusion_process.pdf, 7.

———. *The Law Enforcement Intelligence Function: State, Local, and Tribal Agencies*, http://www.hsdl.org/?view&did=469588.

Cid, David. *Understanding Counterterrorism: A Guide for Law Enforcement Policy Makers and Media*, 2012.

Cilluffo, Frank J., Joseph R. Clark, and Michael P. Downing. *Counterterrorism Intelligence: Law Enforcement Perspectives*. Counterterrorism Intelligence Survey Research. Homeland Security Policy Institute. George Washington University. September 2011.

Clark, Robert M. *Intelligence Analysis: A Target-Centric Approach*. Washington, D.C.: CQ Press, 2004.

CNN. "FBI Agents Interviewed Bombing Suspect in 2011." http://www.cnn.com/2013/04/19/us/boston-suspects-no-links/index.html.

CNN. "Boston Marathon Terror Attack Fast Facts." http://www.cnn.com/2013/06/03/us/boston-marathon-terror-attack-fast-facts.

Connors, Timothy, and John Rollins. Center for Policing Terrorism at the Manhattan Institute. *State Fusion Center Processes and Procedures: Best Practices and Recommendations*. Policing Terrorism Report, No. 2, September 2007.

Council on Foreign Relations. *Domestic Intelligence and the Boston Bombings*, http://www.cfr.org/counterterrorism/domestic-intelligence-boston-bombings/p30557.

Crumpton, Henry A. "Intelligence and Homeland Defense". *Transforming U.S. Intelligence*, edited by Jennifer E Sims and Burton Gerber, 198–219. Washington, D.C: Georgetown University Press, 2005.

CQ Homeland Security. "Fusion Center Hearing." http://homeland.cq.com/hs/.

Dunham, Roger G., Geoffrey P. Alpert. Jennifer E. Davis, and Robert W. Taylor. *Intelligence-Led Policing and Fusion Centers, Critical Issues in Policing: Contemporary Readings*, 6th ed, Waveland Press.

Executive Order 12333. *United States Intelligence Activities* (As amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008).

Executive Order 13470. Further Amendments to Executive Order 12333, United States Intelligence Activities, Part 1 1.1(f), www.fas.org/irp/offdocs/eo/eo-13470.htm.

Flanagen, Sephen J. "Managing the Intelligence Community", *International Security*, vol 10 no. 1 (Summer 1985), MIT Press, http://www.jstor.org/stable/2538790.

Hanson, Stephanie. *Al-Shabaab*. August 10, 2011, http://www.cfr.org/somalia/al-shabaab/p18650.

The Heritage Foundation. *Leadership For America*, http://www.heritage.org/about.

Hulnick, Arthur S. "What's Wrong with the Intelligence Cycle". *Intelligence and National Security,* 21. no. 6. December 2006.

Institute for Intergovernmental Research. *Criminal Intelligence Systems Operating Policies (28 CFR Part 23) Training and Technical Assistance Program,* http://www.iir.com/WhatWeDo/Criminal_Justice_Training/28CFR/.

Intelligence and National Security Alliance. *Intelligence to Protect the Homeland: Taking Stock Ten Years Later and Looking Ahead*. White paper, Arlington: Homeland Security Intelligence Council, 2011.

International Association of Chiefs of Police. *Criminal Intelligence Sharing: A National Plan for Intelligence-Led Policing at the Local, State and Federal Levels*. Alexandria, VA, 2002.

Iowa Department of Public Safety. *Division of Intelligence: Intelligence Cycle*. http://www.dps.state.ia.us/intell/intellcycle.shtml.

Johnson, Loch K., and James J. Wirtz. *Intelligence and National Security: The Secret World of Spies-An Anthology*. Oxford, NY. Oxford University Press. 2008.

Kamarck, Elaine C. *Transforming the Intelligence Community: Improving the Collection and Management of Information*. John F. Kennedy School of Government, Harvard University, IBM Center for the Business of Government, October 2005.

Kimery, Anthony L. *Homeland Security Today*, "DHS I&A Chief Outlines New Vision", May 13, 2010, http://www.hstoday.us.

Law Enforcement Assistance and Partnership. *A Law Enforcement Assistance and Partnership Strategy, Improving Information Sharing Between the Intelligence Community and State, Local, and Tribal Law Enforcement*.

Lowenthal, Mark M. *Intelligence: From Secrets to Policy*. Washington, D.C.. CQ Press. 2003; 2012.

Lyon, Verne. *Domestic Surveillance: The History of Operation CHAOS*, http://www.serendipity.li/cia/lyon.html.

Major Cities Chiefs Criminal Intelligence Enterprise. https://www.majorcitieschiefs.com/pdf/news/mcca_criminal_intelligence_enterprise_initiative_20120329.pdf.

Masse, Todd. Congressional Research Service, *Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches*, RL33616, August 18, 2006.

Mayer, Matt A., and Scott G. Erickson. *Changing Today's Law Enforcement Culture to Face 21st-Century Threats*. The Heritage Foundation. June 23, 2011.

The National Council of Information Sharing and Analysis Centers. http://www.isaccouncil.org/memberisacs.html.

Newsdesk. *Israel Homeland Security*, "A "Pressure Cooker" Warning was Given a Few Times in Recent Years", http://i-hls.com/2013/04/a-pressure-cooker-warning-was-given-in-2004/.

New York Times. FBI Said to Find It Could Not Have Averted Boston Attack, http://www.nytimes.com/2013/08/02/us/fbi-said-to-conclude-it-could-not-have-averted-boston-attack.html?_r=0.

Nolen, Bridget Rose. *Information Sharing and Collaboration in the United States Intelligence Community: An Ethnographic Study of the National Counterterrorism Center*, PhD diss., University of Pennsylvania, 2013.

Office of the Director of National Intelligence. *Leading Intelligence Integration*, http://www.dni.gov/index.php/about/history.

———. Preliminary *Report on the Creation of the Information Sharing Environment*, http://www.ise.gov/sites/default/files/preliminaryreport.pdf.

Office of Homeland Security. *National Strategy for Homeland Security*, July 2002.

Palmieri, Lisa M. *Challenges Facing Law Enforcement Intelligence*, Law Enforcement Intelligence Units and International Association of Law Enforcement Intelligence Analysts, 2011.

———. International Association of Chiefs of Police, "Information Vs. Intelligence: What Police Executives Need to Know", *The Police Chief*, vol. 72, no. 6, Alexandria, VA, June 2005.

RAND. *Predictive Policing – The Role of Crime Forecasting in Law Enforcement Operations, Prediction-Led Policing Business Process Model*, http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf.

Randol, Mark A. Congressional Research Service, *Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches*, RL33616, January 14, 2009.

———. Congressional Research Service, *The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress*, R40602, March 19, 2010.

Rosenbach, Eric. *Confrontation or Collaboration? Congress and the Intelligence Community*. Belfere Center for Science and International Affairs. The Intelligence and Policy Project. Background Memorandum for the 111th Congress. July 2009.

Sims, Jennifer E., and Burton Gerber. *Transforming U.S. Intelligence*. Washington, D.C., Georgetown University Press, 2005.

Sources and Methods: Part 4 – *The Traditional Intelligence Cycle and its History*. http://sourceandmethods.blogspot.com/2011/05/part-4-traditional-intelligence-cycle.html.

Texas Department of Public Safety. *IDP's for Intelligence Analysts at the Texas Department of Public Safety PowerPoint*, www.iafie.org/resource/resmgr/2012_conference/mullins.pptx.

"Targeting Intelligence Gathering in a Dynamic Competitive Environment". *International Journal of Information Management*, vol. 20, no. 3, 2000.

Townsend, Frances. *Intelligence to Protect the Homeland -Taking Stock Ten Years Later*. Intelligence and National Security Alliance, 2011.

U.S. Bureau of Justice Assistance. *Intelligence-Led Policing: The New Intelligence Architecture*, September 2005.

U.S. Central Intelligence Agency. *Training Resources*, https://www/cia/goc/offices-of-cia/intelligence-analysis/training-resources.html.

———. http://vmc.cia-dia.50megs.com/fboi/facttell/intcycle.htm.

U.S. Congress. *110th Congress Public Law, Public Law 110–53, Implementing Recommendations of the 9/11 Commission Act of 2007*.

———. *The Intelligence Community in the 21st Century: Staff Study - Permanent Select Committee on Intelligence House of Representatives 104th Congress*, http://www.gpo.gov/fdsys/pkg/GPO-IC21/html/GPO-IC21–13.html.

———. Statement for the Record Senator Joe Lieberman (Ret) House Committee On Homeland Security, *The Boston Bombings: A First Look*, http://docs.house.gov/meetings/HM/HM00/20130509/100785/HHRG-113-HM00-Wstate-SchwartzK-20130509.pdf, 2013.

———. *Congressional Testimony of Boston Police Commissioner Edward F. Davis, III before the House Committee on Homeland Security,* http://docs.house.gov/meetings/HM/HM00/20130509/100785/HHRG-113-HM00-Wstate-SchwartzK-20130509.pdf, 2013.

U.S. Defense Intelligence Agency. http://www.dia.mil/university/, http://ipv6.dhs.gov/journal/leadership/labels/Intelligence%20and%20Analysis%20Directorate.html.

U.S. Department of Defense. http://www.dodccrp.org/events/9th_ICCRTS/CD/papers/044.pdf.

U.S. Department of Homeland Security. *Intelligence and Information Sharing Initiative: Homeland Security Intelligence and Information Fusion*. Homeland Security Advisory Council. April 28, 2005.

———. *Roles and Function*, Office of Intelligence and Analysis General Counsel Memorandum, July 29, 2008.

———. *DHS' Role in State and Local Fusion Centers is Evolving*. Office of Inspector General Report – OIG-09-12. October 2008.

———. *The Department Develops Its Own Professional Intelligence Workforce*, January 14, 2009.

———. *Bottom-Up Review Report*, July 2010.

———. *Information Sharing with Fusion Centers Has Improved, but Information System Challenges Remain*, Office of Inspector General Report 11-04, October 2010.

———. *2011 National Network of Fusion Centers Final Report*, May 2012.

———. *Role of Fusion Centers in Countering Violent Extremism*, October 2012.

———. *2012 National Network of Fusion Centers Final Report*, June 2013.

———. *State and Major Urban Area Fusion Centers*, http://www.dhs.gov/files/programs/gc_1156877184684.shtm.

———. *Responsibilities of Intelligence Officers*, http://www.dhs.gov/deployed-intelligence-officers-and-protective-security-advisors.

———. http://www.dhs.gov/more-about-office-intelligence-and-analysis-mission.

———. *Fusion Center Guidelines Developing and Sharing Information and Intelligence in a New Era; Guidelines for Establishing and Operating Fusion Centers at the Local, State, and Federal Levels; Law Enforcement Intelligence, Public Safety, and the Private Sector*, http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf.

———. *Target Capabilities List: A companion to the National Preparedness Guidelines*, September 2007, http://www.fema.gov/pdf/government/training/tcl.pdf.

———. Management Directive 8110, *Intelligence Integration and Management*, http://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_8110_intelligence_integration_and_management.pdf.

U.S. Department of Homeland Security and U.S. Department of Justice. *Baseline Capabilities for State and Major Urban Area Fusion Centers: A Supplement to the Fusion Center Guidelines*, September 2008.

U.S. District Court for the District of Massachusetts. Criminal Complaint, *USA v. Dzhokar Tsarnev*, Case No. 13-2106-MBB, April 21, 2013.

U.S. Department of Justice, Federal Bureau of Investigation. Inspection Division Commendation Memorandum to Mr. Roger Stokes, October 27, 2006.

———. Federal Bureau of Investigation. National Security Branch, September 2006, http://www.hsdl.org/?view&did=480684.

———. Federal Bureau of Investigation. http://www.fbi.gov/about-us/intelligence/intelligence-cycle.

———. Global Justice Information Sharing Initiative, *National Criminal Intelligence Sharing Plan*, October 2003.

———. Global Justice Information Sharing Initiative, Findings and Recommendations, *Minimal Criminal Intelligence Training Standards for Law Enforcement and Other Criminal Justice Agencies in the United States*, Version 2, October 2007.

U.S. Department of Justice Memorandum. *28 Code of Federal Regulations, Part 23*, March 31, 2005.

U.S. Senate. Select Committee to Study Governmental Operations with Respect to Intelligence Activities, *Intelligence Activities – National Security Agency and Fourth Amendment Rights*, October 29, 1975, http://www.aarclibrary.org/publib/church/reports/vol5/pdf/ChurchV5_1_Allen.pdf.

Wall Street Journal. "Boston Hearings Delve into FBI Alerts," May 9, 2013. https://www.online.wsj.com/article.

The White House. *National Strategy for Homeland Security*, Washington: The White House, October 2007.

———. *Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the U.S.*, December 2011.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California