NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

STANDING ON THE SHOULDERS OF GIANTS: WHERE DO WE GO FROM HERE TO BRING THE FIRE SERVICE INTO THE DOMESTIC INTELLIGENCE COMMUNITY?

by

Joshua M. Dennis

September 2012

Thesis Co-Advisors: Robert Simeral
Kathleen Kiernan

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2012	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Standing on the Shoulders of Giants: Where Do We Go from Here to Bring the Fire Service into the Domestic Intelligence Community?		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Joshua M. Dennis			
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 United States Fire Service has not only a role but a need to be included in the domestic intelligence community. The fire service in gaining access to information and adding untapped sources of information/intelligence can add value to the efforts of the domestic intelligence community and in return provide value added to fire departments' day-to-day operations. Absent is a strong national guidance for fire service intelligence integration, smart practice models, and local solutions have filled the vacuum. This thesis will look at the future of fire service intelligence sharing and how to pick up where previous efforts left off.

Specifically, a model for a national fire intelligence framework is presented. This model considers current local level intelligence solutions within the fire service, and a holistic approach that can meet the needs of unique individual departments. The secondary intent for this thesis is also to stimulate discussion, advance the evolution of fire service intelligence, suggest some operational models, and provide a point upon which others can build upon.

14. SUBJECT TERMS Fire Service Intelligence, Information Sharing, Domestic Intelligence, Suspicious Activity Reporting			**15. NUMBER OF PAGES** 73
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** 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

STANDING ON THE SHOULDERS OF GIANTS: WHERE DO WE GO FROM HERE TO BRING THE FIRE SERVICE INTO THE DOMESTIC INTELLIGENCE COMMUNITY?

Joshua M. Dennis
District Chief, Chicago Fire Department
J.D., DePaul University, 2003
M.S., Lewis University, 2006
B.A., Saint Xavier University, 1997

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
September 2012

Author: Joshua M. Dennis

Approved by: Robert Simeral
Thesis Co-Advisor

Kathleen Kiernan
Thesis Co-Advisor

Daniel Moran
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The United States Fire Service has not only a role but a need to be included in the domestic intelligence community. The fire service in gaining access to information and adding untapped sources of information/intelligence can add value to the efforts of the domestic intelligence community and in return provide value added to fire departments day-to-day operations. Absent is strong national guidance for fire service intelligence integration, smart practice models, and local solutions have filled the vacuum. This thesis will look at the future of fire service intelligence sharing and how to pick up where previous efforts left off.

Specifically, a model for a national fire intelligence framework is presented. This model considers current local level intelligence solutions within the fire service, and a holistic approach that can meet the needs of unique individual departments. The secondary intent for this thesis is also to stimulate discussion, advance the evolution of fire service intelligence, suggest some operational models, and provide a point upon which others can build upon.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CAD	Computer Aided Dispatch
CBRNE	Chemical Biological Radiological Nuclear Explosives
CUI	Controlled Unclassified Information
DHS	United States Department of Homeland Security
DNI	United States Director of National Intelligence
DOJ	United States Department of Justice
EMS	Emergency Medical Service
FBI	Federal Bureau of Investigation
FDNY	Fire Department City of New York
FEMA	Federal Emergency Management Agency
FLO	Fusion Liaison Officer
FOUO	For Official Use Only
FSIE	Fire Service Intelligence Enterprise
GAO	United States General Accounting Office
HSIN	Homeland Security Information Network
HSINT	United States Department of Homeland Security Intelligence
I&A	United States Department of Homeland Security Office of Intelligence and Analysis
IAFC	International Association of Fire Chiefs
IAFF	International Association of Firefighters
IC	United States Intelligence Community
ISE	Information Sharing Environment
ITACG	Interagency Threat Assessment and Coordination Group

JTTF	Joint Terrorism Task Force
LEO	Law Enforcement Online
LES	Law Enforcement Sensitive
NCTC	National Counterterrorism Center
NJTTF	National Joint Terrorism Task Force
NOC	National Operations Center
NSI	Nationwide Suspicious Activity Reporting Initiative
ODNI	Office of the Director of National Intelligence
OUO	Official Use Only
PPD	Presidential Policy Directive
SAR	Suspicious Activity Reporting
SLT	State Local Tribal
TLO	Terrorism Liaison Officer
USFA	United States Fire Administration

ACKNOWLEDGMENTS

The completion of this thesis would not have been possible without the CHDS staff and faculty. Special thanks are owed to my thesis advisors, Robert Simeral, and Kathleen Kiernan for their patience throughout this process and generosity with their time.

Finally, completion of this program would not have been possible without the patience of Retired Chicago Fire Commissioner Robert S. Hoff, Fire Commissioner José A. Santiago, my wife, and my children (Rachel, Alison, Spencer, Colin).

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. OBJECTIVE

Currently, the majority of the fire service receives intelligence second hand through the media, by the largess of others or through personal relationships. Therefore, currently there is no clear uniform interface upon which fire departments can rely. The objective of this thesis is to advance the existing literature regarding fire service information/intelligence sharing via a long-term solution. This solution can be advanced, implemented and realized through strong national policy linked to a grassroots evolution of information sharing between all fire departments. The grassroots evolution of Fire Service information/intelligence sharing will use different connection points within the domestic intelligence enterprise. The main goal of this solution and thesis is to provide a roadmap allowing all fire departments, regardless of size, to have an avenue to become engaged in the domestic intelligence enterprise.

B. BACKGROUND

The fire service is primarily responsible for the day-to-day mitigation of incidents, not involving arrest or detainment, in the United States. Yet, there is still no national framework for integration of the fire service into the domestic intelligence community. Different approaches have been taken and written about, such as the Fire Service Intelligence Enterprise (FSIE) and local best practices. Large metropolitan fire departments, such as New York and Chicago, have developed divisions dedicated to this task, while other large fire departments, such as Boston and Phoenix, work within law enforcement-established fusion centers.

Intelligence/information sharing was officially addressed by the U. S. Department of Homeland Security (DHS) when DHS's Office of Intelligence and Analysis (I&A) launched the Fire Service Intelligence Enterprise (FSIE) in December 2006. The FSIE began as a pilot information sharing partnership between the Fire Department—City of New York (FDNY) and I&A. The pilot resulted in lessons learned by both DHS and FDNY, while the main lesson learned was the benefit of information sharing between the

federal government and the fire service. In addition, increased clarity was gained regarding specific information that each organization could offer and receive, and the institutional requirements to enable two-way information sharing. This pilot applied to one fire department and provided an example of information/intelligence sharing for large urban departments. Smaller fire departments and fire departments without the resources to dedicate personnel and resources to either an internal intelligence unit or a law enforcement fusion center have no formal mechanism to receive intelligence or provide information to intelligence assets.

As a result of the initial FDNY pilot, in September 2007, 15 fire departments, along with representatives from the International Association of Fire Chiefs (IAFC) and the International Association of Firefighters (IAFF), met with representatives from the federal government,[1] to become the inaugural FSIE Conference. federal government representatives included:

- DHS I&A,
- Homeland Infrastructure Threat and Risk Assessment Center (HITRAC),
- National Preparedness Directorate,
- United States Fire Administration (USFA),
- Emergency Management Response-Information Sharing & Analysis Center (EMR-ISAC),
- The National Operations Center (NOC),
- Federal Emergency Management Agency (FEMA),
- Lessons Learned Information Sharing (LLIS),
- Risk Management Division (RMD),
- Director of National Intelligence (DNI)
- Office of the Program Manager for the Information Sharing Environment (PM-ISE).

The fifteen fire departments included:

- FDNY
- San Francisco

[1] United States Fire Administration. *FSIE Fact Sheet.* Washington, D.C., 2010.

- Los Angeles County
- Los Angeles City
- Seattle
- Houston
- Las Vegas
- Phoenix
- Chicago
- Boston
- Denver
- Washington DC
- Philadelphia
- Baltimore
- Miami Dade County

The keynote speaker at the FSIE conference was the sitting Under Secretary for Intelligence and Analysis (I&A) at the Department of Homeland Security, Mr. Charlie Allen, also appointed as the Chief Intelligence Officer for the department. Mr. Allen made a pledge to support expanding the direct intelligence capabilities of the fire service, both as recipients and suppliers of information. This was reiterated by I&A representatives at subsequent FSIE meetings. Consistently, during the initial phases of the FSIE, I&A was an advocate for greater fire representation within fusion centers. As a member of the U.S. Intelligence Community (IC), I&A worked with the IC to see fusion centers and the fire departments connect as both customers and as valuable sources of information, and for public safety departments to view the IC as a resource and a partner.

As a result of the initial FSIE conference, two working groups were formed. One working group was established to work on the governance of how the fire service and the federal government would communicate. The Governance Working Group was comprised of a seven-department steering committee. The Governance Working Group also monitored network governance developments necessary to renovate existing DHS computer-based communication channels and technological tools to allow secure information and intelligence sharing portals for the fire service community. The second,

Requirements Working Group addressed the information/intelligence requirements for the fire service. The Requirements Working Group was also structured as a seven-department steering committee. The requirements group oversaw the development of national intelligence requirements for the fire service community. The committee identified information/intelligence needs, the critical information required to protect the homeland from national strategic threats, and they determined what information/intelligence fire departments need to know in order to prepare for and safely respond to incidents of an all hazards /all crimes nature. Later in the year, a third working group was added—the Training Development Working Group. This group was tasked with working on the development of training specifically for fire service in intelligence and information sharing. This group's efforts eventually lead to fire service Terrorism Liaison Officer training programs.

C. A BRIEF HISTORY OF FIRE SERVICE INTELLIGENCE

In the time since the 2007 FSIE conference, subsequent conferences and meetings were conducted. A continued commitment was exhibited by major decision makers from the fire service, U.S. Department of Homeland Security (DHS) and other stakeholders discussed information/ intelligence needs, shared best practices, and realized the need to achieve consensus on protocols for information sharing within the fire service community. As a result, the following documents were developed:

- FSIE Concept Plan
- FSIE National Strategy 2008
- FSIE Fact sheet
- FSIE Intelligence Requirements
- Fire Service Integration added as an appendix to the Baseline Capabilities for Fusion Centers

By 2010, the groundwork had been laid and a foundation built for the expansion of the FSIE throughout the fire service. At this point, the focus shifted away from fire departments and toward professional/political/lobbying organizations. The FSIE advisory

group was then formed and fire department representation in the process was reduced from 15 to four fire departments (See Figure 1).[2] At this point, the formal FSIE dissolved. In addition to waning support, other factors that led to the dissolution of the formal FSIE were:

- Decreased ability to maintain engagement due to budgetary concerns
- Attrition/promotion of committee members and key advocates within I&A
- Inability to achieve consensus as to incorporation of other aspects of the fire service, such as:
    - Volunteer fire departments
    - Mutual aid organizations
    - Fire departments outside mega regions
    - Privately operated fire departments
    - The role of the Emergency Medical Service (EMS), with a disparate and diverse system similar to the fire service
        - Relegation of the original FSIE to working group status
        - Formation of a new FSIE Advisory Group (See Chart Below) that replaced fire departments with organizations that had no nexus to intelligence or street operations, such as the National Fire Protection Association and the National Association of State Fire Marshals

Through the passage of time and a maturing of the fusion process, which was in its infancy during the operation of the FSIE, the opportunity now exists for a renewed commitment from I&A and the fire service to revisit the FSIE.

[2] United States Fire Administration. *FSIE Fact Sheet.* Washington, D.C., 2010.

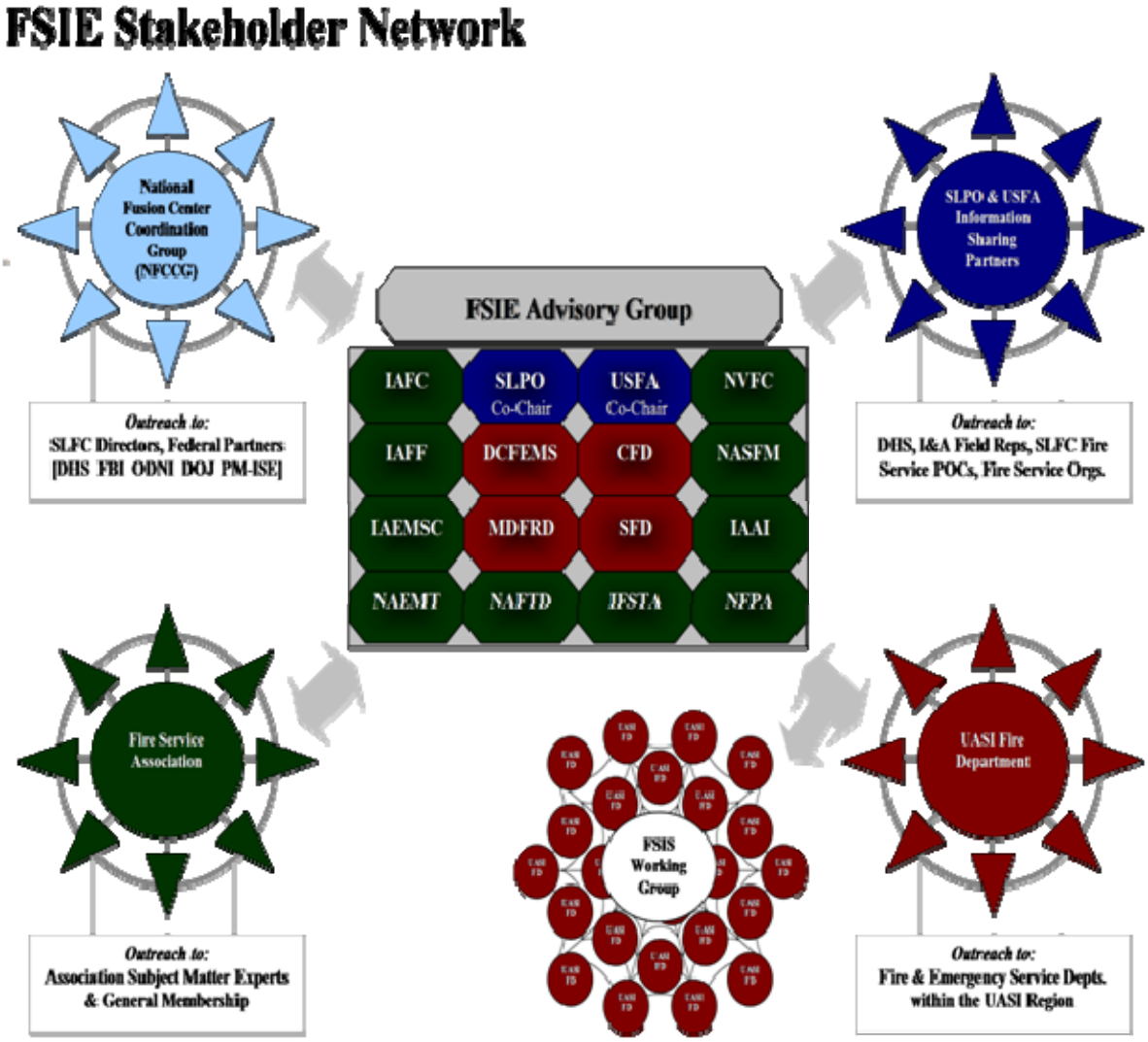

Figure 1. Last Formal Structure of FSIE.

II. LITERATURE REVIEW

In looking at domestic intelligence sharing on the local level and outside law enforcement entities, there are three main areas of literature. The first area of literature to be examined is the fundamentals of intelligence. The second area is the structure of domestic intelligence apparatus. The third area is a delineation of the existing mechanisms of dissemination of the intelligence and intelligence products with state and local government.

A. INTELLIGENCE FUNDAMENTALS

A view of the overall collection, analysis and dissemination of intelligence by government is presented in ten (10) articles contained in volume one (1) of Strategic Intelligence: Understanding the Hidden Side of Government.[3] In addition to articles relating to the history and state of intelligence in the United States, articles also examine the United Kingdom and Canada. To supplement the articles provided in this volume, primary intelligence documents and information are provided in the Appendix, such as:

- The National Security Act of 1947
- Leadership of the U.S. Intelligence Community 1047-2006
- The Aspin-Brown Commission on the Purpose and Challenges of Intelligence

In the introduction to intelligence studies literature, several fundamentals of intelligence are addressed. Collection of intelligence is explored in explaining the "Ints" of intelligence.[4]

- TECHINT – Technical intelligence from satellites and reconnaissance airplanes
- HUMINT – Classic espionage through human intelligence

[3] Lock K. Johnson, ed. *Strategic Intelligence: Understanding the Hidden Side of Government.* Vol. 1. Westport, CT: Praeger Security International, 2007.

[4] Ibid., 4.

- OSINT – Open source intelligence from open literature such as newspapers
- SIGINT – Signals intelligence from capturing communications from one person to another

The analysis of intelligence is next touched upon. Analysis "brings insight to information that has been collected and processed."[5] After information is analyzed, the information is disseminated. Dissemination, for purposes of this thesis, refers to the passing of information to policy officials.[6] In terms of SLT, intelligence dissemination is the delivery of intelligence to first response organizations. Traditionally, the first response organizations that receive intelligence are law enforcement, organizations with formal relationships with groups, such as the JTTF, and fire departments with personal relationships, or fire departments who have developed their own intelligence integration system (with sponsorship).From the research, first response and public safety organizations that have no discernible intelligence integration are public health and emergency management.

This information represents the basic functions of intelligence for the national umbrella under which the SLT intelligence apparatus exist. Figure 2shows where the federal intelligence apparatus falls under the Director of National Intelligence (DNI).

[5] Lock K. Johnson, ed. *Strategic Intelligence: Understanding the Hidden Side of Government.* Vol. 1. Westport, CT: Praeger Security International, 2007, 5.

[6] Ibid.

Figure 2. The Members of the Intelligence Community Grouped by Program Managers, Department, and Service.

The national intelligence enterprise and intelligence community was recently explained in an overview presented to the 111th Congress.[7] The DNI is the head of the U.S. intelligence community (IC) and principal advisor to the President on intelligence issues.[8] The U.S. IC consists of the:

- Central Intelligence Agency (CIA)
- Defense Intelligence Agency (DIA)
- Department of Justice (DOJ) Federal Bureau of Investigation (FBI)
- National Geospatial Intelligence Agency (NGA)

[7] Intelligence, Office of the Director of National. "http://www.dni.gov/overview.pdf." 2009. (accessed October 2011).

[8] Ibid., 1.

- National Reconnaissance Office (NRO)
- National Security Agency (NSA)
- DOJ – Drug Enforcement Administration (DEA) Office of National Security Intelligence (ONSI)
- Department of Energy (DoE) – Office of Intelligence and Counter Intelligence
- Department of Homeland Security (DHS) – Office of Intelligence and Analysis (I&A)
- Department of State – Bureau of Intelligence and Research (INR)
- Department of the Treasury – Office of Intelligence and Analysis (OIA)
- U.S. Army
- U.S. Navy
- U.S. Air Force (USAF)
- U.S. Marine Corps (USMC)
- DHS – U.S. Coast Guard (USCG)

In addition to the intelligence community the Congressional briefing also presents the DNI's ten (10) functions that support the IC.[9]

- National Counterterrorism Center (NCTC)
- National Counterintelligence Executive (NCIX)
- National Counter proliferation Center (NCPC)
- The Special Security Center (SSC)
- The National Intelligence University (NIU)
- Intelligence Advanced Research Projects Activity (IARPA)
- The Center for Security Evaluation's (CSE)

[9] Intelligence, Office of the Director of National. "http://www.dni.gov/overview.pdf." 2009. (accessed October 2011), 2–3.

- The National Intelligence Council (NIC)
- The National Intelligence Coordination Center (NIC-C)
- The Mission Support Center

Under this framework, DHS I&A is designated to "work closely with state, local, tribal, and private sector partners."[10] Therefore, under the IC framework, DHS I&A will be the primary source for IC interaction with SLC for purposes of this thesis. The intelligence from the above groups and agencies is what is placed into the funnel that feeds domestic intelligence consumers. The spigot to the funnel is controlled by DHS I&A and the FBI.

B. DOMESTIC INTELLIGENCE APPARATUS

"DHS tasked as primary source of information for state and local partners," and has had an intelligence component since DHS's 2003 inception.[11] Intelligence elements in six (6) DHS components existed upon formation:

- U.S. Customs and Border Protection (CBP),
- U.S. Immigration and Customs Enforcement (ICE),
- U.S. Citizenship and Immigration Services (USCIS),
- The Transportation Security Administration (TSA),
- U.S. Coast Guard (USCG), and
- U.S. Secret Service.

DHS Intelligence & Analysis (I&A) was formed by Secretary Chertoff during the 2005 reorganization, "to ensure that information related to homeland security threats is

[10] Intelligence, Office of the Director of National. "http://www.dni.gov/overview.pdf." 2009. (accessed October 2011), 15.

[11] Mark A. Randol, *The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress.* Washington, D.C.: Congressional Research Service, May 27, 2009. 1.

collected, analyzed, and disseminated to the full spectrum of homeland security customers in the department, at state, local, and tribal levels, in the private sector and in the Intelligence Community (IC)."[12]

The author assesses DHS's state and local effort by citing the journal *Homeland Security Affairs*, "[t]he Department had become 'irrelevant' to states and localities as a source of intelligence because that intelligence lacks timeliness and adds so little value to local terrorism efforts. In addition, "the stream of intelligence from DHS is useless ... discussions at the pilot sites, that the quality of intelligence support in the wake of critical domestic and international homeland security-related incidents is a top priority for state and local fusion center leaders and a key determinant of how they evaluate DHS analytic support."[13] An example of this is the obvious holiday warnings. No universal standards for fire service integration make it difficult to judge the effectiveness of information sharing because people do not know what they do not know. Another example of this is the "intelligence spam," which has been a common observation of intelligence consumers. The amount of primary documents from DHS regarding information sharing is voluminous but rarely delineates policy regarding intelligence sharing outside of law enforcement. Although universal intelligence sharing has long been a stated goal, there are no clearly articulated steps to achieving that goal.

1. DHS Intelligence Functions

Congress makes information sharing a top priority as Randol cited Homeland Security Act of 2002, Intelligence Reform and Terrorism Prevention Act of 2004, and the Implementing Recommendations of the 9/11 Commission Act of 2007. In addition, Randol correctly points out that intelligence is not only about spies and satellites. Intelligence is about the thousands and thousands of routine, everyday observations and activities. Ergo the importance of "See Something Say Something" and engaging disciplines outside law enforcement.

---

[12] Mark A. Randol, *The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress.* Washington, D.C.: Congressional Research Service, May 27, 2009, 4.

[13] Ibid., 12.

In addition, this article lists DHS I&A products and their purposes along with a brief description of the National Operations Center (NOC) establishing the NOC as the primary national level hub for domestic incident management, operations coordination, and situational awareness. The NOC is staffed by numerous federal, state, and local agencies and fuses law enforcement, national intelligence, emergency response and private sector reporting. [14]

In writing about DHS I&A, each component is addressed including the Office of the Deputy Under Secretary for Field Operations (DU/S-F) State and Local Program Office (SLPO), under which falls the Fusion Center Program intelligence officers.[15] This article further supplies the definition of a fusion center as "collaborative effort of two or more federal, state, local, or tribal government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity"[16]

The article continues by laying out the intelligence functions of the DHS divisions. Looking specifically at:

- Operations Coordination and Planning Directorate (OPS)—Intelligence Division
- U.S. Customs and Border Protection (CBP) Intelligence Element
    - CBP Office of Intelligence and Operations Coordination (OIOC)
    - National Targeting Center (NTC) (Legacy of U.S. Customs Service)
    - Border Field Intelligence Center (BORFIC)
    - Air and Marine Operations Center (AMOC)
        - U.S. Citizenship and Immigration Services (USCIS) - Intelligence Element

[14] Mark A. Randol, *The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress.* Washington, D.C.: Congressional Research Service, May 27, 2009, 10.

[15] Ibid., 15.

[16] "P.L. 110-53, §511, 121 STAT. 322." n.d.

- Transportation Security Administration (TSA) TSA Office of Intelligence (TSA-OI)
- The U.S. Coast Guard (USCG) Intelligence Element
- Cryptologic
- Protective Intelligence and Assessment Division (PID) - USSS

Finally, DHS formal intelligence is shown to include the No Fly and Selectee Lists. The "No Fly" and "Selectee" lists are subsets of the TSDB that are used to screen air travelers. The "No Fly" list contains the names of individuals who are prohibited from boarding an aircraft "based on the totality of information, as representing a threat to commit an act of "international terrorism" or "domestic terrorism" (as defined in 18 U.S.C. 2331).[17]

Overall, this is a good summary of the DHS intelligence functions. This is an excellent background piece, yet very little analysis is presented in the reading. Each of the different missions of the DHS divisions can be assumed to produce a disparate number of intelligence requirements. The differing intelligence requirements more than justify the large number of distinct intelligence shops contained within DHS. What would have tied this article together better would have been to lay out the structure of DHS intelligence, as was done well, and then provide greater detail on how I&A brings all this information together and interacts with SLT entities.

C. STATE AND LOCAL INTELLIGENCE SHARING

The literature regarding state and local intelligence sharing is primarily law enforcement focused. In addition, most of the primary documents regarding this area are DOJ based. Opinions arguments and theories for intelligence sharing expansion beyond law enforcement (e.g., fire service, public health) have come in the form of articles and

[17] Mark A. Randol, *The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress.* Washington, D.C.: Congressional Research Service, May 27, 2009, 38.

prior thesis work. Although there is mention of fire service integration in some of the articles examined, there is no clear uniform policy or model promulgated from the IC regarding this issue.

The information sharing policy for the IC was promulgated in a strategic document from the DNI.[18] This document articulates the information sharing mission, key concepts, goals and objectives. Fostering information sharing is mandated of the DNI, as per the Intelligence Reform and Terrorism Prevention Act of 2004.[19] The DNI's articulated information sharing mission for the IC is "Improve responsible, secure information sharing across the Intelligence Community and with external partners and customers."[20] Below is the DNI's information sharing goals:[21]

1. Optimize the Sharing of Information and Intelligence within the IC and with Partners and Customers to Enable Decision Advantage
2. Maximize and Integrate IC Capabilities to Discover, Access, Retain, Store, Share, and Exploit Information
3. Maximize and Integrate IC Capabilities to Secure Information
4. Review, Align, and Strengthen the Governance Framework to Optimize Responsible Information Sharing, while Protecting Civil Liberties and Privacy
5. Promote a Culture of Responsible Information Sharing

Goal one (1), **"**Optimize the Sharing of Information and Intelligence within the IC and with Partners and Customers to Enable Decision Advantage," is directly germane to this thesis as goal one (1) seeks to understand the intelligence needs of SLT entities and directs the IC to address those needs. Addressing SLT needs can be achieved, per the DNI, through meeting the following objectives**:**[22]

---

[18] *United States Intelligence Community: Strategic Intent for Information Sharing 2011-2015.* Washington, D.C.: Office of the Director of National Intelligence, 2011.

[19] 50 USC 403–103(g).

[20] Ibid., ii.

[21] Ibid., 2–3.

[22] Ibid., 2.

1.1. Identify, validate and address IC, partner, and customer information sharing needs

1.2. Manage IC, partner, and customer sharing relationships

1.3. Identify, acquire, and provide relevant information both inside and outside the IC to improve decision advantage

1.4. Leverage information sharing capabilities of customers and partners for use by the IC

In light of fusion, and the goal under which the objectives above are meant to address partners and customers, they will be assumed to be various SLT entities. Furthermore, by virtue of the fact that this document is from the DNI, this mission, these goals, and each goal's objectives are the controlling doctrine for national intelligence and information sharing across the entire IC.

Testimony regarding the DHS I&A SLT information sharing environment (ISE) was given in October of 2011, by Eileen R. Laurence Director, Homeland Security and Justice Issues. Subsequent to this testimony, the U.S. General Accounting Office (GAO) issued a report.[23] In its summary of the testimony the GAO wrote,

> In response to its mission to share information with state and local partners, DHS's Office of Intelligence and Analysis (I&A) has taken steps to identify these partner's information needs, develop related intelligence products, and obtain more feedback on its products. I&A also provides a number of services to its state and local partners that were generally well received by the state and local officials we contacted. However, I&A has not yet defined how it plans to meet its state and local mission by identifying and documenting the specific programs and activities that are most important for executing this mission. The office also has not developed performance measures that would allow I&A to demonstrate the expected outcomes and effectiveness of state and local programs and activities. In December 2010, GAO recommended that I&A address these issues, which could help it, make resource decisions and provide accountability over its efforts.[24]

[23] *Information Sharing: Progress Made and Challenges Remaining in Sharing Terrorism-Related Information.* Statement for the Record To the Committee on Homeland Security and Governmental Affairs, U.S. Senate, United States Government Accountability Office, Washington, D.C.: GAO, October 2011.

[24] Ibid., 1.

This document points out on numerous occasions that SLT information sharing's focus is solely based on Fusion Centers and law enforcement, "Consistent with the Intelligence Reform Act, the ISE is to provide the means for sharing terrorism-related information across five communities—homeland security, law enforcement, defense, foreign affairs, and intelligence—in a manner that, among other things, leverages ongoing efforts."[25] This approach ignores not only the totality of first response organizations but also private sector stakeholders (e.g., owners and operators of critical infrastructure), and other government stakeholders (e.g., public health). In addition, the GAO illuminates efforts to bolster fusion centers with collaboration from the DOJ.[26] Fusion centers are further discussed in terms of maintaining operations, in light of budget constraints, with additional grant funding, training, and technical assistance from DHS.[27] Finally, this report acknowledges that thirty-seven (37) of the seventy-two (72) recognized fusion centers fail to meet the designated fusion center baseline capabilities, designed primarily to meet local law enforcement needs.[28]

The Interagency Threat Assessment and Coordination Group (ITACG) operates out of the National Counterterrorism Center (NCTC) to coordinate the dissemination of information from DHS and DOJ to SLT entities within the homeland security enterprise. In 2009, the ITACG published an intelligence guide for first responders "to assist state, local, tribal law enforcement, firefighting, homeland security, and appropriate private sector personnel in accessing and understanding federal counterterrorism, homeland security, and weapons of mass destruction intelligence reporting."[29] This guide is a basic guide crafted for all disciplines and provides baseline information or an introduction, for those new to intelligence, of the basic concepts, jargon, and facets of intelligence and the intelligence community.

---

[25] *Information Sharing: Progress Made and Challenges Remaining in Sharing Terrorism-Related Information.* Statement for the Record To the Committee on Homeland Security and Governmental Affairs, U.S. Senate, United States Government Accountability Office, Washington, D.C.: GAO, October 2011, 6.

[26] Ibid., 9.

[27] Ibid., 10.

[28] Ibid., 12.

[29] *Interagency Threat Assessment and Coordination Group (ITACG) Intelligence Guide for Firest Responders.* Washington, D.C.: National Counterterrorism Center, 2009, 10.

After intelligence sources are explained the Intelligence Community (IC) and the activities of the IC are presented. Intelligence sources and the IC are built upon with an explanation of the intelligence cycle:[30]

1. Planning and Direction: Establishing the intelligence requirements of the policymakers – the President, the National Security Council, military commanders, and other officials in major departments and governmental agencies.

2. Collection: Gathering of raw data from which finished intelligence is produced.

3. Processing and Exploitation: Conversion of large amounts of data to a form suitable for the production of finished intelligence; includes translations, decryption, and interpretation of information stored on film and magnetic media through the use of highly refined photographic and electronic processes.

4. Analysis and Production: Integration, evaluation, and analysis of all available data and the preparation of a variety of intelligence products, including timely, single-source, event-oriented reports and longer term, all-source, finished intelligence studies.

5. Dissemination: Delivering the products to consumers who request them.

The ITACG Guide then delivers the five (5) categories of finished intelligence:[31]

1. Current intelligence

2. Estimative intelligence

3. Warning intelligence

4. Research intelligence

5. Scientific and technical intelligence

[30] *Interagency Threat Assessment and Coordination Group (ITACG) Intelligence Guide for Firest Responders.* Washington, D.C.: National Counterterrorism Center, 2009, 18–19.

[31] Ibid., 20–22.

The second section of the ITACG Guide is dedicated to the handling of Controlled Unclassified Information (CUI). This is important to public safety personnel new to receiving information from official sources. The reason why this section is important to new intelligence/information recipients is that CUI may be commonly available to responders on all level of an organization. Having information widely distributed increases the chance for misuse as CUI, does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is pertinent to the national interests of the United States or to the important interests of entities outside the federal government, and under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. CUI includes many caveats, such as "FOR OFFICIAL USE ONLY" (FOUO).[32]

In addition, this section makes the important designation that FOUO is not a classification akin to "Secret," but a designation as to how a document or the information therein should be disseminated or controlled. FOUO information is not for the public but can be given to others with the approval of the originating agency.[33] Further in the CUI explanation a definition of need-to-know is given. Need-to-know is defined by the ITACG as, "the determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to perform or assist in the lawful and authorized governmental function, i.e., access is required for the performance of official duties."[34] Finally, the CUI section only FOUO is presented as a universal information caveat, although individual agency created caveats, such as Law Enforcement Sensitive (LES) and Official Use Only (OUO) are acknowledged as being used and possibly having additional requirements, as determined by the agency assigning a LES or OUO caveat.[35] The fact that these additional designations are acknowledged but

---

[32] *Interagency Threat Assessment and Coordination Group (ITACG) Intelligence Guide for Firest Responders.* Washington, D.C.: National Counterterrorism Center, 2009, 26.

[33] Ibid.

[34] Ibid., 27.

[35] Ibid.

not explicitly endorsed is interesting in that the question becomes—was this a deliberate omission as LES and OUO could be viewed as a method one discipline could use to insulate information from other disciplines?

Next, the ITACG Guide addresses security clearances. Clearance needs, levels, grantors and basic procedures are presented. After clearances are addressed, the utility of intelligence is presented. Intelligence utility is presented as what intelligence can do and what intelligence cannot do. What intelligence can do is described as:[36]

- Providing decision advantage, by improving the decision-making of consumers and partners while hindering that of our enemies.
- Warning of potential threats.
- Insight into key current events.
- Situational awareness.
- Long-term strategic assessments on issues of ongoing interest.
- Assistance in preparation for senior-level meetings that include national security-related subjects.
- Pre-travel security overviews and support.
- Reports on specific topics, either as part of ongoing reporting or upon request for short-term needs.
- Compiling U.S. government knowledge on persons of interest.

What intelligence cannot do is presented as intelligence cannot violate U.S. law and intelligence cannot predict the future.[37]

Intelligence products for first responders are the next topic of the ITACG Guide. The intelligence product section lists both classified and unclassified products and information sources and is divided by report type. Examples of situational awareness, threat reporting sources, and information portals are unclassified, such as HSIN, LEO,

[36] *Interagency Threat Assessment and Coordination Group (ITACG) Intelligence Guide for Firest Responders.* Washington, D.C.: National Counterterrorism Center, 2009, 34.

[37] Ibid., 35.

Intelink-U, RISSNET, TRIPwire, FPS Portal, and Open Source Center (OSC) or Secret, such as NCTC Online—Secret (NOL-S), Office of Intelligence and Analysis (OI&A) webpage, FBINet, and FBI Intelink/SIPRNet.[38] Information report examples are Intelligence Information Report (IIR) and Homeland Information Report (HIR).[39] Other information examples given are:[40]

- Intelligence Assessment (IA)
- Threat Assessment (TA)
- Special assessment (SA)
- Intelligence Bulletin (IB)
- Roll Call Release
- Terrorism Summary (TERRSUM)

What each information example contains is given; along with variations on information types (e.g., IAs and IBs can be joint and written by multiple agencies). This leads to the next section of the Guide that addresses how to understand information received, from all sources and how to understand language used in intelligence documents. Understanding intelligence writing, language used, and why certain writing types and language are used is extremely important to any person new to intelligence. The guide then concludes with a dictionary of intelligence terms and a list of common intelligence acronyms.

The value of this guide is that the inclusion of new disciplines into the intelligence cycle. Consumers and providers of information/intelligence will gain a broader perspective through familiarization of content. The ITACG's guide is a good baseline for the uninitiated from any discipline due to the general information given and lack of any particular imbedded biases toward any one discipline or group through discipline specific

---

[38] *Interagency Threat Assessment and Coordination Group (ITACG) Intelligence Guide for Firest Responders.* Washington, D.C.: National Counterterrorism Center, 2009, 38, 45–46.

[39] Ibid.

[40] Ibid., 39.

jargon, examples, or pre-established discipline based information access restrictions. Finally, it is ironic that for all of DHS's edicts regarding information sharing the documents addressing fire service integration into intelligence came from the DOJ.[41]

As a result of the number of academic works and theses addressing the topic of information sharing and the information above, this thesis will attempt to advance both theory and practice by identifying the next steps required to develop a national standard and general framework for intelligence sharing with the fire service. All of this information shows the frameworks in place for information sharing. In light of all of these systems, programs, inputs, and outputs, there remains no clear method for inclusion of the fire service into domestic information and intelligence sharing. Yet, all of the information above show that avenues for information sharing exist and the rules/policies/procedures the fire service will need to follow. This thesis will show how this can be leveraged by the fire service to allow for information and intelligence sharing across the fire service.

[41] Justice, United States, Department of "Fire Service Integration for Fusion Centers: An Appendix to the Baseline Capabilities for State and Major Urban Area Fusion Centers." April 2010, 18.

III. RESEARCH METHOD

For this thesis, a new concept is being proposed for information/intelligence sharing between U.S. domestic intelligence and the fire service. This new concept is based upon the lessons learned from and previous efforts of the Fire Service Intelligence Enterprise (FSIE). This new concept will provide guidance for local fire departments to gain access to and provide information/intelligence to U.S. domestic intelligence.

To build the integration concept, this thesis looks at how the federal domestic intelligence framework addresses the fire service. In addition, specific policies to foster intelligence sharing across the entire fire service and the differences between policies and/or achieved/unachieved goals will be examined. Federal frameworks are important, as national intelligence efforts are led by the federal government. Looking to these frameworks using appreciative inquiry is the foundation upon which any fire service solution will be based for not only successful integration, but to also maintain continuity within the domestic intelligence enterprise. As a result of this examination, a new avenue for fire service integration will be recommended for development and implementation.

Furthermore, in looking at smart practices and policy documents, the following questions focused the research:

1. How can the fire service as a whole be integrated into the domestic intelligence community?
    a. What is the current framework of domestic intelligence sharing?
    b. What is the current framework for integrating the fire service into domestic intelligence sharing?
    c. Is a national solution the best answer?
    d. How comprehensive should a national solution be?
2. What is the future of intelligence sharing with the fire service?
    a. What is the role of technology?
    b. What role does suspicious activity reporting play?

With these questions in mind, policies and plans related to intelligence sharing with SLT entities were examined and compared. In addition, current trends and information relating to how intelligence and information is currently shared among fire departments and with members of the IC and nodes, such as fusion centers, was part of the research.

IV. DISCUSSION

Currently there is no uniform system for information/intelligence sharing throughout the entire fire service. As a result, different methods of information/intelligence sharing exist, with no concerted effort of outreach across departments is in practice.

A. WHY IS THE FIRE SERVICE IMPORTANT IN INTELLIGENCE?

1. General Advantages of Information Sharing

Consistently when speaking of or about information/intelligence sharing with the fire service the question "why" is usually raised. This is a question that begs answering for not only the fire service but other groups, public and private sector, with public safety responsibilities. In the following list of advantages of sharing information, one could make an argument of replacing "fire" with emergency management or public health:

- **Increased Public Safety** by making timely, accurate and complete public safety information available to all fire service decision makers.
- **Improved Accuracy** of information by having data available to all fire services.
- **Implement information-driven and risk-based detection,** prevention, deterrence, response, protection and emergency management efforts.
- **Identify** rapidly both immediate and long-term threats.[42]

In addition to the fire specific justification presented in the fire service appendix to the *Baseline Capabilities for State and Major Urban Area Fusion Center,s* the Interagency Threat Assessment and Coordination Group (ITACG) also listed the advantages to fire service information sharing.

[42] Group, Interagency Threat Assessment and Coordination. "Intelligence Guide for First Responders." 2nd Edition, Washington, D.C., 2011, 8–9.

2. Advantages to Fire Service Information Sharing

As our Nation's first "preventers and responders," along with being the primary first mitigators of most domestic emergencies and incidents, fire service personnel are critical to our efforts to protect the homeland and to respond if an incident occurs. The fire service must have access to the information that enables them to protect our local communities. In addition, fire officials are often best able to identify potential threats or anomalies that exist within their jurisdictions. The fire service has a high degree of personal interaction with the public and an acute situational awareness within the communities they serve. The fire service is a full and trusted partner with the federal government in our Nation's efforts to protect and respond to incidents involving our nation's critical infrastructure, and therefore, they must be a part of an information sharing framework that supports an effective and efficient two-way flow of information enabling officials at all levels of government to counter and respond to threats.

a. Fire Service Public Interaction and Education

The role the fire service plays in fire prevention and public education can include the enforcement of building codes through inspections. This and other fire prevention functions allow the fire service to gain access to information not commonly possessed by other members of the homeland security enterprise (e.g., floor plans, inventories of hazardous materials, and building occupants). Public education allows the fire service an avenue for public interaction to disseminate information, and gain valuable insight to the community and how to best serve the community. An example of a national public education program, as it applies to information collection is "see something say something." "See something say something's purpose is to raise public awareness of indicators of terrorism and terrorism-related crime, and to emphasize the importance of reporting suspicious activity to the proper local law enforcement authorities."[43]

[43] *United States Department of Homeland Security*, n.d. http://www.dhs.gov/if-you-see-something-say-something-campaign (accessed August 22, 2012).

b. Fire Service Public Interactions via EMS

The fire service and fire departments with integrated EMS respond to hundreds of thousands of response calls a year, resulting in contact with people and dwellings not covered by fire prevention code enforcement. In addition, these EMS assets would be the first to detect the signs and symptoms of chemical or biological attacks, if those attacks are not self-announcing or clandestine in nature.

c. How Information Sharing Benefits the Fire Service

The fire service can both provide information and intelligence to the IC and benefit from information and intelligence disseminated from the IC. In their "Intelligence Guide for first Responders," the Interagency Threat Assessment and Coordination Group (ITACG) espoused eight (8) points of what intelligence can do or provide.[44] Point one reads, "Decision advantage, by presenting information and analysis that can improve the decision-making process for consumers and partners while hindering that of our enemies."[45] In planning for preplanned events, and self-announcing incidents (an incident that can be foreseen as possibly occurring with the time and/or date of occurrence being completely spontaneous.), day-to-day operations, and incident mitigation; additional information and knowledge, coupled with experience, can alter decisions and actions, while improving outcomes. This "decision advantage" in terms of self-announcing incidents leads to another attribute of intelligence—"Situational Awareness."[46] Situational awareness is important for fire departments to know the whole picture not only for mitigation but also indicators of terrorist activity. Indicators can present in any number of ways from an EMS call, while conducting a fire prevention inspection, fire company response district familiarization, or a fire company performing target hazard assessments.

---

[44] Group, Interagency Threat Assessment and Coordination. "Intelligence Guide for First Responders." 2nd Edition, Washington, D.C., 2011, 8–9.

[45] Ibid.

[46] Ibid.

The importance of situational awareness is also clearly articulated by the first fire department to delve into the issue of why the fire service has a need for access to information/intelligence from? the Fire Department of New York City. In the FDNY Terrorism and Disaster Preparedness Strategy, the importance of situational awareness reads as such, "Real-time intelligence and information lead to a heightened state of situational awareness, which is imperative in both the planning and responding stages of operations. In reaction to information gathered and based on the type of intelligence received, the FDNY can increase inspection activity to assist in detection or strategically locate additional resources to act as a terrorism deterrent."[47] In addition, as many other documents have been written about this topic, a recent thesis on the subject of situational awareness writes "Through the sharing of pre-incident information and intelligence, and real-time incident updates, situational awareness will be enhanced to support both local fire departments and DHS's preparedness efforts. Rapid and comprehensive information sharing will also be imperative to establishing a common operational picture on the local and national levels during a major incident."[48]

d. Benefits to Planning and Training

In addition, four things intelligence can "do" that affects fire service planning and training are, "Warning of potential threats, Insight into key current events, Long-term strategic assessments on issues of ongoing interest, Reports on specific topics, either as part of ongoing reporting or upon request for short-term needs."[49]Intelligence involving those topics can affect long-term fire service training as to what CBRNE methods should members be trained to mitigate, based on threats. In addition, what potential targets within a fire department's jurisdiction can be derived based on current events. Furthermore, reports on specific topic can be included with germane training evolutions and/or documents.

---

[47] Fire Department City of New York, "Terrorism and Disaster Preparedness Strategy." New York, New York, 2007, 20.

[48] Rosemary Cloud, "Future Role of Fire Service in Homeland Security." Monterey, California: Naval Postgraduate School, September 2008.

[49] Group, Interagency Threat Assessment and Coordination. "Intelligence Guide for First Responders." 2nd Edition, Washington, D.C., 2011, 8–9.

Of the ODNI's points, as restated by the ITACG, of what intelligence can do, two of the points apply: (1) "Pre-travel security overviews and support, and (2) Knowledge on persons of interest involve either someone's personal information or travel do not support the value that can be added by intelligence to the fire service.[50] Both personal information and travel alerts do not fall clearly into the operations or mission of the fire service.

An example of using information, not intelligence, comes in the form of what focus limited planning resources would have. By way of example, the annual worldwide threat assessment from the Director of National Intelligence stated: "The IC judges that lone actors abroad or in the United States—including criminals and homegrown violent extremists (HVEs) inspired by terrorist leaders or literature advocating use of CBR materials—are capable of conducting at least limited attacks in the next year, but we assess the anthrax threat to the United States by lone actors is low."[51] In light of this statement, a fire department may, if faced with a choice between where to focus planning over the next year, choose to focus more on CBR as opposed to anthrax, if after a threat analysis HVE has a history and/or is rated high in as a threat to their jurisdiction.

3. What Intelligence Cannot Do for the Fire Service

Just as those outside of the fire service can learn about the value added to information/intelligence sharing, the fire service needs to understand what the access to intelligence cannot necessarily provide or solve. Access to security clearances in order to access intelligence related products is a complicated process, bound by rules and limited by policies that require need-to-know information, in addition to the means by which it was collected and sourced. That burden of responsibility cannot be equally shared across the service. Just as there are things that intelligence can do, there are things that

[50] Group, Interagency Threat Assessment and Coordination. "Intelligence Guide for First Responders." 2nd Edition, Washington, D.C., 2011, 8–9.

[51] James R. Clapper, "Unclassified Statement for the Record on the Worldwide Threat Assessment of the U.S. Intelligence Community for theSenate Select Committee on Intelligence." *Statement for the Record.*Washington, D.C., January 31, 2012, 2.

intelligence cannot do. The ODNI stressed that the things intelligence cannot do list reflects that, "Realistic expectations will help consumers fill their intelligence needs."[52] Realistic expectations are important for not only current consumers of intelligence but future consumers of intelligence. Understanding the limitations of access to intelligence related products is a fundamental first step towards eliminating misperceptions; and developing a realistic, operationally sound practice for the fire service. For example: Intelligence, cannot:

- Predict the future. Intelligence can provide assessments of likely scenarios or developments, but there is no way to predict what will happen with absolute certainty.

- Violate U.S. law. The activities of the Intelligence Community (IC) must be conducted consistent with all applicable laws and executive orders, to include the National Security Act of 1947, as amended; the Foreign Intelligence Surveillance Act; the Intelligence Reform and Terrorism Prevention Act (IRTPA); the Privacy Act of 1974; the Detainee Treatment Act; Homeland Security Act of 2002, as amended; Executive Order 12333; and the Military Commission Act.[53]

B. INTEGRATION APPROACHES

In terms of the United States IC, which approaches intelligence from a national strategic perspective, 30,000 feet above what applies to the first fire engine arriving at a fire, "Homeland security intelligence could be viewed as primarily a federal activity."[54] Under this strictly federally structured, and statutorily mandated, approach; "Geography is not as important …, as the federal entities that engage in homeland security intelligence may, directly or indirectly, collect information outside the United States."[55] As this discussion examines collection and dissemination of information on a local level, there are two possible approaches, as written by Todd Masse in a document for the

---

[52] Office of the Director of National Intelligence. "U.S. National Intelligence: An Overview 2011." Washington, D.C., 2011, 40.

[53] Group, Interagency Threat Assessment and Coordination. "Intelligence Guide for First Responders." 2nd Edition, Washington, D.C., 2011, 8–9.

[54] Todd Masse, *Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches.* Washington, D.C.: Congressional Research Service, 2006, 16.

[55] Ibid.

Congressional Research Service, titled "*Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches.*"[56] Those approaches are the Geographic Approach and the Holistic Approach.

1. Geographic Approach to Integration

Under the Geographic Approach, Masse opines: "Homeland security intelligence can be viewed, some might argue rather simplistically, in geographic and federal/state/local government terms. That is, if the intelligence collection activity takes place within the United States—whether it be by a federal agency or a state, local, tribal, or private sector actor, it would be considered HSINT."[57] Under this approach, fire service information/intelligence sharing governance and/or structure would be governed strictly by political division and subdivision. Although the geographic approach is a good method for integration of small and medium sized fire departments, by using a regional concept, this method in and of itself may not best serve the fire service. Portions of the fire service exist that have no allegiance to one political subdivision, for example, fire protection districts and mutual aid organizations. Fire departments are found to be formed on the county level of government, municipal level of government, township level, and by agreed upon compact. Fire departments arising out of agreed upon compacts are the result of units of government that decide to share responsibility of funding fire protection and form a fire protection district. The fire protection district is responsible to a board and not one particular unit of government. Fire departments have a diverse number of possible political organs that could have formed a particular department. A fire department can even respond to or be responsible for areas that house different fusion centers, and or, include more than one state, as a result of mutual aid responsibilities. As a result of no universal political governance structure that would be applicable to all fire departments, elected political subdivisions may not be adequate as a

---

56 Todd Masse, *Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches.* Washington, D.C.: Congressional Research Service, 2006, 15.

57 Ibid.

sole means to address information and intelligence sharing integration. As a result, the FEMA Regions should take a more active role in integrating the fire service into information/intelligence sharing.

2. Holistic Approach to Integration

Masse's Holistic Approach ignores political implications entirely and their geographic constraints as he writes, "Under this approach, HSINT is not bounded by geographic constraints, level of government, or perceived mutual mistrust between public and private sectors. That is, the approach recognizes no borders and is neither "top down" nor "bottom up"… It involves and values equally information collected by the U.S. private sector owners of national critical infrastructure, intelligence related to national security collected by federal, state, local, and tribal law enforcement officers, as well as the traditional "Ints" collected by statutory members of the IC."[58] This more flexible approach is better suited for a diverse and divergent group such as the fire service. Yet, this approach ignores the natural benefits of relationships between large government agencies and large political organs. In addition, the leverage and importance of large political organizations is not fully exploited.

Both the geographic and holistic approaches are extreme opposites, have merit in application, and work in different circumstances. Perhaps a case-by-case application of both is the best approach to using these methods? The important part of both is: one, they are not mutually exclusive, and two, they shift the HSINT focus away from the 30,000 foot federal level. The shift in approach from a 30,000 foot national (strategic) level to 20,000 foot regional (operational) level, 10,000 foot local (tactical) level or as others should examine, the street level. This is further bolstered by Charles K. Edwards' Inspector General's report "*DHS' Efforts to Coordinate and Enhance Its Support and Information Sharing with Fusion Centers,"* where it is retold that, "on September 10, 2010, the Secretary addressed first responders at the New York City Emergency Operations Center, explaining the department's shift to a "hometown-centric" approach.

[58] Todd Masse, *Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches.* Washington, D.C.: Congressional Research Service, 2006, 17.

By getting departmental information, tools, and resources to first responders, citizens, community groups, and the private sector, DHS can be more effective. The National Network of Fusion Centers is crucial to this effort.[59] There are two important pieces to this anecdote. First, the Secretary's mention of "hometown-centric approach" places value on local partnerships and exchanging of information. Second, the Secretary stated the local partners as "first responders, citizens, community groups, and the private sector" a wide array of untapped resources, especially in light of the struggles of including first responders outside of law enforcement. None the less, this is a clear indication that information/intelligence sharing expansion is validated as a priority at the highest level of DHS.

C. INTEGRATION INPUTS AND PRODUCTS

Prior to DHS, domestic intelligence dissemination was the purview of the FBI and JTTF. As a result, many fire departments may have developed relationships with the FBI and JTTF, for information/intelligence sharing. These relationships may or may not have been a reflection on local law enforcement as much as a cutting out the middle man and in order to receive timely and accurate intelligence. In relation to the evolution of DHS and its statutory authority related to the dissemination of information/intelligence to state and local government, through fusion centers; organizations may not fully understand the important role of JTTFs and other information/intelligence nodes that predate fusion centers. Using information from the ITACG, this section will begin by distinguishing between the JTTF and fusion centers. Next, other information/intelligence nodes will be presented. Finally, information/intelligence products produced by nodes and agencies will be listed.

In general, "**JTTFs** are FBI-sponsored, multijurisdictional task forces established specifically to conduct terrorism-related investigations. Analytic and information-sharing efforts carried out by the JTTFs are done solely to support those investigative efforts. Also, each FBI office contains a Field Intelligence Group, which is the main interlocutor

[59] Charles K. Edwards, *DHS Efforts to Coordinate and Enhance its Support and Information Sharing with Fusion Centers.* Office of the Inspector General Report, Washington, D.C.: United States Department of Homeland Security, November 2011, 14.

with the fusion center. **Fusion centers**, in contrast, are information sharing and analytic entities and do not focus solely on terrorism. They are state and locally owned and operated information analysis centers that analyze information and intelligence regarding a broad array of criminal and other activities related to homeland security. Fusion centers focus on trend and pattern analysis that is intended to help state and local law enforcement mitigate emerging crime problems, including terrorism and other threats to homeland security."[60] In the definitions of both the JTTF and fusion centers, both are strictly defined as crime based, one all crimes (Fusion) and one strictly terrorism related (JTTF).

Specifically, per the ITACG, below is a description of recognized nodes or intuitional inputs:

Joint Terrorism Task Force (JTTF): JTTFs serve as the coordinated "action arms" for federal, state, and local government response to terrorist threats in specific U.S. geographic regions. The FBI is the lead agency that oversees JTTFs. The benefits of a JTTF include:

- "one-stop shopping" for law enforcement information or investigation of suspected or real terrorist activities;
- use of a shared intelligence base;
- ability to prosecute cases in the jurisdiction that is most efficient and effective;
- task-force member awareness of investigations within a jurisdiction and ability to assist in investigations in other jurisdictions; and
- familiarity among agencies, investigators, and managers before a crisis occurs.[61]

The mission of a JTTF is to leverage the collective resources of the member agencies for the prevention, preemption, deterrence, and investigation of terrorist acts that

[60] Group, Interagency Threat Assessment and Coordination. "Intelligence Guide for First Responders." 2nd Edition, Washington, D.C., 2011, 36.

[61] Ibid., 34.

affect United States interests, to disrupt and prevent terrorist acts, and to apprehend individuals who may commit or plan to commit such acts. To further this mission, a JTTF serves as a means to facilitate information sharing among JTTF members.

- As of January 2011, there are 104 JTTFs based nationwide, including at least one in each of the FBI's 56 field offices.
- More than 600 state and local agencies participate in JTTFs nationwide. Federal representation includes the U.S. Intelligence Community, the Departments of Homeland Security, Defense, Justice, Treasury, Transportation, Commerce, Energy, State, and Interior, among others.[62]

Fusion Centers: A fusion center is a dedicated element, run by the applicable state or local jurisdiction, that exchanges information and intelligence, maximizes resources, streamlines operations, and improves the ability to disrupt, prevent, respond to, and recover from all threats by analyzing data from a variety of sources. A fusion center is defined as a "collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing a center's ability to detect, prevent, investigate, and respond to criminal and terrorist activity." Fusion centers focus primarily on the intelligence and fusion processes through which information is gathered, integrated, evaluated, analyzed, and disseminated. State and major urban area fusion centers provide analysis and information-sharing capabilities that support the efforts of state and local law enforcement to prevent and investigate crime and terrorism. Fusion centers receive information from a variety of sources, including state and local tips and leads, as well as federal information and intelligence. By "fusing" information from a wide variety of disciplines to conduct analysis, fusion centers generate products that are timely and relevant to their customers' needs. This allows state and local law enforcement to address immediate and emerging threat-related circumstances and events. It also supports risk-based, information-driven prevention, response, and consequence management.

62 Group, Interagency Threat Assessment and Coordination. "Intelligence Guide for First Responders." 2nd Edition, Washington, D.C., 2011, 35.

- As of January 2011, there are 72 designated fusion centers (50 state and 22 Major Urban Areas).

- Fusion centers are designed to involve every level and discipline of government, private-sector entities, and the public—though the level of involvement of some participants will vary.

- Fusion centers are state and locally owned and operated. The Department of Homeland Security (DHS) has a statutory program to support fusion centers.[63]

National Joint Terrorism Task Force (NJTTF)): The mission of the NJTTF is to enhance communication, coordination, and cooperation between federal, state, and local government agencies representing the intelligence, law enforcement, defense, diplomatic, public safety, transportation, and homeland security communities by providing a point of fusion for terrorism intelligence and by supporting the JTTFs throughout the United States.

- The NJTTF was established in July 2002 to serve as a coordinating mechanism with the FBI's partners.

- As of January 2011, forty-nine agencies are represented in the NJTTF, which has become a focal point for information sharing and the management of large-scale projects that involve multiple partners.[64]

National Operations Center (NOC): The mission of the NOC is to serve as the primary national level hub for domestic situational awareness, common operating picture, information fusion, information sharing, communications, and operations coordination pertaining to the prevention of terrorist's attacks and domestic incident management. The NOC serves as the nation's nerve center for information collection and sharing. Pursuant to Section 515 of the Homeland Security Act of 2002, the NOC is the principal operations center for DHS. As the principal operations center, Congress tasked the NOC with performing two key responsibilities:

---

[63] Group, Interagency Threat Assessment and Coordination. "Intelligence Guide for First Responders." 2nd Edition, Washington, D.C., 2011, 35–36.

[64] Ibid., 37.

- First, the NOC shall provide situational awareness and a common operating picture for the entire federal government, and for state, local, and tribal governments as appropriate, in the event of a natural disaster, act of terrorism, or other manmade disaster.

- Second, the NOC shall ensure that critical terrorism and disaster-related information reaches government decision makers.

By performing its mission, the NOC enables the Secretary DHS and other leaders to make informed decisions and identify courses of action during an event or threat. The Secretary has assigned the NOC to the DHS Office of Operations Coordination and Planning (OPS). The NOC is comprised of five operational components: the NOC-Watch, Federal Emergency Management Agency National Response Coordination Center (NRCC), DHS National Infrastructure Coordinating Center (NICC), Office of Intelligence and Analysis/Intelligence Watch and Warning Branch and the OPS Planning Element. Each NOC operational component remains an independent entity under the program management of its parent DHS Component. By drawing upon and leveraging the authorities and capabilities of each NOC operational component, the NOC—as a cohesive and integrated whole—serves as the primary national hub for situational awareness and operations coordination across the federal government for incident management and as the national fusion center, collecting and synthesizing all-source information, including information from the state fusion centers, across all-threats and all hazards information covering the spectrum of homeland security partners.[65]

In addition to the physical nodes for information/intelligence, there are also virtual nodes, such as the Homeland Security Information Network (HSIN) and Law Enforcement Online (LEO). With these, and other, virtual nodes comes For Official Use Only (FOUO) information, typically available to first responders, and classified information, available to those with proper clearance located at a physical node. For example, first responders with the appropriate level of clearance and access can view classified information on National Counterterrorism Center (NCTC)—currently, the DHS Office of Intelligence and Analysis portal, and other sites on SECRET level systems,

[65] Group, Interagency Threat Assessment and Coordination. "Intelligence Guide for First Responders." 2nd Edition, Washington, D.C., 2011, 38.

such as FBI Network (FBINet), Homeland Secure Data Network (HSDN), Joint Deployable Intelligence Support System (JDISS), and Secure Internet Protocol Router Network (SIPRNet).[66]

Realistically, the vast majority of the fire service has little need to know the sources and methods resulting in a piece of intelligence, thereby, negating the need for TOP SECRET clearances. Although, certain time sensitive classified intelligence warrants key decision makers possessing at a minimum of a SECRET clearance. Absent a mature integrated intelligence program, possibly TLO based, clearances below the highest command levels would be a justification for another thesis. Typically, the products the fire service should expect are FOUO and may fall into different categories. The categories disseminated by the IC domestically are Information Reports, Intelligence Assessments (IA), Intelligence Bulletins (IB), Threat Assessments (TA) or Special Assessments (SA).[67]

Per the ITACG, below is a brief description of each report type:

Information Reports are messages that enable the timely dissemination of unevaluated intelligence within the Intelligence Community and law enforcement. These products include:

- FBI IIR (Intelligence Information Report)
- DHS HIR (Homeland Information Report)

Intelligence Assessments (IA) are finished intelligence products resulting from the intelligence analysis process. Assessments may address tactical, strategic, or technical intelligence requirements.

Intelligence Bulletins (IB) are finished intelligence products used to disseminate information of interest, such as significant developments and trends, to the intelligence and law enforcement communities in an article format. IBs do not address threat warning information.

---

66 Group, Interagency Threat Assessment and Coordination. "Intelligence Guide for First Responders." 2nd Edition, Washington, D.C., 2011, 28–29.

67 Ibid.

Threat Assessments (TA) or **Special Assessments (SA)** provide in-depth analyses related to a specific event or body of threat reporting and may address non-terrorist threats to national security.

Joint Products are intelligence assessments and bulletins produced jointly with other agencies (dual or multiple seals). When written jointly, these products may be formatted differently than the single-seal versions, depending on the format agreed to by participating agencies.[68]

Finally, in addition to different report types specific summaries that may provide value to the fire service are below:

Joint Intelligence Bulletin (JIB). The JIB provides timely information or analysis on a recent or current event or development of interest to all information and analysis customers and is produced at various classification levels. It focuses on Homeland Security issues, is written on an ad hoc basis, and is generally one to three pages. It is available on HSIN, LEO, or HSDN, depending on the classification of the information.

Roll Call Release (RCR). Available on HSIN and LEO, the RCR is a collaborative For Official Use only (FOUO) product developed by DHS, FBI, and the ITACG. The product is written specifically for state, local, and tribal "street-level" first responders, and focuses on terrorist tactics, techniques, procedures; terrorism trends; and potential indicators of suspicious activity. The product, written on an ad hoc basis, is focused on one subject, and fits on one page.

Terrorism Summary (TERRSUM). The TERRSUM is a SECRET digest of terrorism related intelligence of interest to federal and non-federal law enforcement, security and military personnel. Produced Monday through Friday, the TERRSUM includes terrorism-related intelligence available to NCTC and other Intelligence

68 Group, Interagency Threat Assessment and Coordination. "Intelligence Guide for First Responders." 2nd Edition, Washington, D.C., 2011, 28–29.

Community elements. The product is available on SECRET-level systems to appropriately cleared personnel at state and major urban area fusion centers and Joint Terrorism Task Forces.

Worldwide Incidents Tracking System (WITS).WITS is the U.S. government's authoritative database on terrorist attacks compiled exclusively from open source information. Maintained by the NCTC, WITS is publicly available at www.nctc.gov. Users can search for attack data and sort it by a broad range of characteristics, to include type of attack, location, facility, perpetrator, and other attributes. Users also can plot incidents on maps using Google Earth and Google Map. State, local, and tribal law enforcement and first responders use WITS to track terrorist trends, support event planning, and provide context for terrorist activities.[69]

Above a number of nodes, databases, and products have been presented. Each of these nodes, databases, and products represent either a method or source of information that an individual fire department can utilize to share or gain information and intelligence. The diversity of options can be utilized by a diverse number of fire departments. These diverse departments with different resource levels and different formal relationships can use the above as possible starting points or fodder for ideas as to how to both receive and pass on information.

[69] Group, Interagency Threat Assessment and Coordination. "Intelligence Guide for First Responders." 2nd Edition, Washington, D.C., 2011, 28–29.

V. CONCLUSIONS AND RECOMMENDATIONS

In devising a new strategy for fire service information sharing, the main elements of the DHS Intelligence Strategy provided a road map. The main elements are: Vision, Mission,

Definitions, and Goals and Objectives.[70]

> The primary statutory definition that applies is that which appears in the Homeland Security Act of 2002, which defines homeland security *information* as any information possessed by a federal, state, or local agency that (a) relates 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.[71]

A. STRATEGY RECOMMENDATIONS

This thesis recommends the facilitation of bottom up inclusion of the fire service in information and intelligence sharing through access to intelligence nodes. The strategy to implement a new system for fire service integration into domestic information/intelligence sharing needs to address current and emerging threats. This strategy should allow for improved and timely information/intelligence, as well as facilitate the flow of this information to all partners—state, local, tribal or federal, with the objective of providing a roadmap for individual fire departments to establish a bi-directional information conduit between the fire service and DHS.

Based on current grassroots networks and existing relationships, fire departments could have the option to use FEMA Regions, hegemonic fire departments with resources and relationships, law enforcement entities having interaction with fusion centers or through relationships gained through mutual aid agreements. Hegemonic fire departments are departments with the resources and capabilities to assist departments regionally, and in extreme circumstances nationally, in mitigating incidents they may lack the personnel

---

70 Todd Masse, *Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches.* Washington, D.C.: Congressional Research Service, 2006, 11.

71 Ibid., 12.

or capability to mitigate. In addition, hegemonic have the resources to be national leaders in research, development, and beta testing new concepts. Optimally, this would be legitimized and codified per a national directive, which mandates the alignment of federal coordination, structures, capabilities, and resources into a unified, all-discipline, and all-hazards approach to domestic information management. An example of such a directive would be a Presidential Policy Directive (PPD). For example, PPD addresses National Preparedness coordination across discipline.[72] A codified national directive would be consistent with the National Strategy for Information Sharing, which states, "Authorities at all levels of our federal system must share a common understanding of the information needed to prevent, deter, and respond to terrorist attacks.[73] The common understanding will be achieved through a framework that enables: (1) Federal entities to work together to provide information in ways that better meet the needs of state, local and tribal partners; and (2) Information gathered at the state and local level to be processed, analyzed, disseminated, and integrated with information gathered at the federal level."

1. Recommendation: Development of System

It is the goal that organic nodes will develop, through grassroots efforts that will allow information to flow as a result of existing organization relationships, as opposed to through a nationally mandated system. Systems theory shows the power and resiliency of a network, if the number of nodes is increased. A more resilient system will withstand stress by its redundancy and plasticity "to absorb shocks and rechanneling its efforts to remain intact."[74] For instance, Metcalf's Law states the power of a network increases exponentially to the amount of linked nodes.[75] (See Figure 3).Furthermore, robust interconnected networks allow for speed of movement and more effective decisionmaking allowing choices to be made on the level where choices are most immediately felt and information is either used or gathered. In other words, a "distributed

---

[72] Presidential Policy Directive (PPD 8).

[73] National Strategy for Information Sharing: Sucesses and Challenges In Improving Terrorsim-Related Information Sharing." Federal Report, Washington, D.C., 2007.

[74] John Arquilla and David Ronfeldt, *Networks and Netwars* (Santa Monica: RAND, 2001), 123.

[75] Ibid., 35.

structure" that permits timely decisions made by those closest and most familiar to the issue rather than through a cumbersome wait engendered by a hierarchal command geographically removed from the scene.[76]

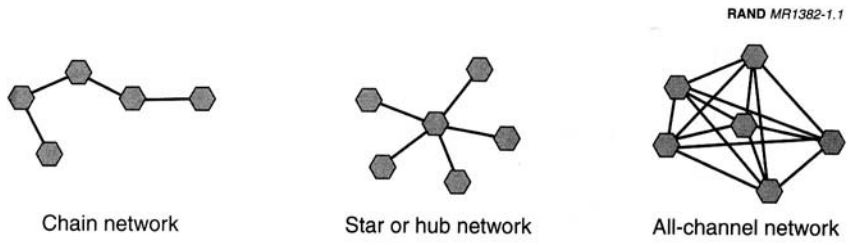

Figure 1.1—Three Basic Types of Networks

Figure 3. Three Basic Types of Networks.[77]

In the proposed Fire Service Information Sharing System, there are no predestinated central nodes. Under the FSIE, the fifteen (15) departments were intended to become central nodes in a network that would expand beyond the fifteen partners to their surrounding localities. In the Fire Service Information Sharing System, the onus is placed on individual departments to decide the best network to join and at what level of engagement. Each individual department can determine their level of engagement depending upon their need and capabilities. The level of engagement, or decision not to become engaged, by departments is at individual departments sole discretion

The transference of integration of responsibility to the lowest levels of the system avoids the issues having a system of like nodes (departments with similar capabilities and similar size) that could lead to a tiered system of nodes based upon department sizes, organization (e.g., volunteer vs. career) and capabilities. In addition, nodes formed organically with different access points does not result in a single point of failure or reliance upon a single place for interaction (e.g., HSIN) and a single program sponsor

[76] Committee on Homeland Security, *The Homeland Security Information Network: An Update on DHS Information-Sharing Efforts* (Washington, DC: U.S. House of Representatives One Hundred Ninth Congress, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, 2007), 41, U.S. Government Printing Office, Serial No. 109–101.

[77] John Arquilla and David Ronfeldt, *Networks and Netwars* (Santa Monica: RAND, 2001), 8.

(e.g., DHS I&A or FBI). As a result of different fire department sizes, organization, and capability one person or one group being responsible for the Fire Service Information Sharing System may not be effective or capable of representing all. Therefore, each department is empowered to represent themselves in becoming engaged in the Fire Service Information Sharing System.

Arquilla writes that networks are "measured across five levels of analysis:

- Organizational level-its organizational design;
- Narrative level-the story being told;
- Doctrinal level-the collaborative strategies and methods;
- Technological level-the information systems;
- Social level-the personal ties that assure loyalty and trust.[78]

Furthermore, "The strength of a network, perhaps especially the all-channel design, depends on its functioning well across all five levels. The strongest networks will be those in which the organizational design sustains by a winning story and a well-defined doctrine, and in which all of this layers atop advanced communication systems and rests on strong personal ties at the base. Each level, and the overall design, may benefit from redundancy and diversity. Each level's characteristics are likely to affect those of the other levels."[79]

As the system develops and evolves, it should be measured against Arquilla's levels of analysis. Based upon the ongoing analysis, the system can be adjusted and improved. This would be affective as analysis would be based on actual outcomes as opposed basing the system on analysis of predicted possible outcomes. For example, the FSIE focused on HSIN as the technological level solution. With technology ever changing and the diverse level of technological infrastructure throughout the Fire Service, a predetermined solution was not and will not be effective. Furthermore, a grassroots

[78] John Arquilla and David Ronfeldt, *Networks and Netwars* (Santa Monica: RAND, 2001), 324.

[79] Ibid.

based system would have an increased chance of success on a social level, as preexisting organizational relationships, and by extension personal ties, can be leveraged to form a network node. Yet, regardless of how the node and relationships are formed and the system evolves, there needs to be given a clear vision and expectations for fire service integration. Therefore, a mission and goals will be articulated.

2. Recommended Mission and Goals

a. Mission

The United States Fire Administration will create and maintain documents and supporting policies to facilitate collaboration with accurate, complete, and timely flow of information on fire service issues.

b. Vision

Foster a collaborative environment that will facilitate the fire service using organizational relationships with either their FEMA Region or existing law enforcement collaborators for information/intelligence sharing and eventually suspicious activity reporting. As a result of research into the work done by the FSIE, realistic goals can be transferred.

c. Goals

(1) Institute Uniform Information Sharing Framework. This goal focuses on providing guidance to FEMA Regions and Law Enforcement entities as to coordination of information sharing with fire departments:

- Develop a framework to increase information sharing across the fire service community and with state, local and federal partners.

- Mechanisms to instill common avenues of integration practices for organizations facilitating intelligence and information sharing between fire departments and fusion centers.

- Reduce risks to civil liberty and privacy infractions from greater information sharing.

- Assist uniform information/intelligence sharing knowledge and capabilities through the availability of training programs and model standards for fire department use in developing internal sharing policies and procedures.

- The integration of fire departments should be complementary to "fusion centers" but not exclusionary tied to "fusion centers" as the only avenue for interaction.

(2) Advance Fire Service Intelligence Requirements. The FSIE and its working group, with support and assistance from DHS I&A, developed a working set of intelligence requirements for the fire service:

- Revisit and review requirements and update, if necessary.

- Distribute the fire service requirements to all fusion centers and applicable IC members for use by analysts.

- Develop fire service requirement training for intelligence analysts working or wishing to work in fusion centers.

(3) Enhance Collaboration across the Community. Collaboration was a constant theme across the research and in most official policy documents. This goal focuses on developing incentives (e.g., at the institutional, leadership, and workforce levels) for collaboration with fire service community by all levels of law enforcement and FEMA regions to instill the "responsibility to provide" culture, share knowledge and provide expertise:

- Develop information sharing communication programs to create awareness of a "responsibility to provide" culture.

- Create programs to transform the culture from a "need to know" to a "responsibility to provide" mindset.

- Allow grass roots sharing initiatives to flourish between fire departments through the conduits determined to be most appropriate and expedient, for both individual fire departments and their link to the fusion center/partner.

- Provide smart practices and success stories of the different methods used by fire departments to gain access to intelligence/information.

- Each FEMA Region will be responsible for monitoring and assisting/facilitating, if necessary, the partnering of fire departments with an organization engaged in the fusion process.

- Integration would focus on using any available point of contact not just one, examples of different points of contact are shown in Figure 4:[80]

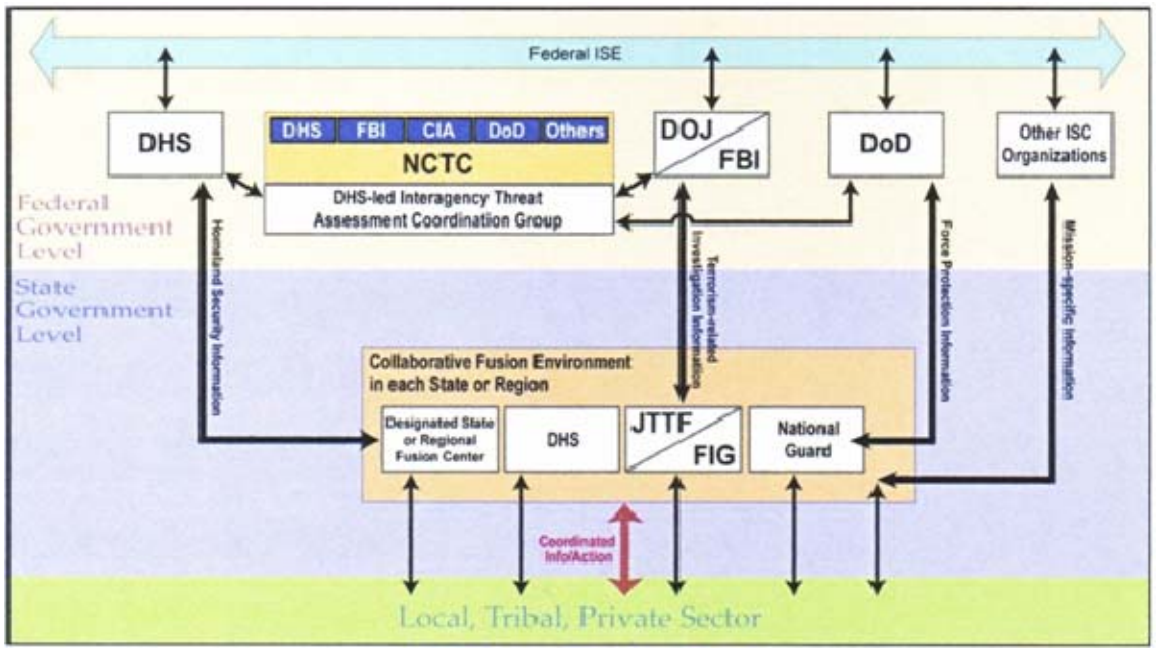

Figure 4. Flow of Information to and from the IC to SLT.

[80] Information Sharing Environment Program Manager, *Information Sharing Environment Implementation Plan* (Washington, DC: Office of the Director of National Intelligence, 2006), 71.

3. Recommended Strategic Plan

This framework for multiple avenues for access to information/intelligence shares the same core principles as the previous, FSIE:

- Effective information sharing comes through strong partnerships among federal, state, local, and tribal authorities, and private sector organizations;
- Information acquired for one purpose, or under one set of authorities, might provide unique insights when combined, in accordance with applicable law, with seemingly unrelated information from other sources, and therefore a culture of awareness in which people at all levels of government remain cognizant of the functions and needs of others and use knowledge and information from all sources to support mutual efforts to protect the homeland must be fostered;
- Information sharing must be woven into all aspects of fire service activity, including preventive and protective actions, actionable responses, event preparedness, and response to and recovery from catastrophic events;
- The procedures, processes, and systems that support information sharing must draw upon and integrate existing technical capabilities and must respect established authorities and responsibilities; and
- Develop training, awareness, and exercise programs to ensure that State, local, and tribal personnel are prepared to deal with terrorist strategies, tactics, capabilities, and intentions, and to test plans for preventing, preparing for, mitigating the effects of, and responding to all-hazard events.

The strategy for achieving the mission and goals involves leveraging the positive work and documents from the FSIE. In addition to using all authorities, resources, programs, and capabilities of FSIE, participants can assist in the execution of this plan as effectively as possible and to promote a culture where sharing all-hazards information is a core value.

Therefore, the operating environment that flows from this vision and these goals will draw upon existing systems and capabilities, observe and respect the roles and responsibilities of participating federal entities, and facilitate a coordinated, collaborative approach to appropriate information sharing among the entire fire service. This environment will create a powerful national capability to share, search, and analyze threat

information across jurisdictional boundaries and provide a distributed, secure, and trusted environment for transforming data into actionable information. The resulting environment will also recognize and leverage the vital roles played by state and major urban area information fusion centers, which represent crucial investments toward improving the nation's all-hazards capacity.

4. Summary

The successful implementation of this plan has the potential to create an environment in which all fire departments have an opportunity to pursue an avenue for information/intelligence sharing. By not mandating a one size fits all, one point of access to fit the disparate fire service information/intelligence sharing can grow from the grass roots level and be met half way by naturally allied organizations with access to information/intelligence and achieving the stated purpose, goals, and objectives: to enable fire service partnerships, enhance the lawful sharing of information, and to coordinate interactions with state and local fusion centers. At this end state, the fire service will have information that is timely and can potentially influence actions to be taken, have information tailored to the needs of individual participants—the right information provided at the right time, over the right pathways—and have information that can be exchanged within the system of rules established to protect that information.

B. AREAS FOR FURTHER STUDY

In terms of information/intelligence sharing, the FSIE brought the fire service a long way, in terms of producing the foundation documents needed for integration. Yet there is still work that remains to be done. This thesis examined options at a 10,000 foot level for organizational sharing; however, that is only a first step in an important process bound with obstacles for acceptance in the information sharing domain that will require fundamental shifts in organizational culture. The scope of this endeavor limited the thorough examination of departmental operational implementation, including TLOs and security clearances. The universal key to any future initiative or proposal requires flexibility in order to be assimilated into fire culture, theory and practice and cannot be initially strictly tech based.

In light of the research for this document, the author pointed to two large topics suffering from volumes of ever changing information.

C. LEVERAGING CURRENT TECHNOLOGY AND THE FUTURE

As presented in the discussion section, there are a wide variety of systems and products accessible to various levels of responders, officials and agencies. To supplement existing systems, individual fusion centers and other nodes may have systems for dissemination and collection. This is a topic in and of itself meriting study. Yet, with ever evolving technology, any technological solution needs to be adaptable and scalable. By nature, the fire service and its 150 years unimpeded by progress is technology averse. In addition, older urban areas may not have the technological backbone to support a robust information sharing system.

A possible solution would be to design specific platforms over or in conjunction with existing platforms. Such existing platforms are computer aided dispatch (CAD) and existing email distribution systems. As opposed to creating an entirely new system, CAD can be the backbone for an information delivery and transmission system. This solution also limits the unauthorized access or abuse of the system. A CAD based system would be physically tied to fire apparatus and fire houses. Furthermore, most CAD systems are closed loop, restricting external access, while allowing for information to be pushed to a partner node. How individual portals are constructed is a matter of department preference. Below are examples of existing information networks from which ideas can be gleamed.

Intelink-U. Intelink-U is the Intelligence Community's (IC) sensitive but unclassified-sharing network. Content is provided by the IC, other government agencies, foreign partners, academia, and open sources. Accounts are available to individuals with federal, state, local, and tribal homeland security and law enforcement responsibilities.

- *Web site: https://www.intelink.gov.*
- *Access: Go to web site, click on "Sign In," and proceed to "New Account Registration."*

Law Enforcement Online (LEO). LEO can be accessed from any computer system with an Internet connection. It is an official government information-sharing and electronic-communications portal. LEO provides FBI, joint FBI-DHS, NCTC, and nonfederally produced intelligence products at the For Official Use Only (FOUO) level. Accounts are available to federal, state, local, and tribal personnel performing homeland security or law enforcement duties and personnel from foreign law enforcement agencies.

- *Web site: http://www.leo.gov*
- *Access: Go to web site, click on the "LEO Membership Criteria," then the "LEO*
- *User Application," or contact the LEO helpdesk at 1-888-334-4536, or via e-mail at helpdesk@leo.gov*

OpenSource.gov. The Open Source Center (OSC) and its partners provide timely and tailored translations, reporting, and analysis on foreign policy and national security issues. Featured are reports and translations from thousands of publications, television and radio stations, and Internet sources around the world. Also among the site's holdings are a foreign video archive and fee-based commercial databases for which OSC has negotiated licenses. OSC's reach extends from hard-to-find local publications and video to some of the most renowned thinkers on national security issues inside and outside the U.S. government. Accounts are available to federal, state, and local government employees and contractors.

- *Web site: http://www.opensource.gov.*
- *Access: Apply online via web site.*

Regional Information Sharing Systems Network (RISSNET). RISSNET facilitates information sharing within the law enforcement community to combat multijurisdictional criminal activities and conspiracies. It is composed of six multistate intelligence centers (RISS Intelligence Centers). Membership includes federal, state, local, and tribal law enforcement agencies.

- *Access is requested through the regional RISS Intelligence Centers*
- *Web site: http://www.riss.net*
- *Contact information available at http://www.riss.net/Centers.aspx*

Technical Resources for Incident Prevention (TRIPwire).TRIPwire is the Department of Homeland Security's 24/7 online, secure, collaborative, information-sharing network for bomb squad, law enforcement, and other emergency services personnel to learn about current terrorist Improvised Explosive Device (IED) tactics, techniques, and procedures, including design and emplacement considerations. TRIPwire combines expert analysis and reports with relevant documents, images, and videos gathered directly from terrorist sources to help law enforcement anticipate, identify, and prevent IED incidents.

- *Web site: https://www.tripwire.dhs.gov.*
- *Access: For more information about the TRIPwire system, please contact the Office for Bombing Prevention at OBP@dhs.gov or through the TRIPwire help desk at help@ tripwire-dhs.net*[81]

In addition to the development of a system, internal policies and procedures need to be developed on a department by department basis in conjunction with their sharing partner or node. To assist in forming individual policies and the following links may be of assistance and are valid as of January 2011.

- Guidance for Building Communities of Trust *http://nsi.ncirc.gov/documents/e071021293_BuildingCommTrust_v2-August%2016.pdf*
- NSI Training Overview *http://nsi.ncirc.gov/documents/NSI_Training_Overview.pdf*
- National Strategy for Information Sharing: *http://georgewbush-whitehouse.archives.gov/nsc/infosharing/index.html*
- National Information Exchange Model: *www.niem.gov*[82]

[81] Group, Interagency Threat Assessment and Coordination. "Intelligence Guide for First Responders." 2nd Edition, Washington, D.C., 2011, 53–54.

[82] Ibid., 77.

D. SUSPICIOUS ACTIVITY REPORTING AND THE FUTURE

The most misunderstood facet of information/intelligence sharing, as it related to the fire service, is the concept of suspicious activity reporting (SAR). This is a topic of future study due to the availability of possible technological solutions, legal issues, possible threat to the positive public perception enjoyed by the fire service, and implementation strategies. Regardless of ones feeling on the issue, in order to be a full partner in disseminating and receiving information/intelligence SAR usage in the fire service will need to be addressed. As the following quote from the ITACG shows, this is an issue that if not addressed will be a priority, "Because of the nature of their work, the more than 800,000 law enforcement and 1.2 million firefighters in the United States are perfectly poised to identify criminal activity that may be precursor indicators of acts of terrorism. In many instances, information that is based on suspicious behavior has led to the disruption of a terrorist attack, the arrest of individuals intending to do harm, or the corroboration of existing intelligence. It is of utmost importance that information on suspicious activities be shared with between federal, state, local, tribal, and private-sector partners."[83]

As it currently stands, the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) "is a comprehensive and coordinated effort to establish a "unified process for reporting, tracking, and accessing SARs" in a manner that rigorously protects the privacy and civil liberties of Americans. The NSI strategy is to develop, evaluate, and implement common processes and policies for gathering, documenting, processing, analyzing, and sharing information about terrorism-related suspicious activities … The long-term goal is that federal, state, local, and tribal law enforcement organizations, as well as the private sector, will participate in a standardized and integrated approach to SAR."[84] SAR is viewed important as an aid to law enforcement entities to carry out counterterrorism-related activities initiate investigations and provide information on all crimes. Using information gleaned in plain view of criminal activity or behavior, the

83 Group, Interagency Threat Assessment and Coordination. "Intelligence Guide for First Responders." 2nd Edition, Washington, D.C., 2011, 76.

84 Ibid., 74.

hope is that if this activity has a nexus to terrorism, law enforcement can become alerted to the planning of a terrorist attack prior to the attack being carried out.

As with any new initiative, and especially one this potentially controversial, looking at this incident will need to address comprehensive training, policies and procedures to protect privacy and civil liberties, operational policies, and technical applications. More in-depth information and documents on this issue can be found at the following web sites that are valid as of January 2011.

- Privacy, Civil Rights, and Civil Liberties Protections: A Key Component of the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) http://nsi.ncirc.gov/documents/NSI_Privacy_Briefing.pdf[85]
- Additional resources and publications on the SAR initiative or the SAR process can be located at: www.nsi.ncirc.gov[86]
- Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project: www.it.ojp.gov/documents/SARReportOctober2008.pdf[87]
- Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR): http://nsi.ncirc.gov/resources.aspx[88]

85 Group, Interagency Threat Assessment and Coordination. "Intelligence Guide for First Responders." 2nd Edition, Washington, D.C., 2011, 77.

86 Ibid.

87 Ibid.

88 Ibid.

LIST OF REFERENCES

"50 USC 403–103(g)." n.d.

Arquilla, John, and David Ronfeldt. *Networks and Netwars.* Santa Monica: Rand Corporation, 2001.

Clapper, James R. "Unclassified Statement for the Record on the Worldwide Threat Assessment of the U.S. Intelligence Community for theSenate Select Committee on Intelligence." *Statement for the Record.* Washington, D.C., January 31, 2012.

Cloud, Rosemary. "Future Role of Fire Service in Homeland Security." Monterey, California: Naval Postgraduate School, September 2008.

Edwards, Charles K. *DHS' Efforts to Coordinate and Enhance its Support and Information Sharing with Fusion Centers.* Office of the Inspector General Report, Washington, D.C.: United States Department of Homeland Security, November 2011.

Fire Department City of New York. "Terrorism and Disaster Preparedness Strategy." New York, New York, 2007.

The Homeland Security Information Network: An Update on DHS Information-Sharing Efforts. Washington, D.C.: United States House of Represenatives 109th Congress Committee on Homeland Security, Subcommittee Committee on Intelligence, Information Sharing, and Terrorism Risk Assessment, 2007.

Information Sharing Enviroment Implementation Plan. Office of the Director of National Intelligence, Washington, D.C.: Information Sharing Enviroment Program Manager, 2006.

Information Sharing: Progress made and Challenges Remaining in Sharing Terrorism-Related Information. Statement for the Record To the Committee on Homeland Security and Governmental Affairs, U.S. Senate, United States Government Accountability Office, Washington, D.C.: GAO, October 2011.

Interagency Threat Assessment and Coordination Group (ITACG) Intelligence Guide for Firest Responders. Washington, D.C.: National Counterterrorism Center, 2009.

Johnson, Loch K., ed. *Strategic Intelligence: Understanding the Hidden Side of Government.* Vol. 1. Westport, CT: Praeger Security International, 2007.

Masse, Todd. *Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches.* Washington, D.C.: Congressional Research Service, 2006.

"National Strategy for Information Sharing: Sucesses and Challenges In Improving Terrorsim-Related Information Sharing." Federal Report, Washington, D.C., 2007.

Office of the Director of National Intelligence. "U.S. National Intelligence: An Overview 2011." Washington, D.C., 2011.

Office of the Director of National Intelligence. "http://www.dni.gov/overview.pdf." 2009. (accessed October 2011).

"P.L. 110-53, §511, 121 STAT. 322. " n.d.

"Presidential Policy Directive 8: National Preparedness." Washington, D.C., March 30, 2011.

Randol, Mark A. *The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress.* Washington, D.C.: Congressional Research Service, May 27, 2009.

United States Department of Homeland Security. n.d. http://www.dhs.gov/if-you-see-something-say-something-campaign (accessed August 22, 2012).

United States Fire Administration. *FSIE Fact Sheet.* Washington, D.C., 2010.

United States Intelligence Community: Strategic Intent for Information Sharing 2011-2015. Washington, D.C.: Office of the Director of National Intelligence, 2011.

United States Department of Justice."Fire Service Integration for Fusion Centers: An Appendix to the Baseline Capabilities for State and Major Urban Area Fusion Centers." April 2010, 18.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. United States Fire Administration
   Emmitsburg, Maryland