NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

IDENTIFYING BEST PRACTICES IN THE DISSEMINATION OF INTELLIGENCE TO FIRST RESPONDERS IN THE FIRE AND EMS SERVICES

by

Thomas J. Richardson

September 2010

Thesis Advisor:	Robert Simeral
Second Reader:	Lauren Fernandez

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE September 2010	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE Identifying Best Practices in the Dissemination of Intelligence to First Responders in the Fire and EMS Services	5. FUNDING NUMBERS
6. AUTHOR(S) Thomas J. Richardson	
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__NPS.2010.0047-IR-EP7-A_____

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

13. ABSTRACT (maximum 200 words)

September 11, 2001, thrust the fire service into the world of intelligence but the evolution of its involvement has been slow and challenging. The evolving role in the intelligence process presents unprecedented challenges. This expanded role has presented an opportunity to contribute to the homeland security prevention and protection mission in addition to their traditionally recognized role in response and recovery.

As fire service participation expands and the macro level sharing of intelligence between the fire service and the intelligence/law enforcement communities becomes more recognized as a matter of course, it will be necessary for fire service agencies also to develop internal mechanisms of disseminating intelligence to field level personnel. If field level personnel do not receive timely, credible, and actionable information, driven by the intelligence process, before, during and after an incident, their lives, as well as the lives of the public they are trying to help, can be jeopardized.

This thesis presents research to answer the question, "how can information and intelligence be better disseminated to local first responders to enhance situational awareness, provide a higher degree of responder safety, and better protect the public?" Structured interviews were conducted to examine existing models being used to disseminate intelligence to first responders who were surveyed to determine what type of intelligence they preferred to receive, and in what format they would prefer to receive it. The findings revealed that first responders want intelligence products in an easily accessible concise format available in real time.

14. SUBJECT TERMS Fire Service, First Responders, Intelligence, Dissemination, Firefighter Training, Emergency Preparedness, Emergency Response	15. NUMBER OF PAGES 105
	16. PRICE CODE

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

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

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

IDENTIFYING BEST PRACTICES IN THE DISSEMINATION OF INTELLIGENCE TO FIRST RESPONDERS IN THE FIRE AND EMS SERVICES

Thomas J. Richardson
Battalion Chief, New York City Fire Department (FDNY)
B.S., State University of New York, 2006

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 2010**

Author: Thomas J. Richardson

Approved by: CAPT Robert Simeral
Thesis Advisor

Lauren Fernandez, DSc
Second Reader

Harold A. Trinkunas, PhD
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

September 11, 2001 thrust the fire service into the world of intelligence but the evolution of its involvement has been slow and challenging. The evolving role in the intelligence process presents unprecedented challenges. This expanded role has presented an opportunity to contribute to the homeland security prevention and protection mission in addition to their traditionally recognized role in response and recovery.

As fire service participation expands and the macro level sharing of intelligence between the fire service and the intelligence/law enforcement communities becomes more recognized as a matter of course, it will be necessary for fire service agencies also to develop internal mechanisms of disseminating intelligence to field level personnel. If field level personnel do not receive timely, credible, and actionable information, driven by the intelligence process, before, during and after an incident, their lives, as well as the lives of the public they are trying to help, can be jeopardized.

This thesis presents research to answer the question, “how can information and intelligence be better disseminated to local first responders to enhance situational awareness, provide a higher degree of responder safety, and better protect the public?” Structured interviews were conducted to examine existing models being used to disseminate intelligence to first responders who were surveyed to determine what type of intelligence they preferred to receive, and in what format they would prefer to receive it. The findings revealed that first responders want intelligence products in an easily accessible concise format available in real time.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACTIC	Arizona Counterterrorism Intelligence Center
CBRNE	Chemical, Biological, Radiological, Nuclear, and Explosive
COI	Communities of Interest
DHS	Department of Homeland Security
DNI	Director of National Intelligence
EAM	Emergency Action Message
EMR-ISAC	Emergency Management and Response—Information Sharing and Analysis Center
EMS	Emergency Medical Response
ESS	Emergency Services Sector
FBI	Federal Bureau of Investigation
FDNY	New York Fire Department
FDOC	Fire Department Operations Center
FEMA/NPD	Federal Emergency Management Agency, National Preparedness Directorate
FLETC	Federal Law Enforcement Training Center
FLO, TLO, ILO	Fire Service Fusion, Terrorism, Intelligence Liaison Officers
FSIE	Fire Service Intelligence Enterprise
GAO	Accountability Office
HSIN	Homeland Security Information Network
I&A/SLPO	Intelligence and Analysis, State and Local Program Office
IAFC	International Association of Fire Chiefs
IAFF	International Association of Firefighters
IC	Intelligence Community
iCAV	Integrated Common Analytical Viewer
ICS	Incident Command System
IED	Improvised Explosive Devices
ITACG	Interagency Threat Assessment and Coordination Group
JTTF	Joint Terrorism Task Force
LES	Law Enforcement Sensitive
MDT	Mobile Data Terminal

NextGen	Next Generation
NFA	National Fire Academy
NOC	National Operations Center
NPS	Naval Postgraduate School
NRF	National Response Framework
NVFC	National Volunteer Fire Council
POC	Point of Contact
ROIC	Regional Operations Intelligence Center
SWAT	Special Weapons and Tactics
TLO	Terrorism Liaison Officer
U/FOUO	Unclassified/For Official Use Only
WMD	Weapons of Mass Destruction

ACKNOWLEDGMENTS

My participation in this program would not have been possible without the support of the New York City Fire Department administration. I would like to sincerely thank former Commissioner Nicholas Scoppetta who was the fire commissioner when I started the program. He had the foresight to allow members of the FDNY to begin their involvement with this incredible educational opportunity to enhance the professional development of fire officers and chief officers. I also want to thank Chief of Department Salvatore Cassano (now Fire Commissioner), and current Chief of Department Edward Kilduff for their support while participating in the program. Without the support and sponsorship of the FDNY, it would be much more difficult to complete such an intense degree program. I also owe a great deal of gratitude to my fellow chief officers in Battalion 38 for stepping up while I was not in the battalion during the in-residence periods and covering my areas of responsibility.

This has been quite a journey and I am professionally and personally better for having traveled this difficult road. I have done so with some extremely bright and talented people in my cohort and I thank them for their friendship, scholarship, and intellectual spirit. The professors throughout the program were always encouraging, helpful, and mindful of the difficulties that working professionals could have while trying to do all of the required coursework. CHDS has developed an incredible group of educators in the homeland security discipline who without question significantly contribute to preparing homeland security professionals who will make our nation a safer place to live. In particular, I would like to acknowledge and thank Chris Bellavita for his tenacious style of educating. In my case, he allowed me to develop the confidence to realize that I could do the work and contribute to the overall homeland security discussion. CAPT Robert Simeral was a true professional and provided me with solid advice and expertise during the thesis process as my advisor. He was quick to return

feedback which enabled me to move forward. Lauren Fernandez was a tremendous asset to me during the research course while developing my thesis topic and was a great help as the second reader for my thesis.

We should all be proud of what we have accomplished and be especially thankful to our families for allowing us to participate in this journey. I probably cannot thank my wife Julie enough for her support and understanding throughout the eighteen months, and especially while completing the thesis. She spent not only the in-residence periods keeping the ship sailing at home, but many lonely days and nights while I was buried in my office doing school work. It was also my intent to display to my three children, Jessica, Jenna, and Thomas that it is never too late to learn new things and take on new challenges; it can make you a better person and enable you to contribute more to your community and society as a whole. I love you all for your support and encouragement.

I. INTRODUCTION

A. PROBLEM STATEMENT

September 11, 2001, thrust the fire service[1] into the world of intelligence but the evolution of its involvement has been slow and challenging. Perhaps the reason for this has been, from the intelligence community (IC) and law enforcement perspectives, that the fire service should normally receive intelligence only when it is absolutely necessary or specifically requested. The intelligence requirements are different for law enforcement and the fire service. Law enforcement needs intelligence to prevent criminal and terrorist acts from occurring. The fire service needs intelligence to reduce the risks to their personnel and to be better prepared for responses to a terrorist attack to save the most lives. This difference in requirements leads to a recognition that mechanisms are needed to enable the distribution of intelligence and information in a timely and efficient manner so that the different consumers receive what they need to accomplish their missions.

The major information and intelligence-sharing gap that needs to be filled is between the law enforcement community and their fire service counterparts. Several federal initiatives are attempting to fill this gap, including the Department of Homeland Security (DHS) Office of Intelligence & Analysis, the U.S. Fire Administration's Fire Service Intelligence Enterprise (FSIE) and the DHS Office of Infrastructure Protection's Emergency Services Sector Information Sharing Working Group, among others. These initiatives have focused mainly on promoting the integration of fire and emergency services intelligence interests into state and local fusion centers. Fusion centers comprised of multi-discipline personnel have become the major intelligence analysis, information sharing, and

[1] For the purpose of this thesis, the fire service includes firefighters and emergency medical personnel.

exchange conduits between the IC and law enforcement. The fire service is still struggling to become a full partner in this process. Further study is necessary to understand how the fire service can become a full and contributing partner. If this gap can be filled, the right information quickly reaches field personnel and becomes more relevant to the strategic and tactical decision makers, who can provide a better level of safety and preparedness for all emergency service personnel.

B. BACKGROUND

A formal process for sharing intelligence and homeland security related information with the fire service at the federal, state, local, and tribal levels began in 2007 when the FSIE was created. The FSIE was established by DHS because both the IC and the fire service recognized that firefighters played an important role in the intelligence process. The goal of this initiative was to enable the integration of the fire service into state and local fusion centers (FSIE Concept Plan, 2009, p. ii). DHS and the fire service recognized that an improvement in two-way communications for information sharing to occur was necessary.

This initiative has been a step forward in the evolution of the relationship between the fire service and the IC. The information and intelligence sharing relationships for the fire service continue to be better defined and a better understanding of the appropriate role of the fire service within the intelligence cycle is developing.

If first responders are to receive sensitive information, some concerns of the law enforcement community and the general public are the protection of privacy, the possibility of compromising law enforcement investigations, and the possibility of exposing IC or law enforcement sources. This is a legitimate concern but an argument can be made that a precedent exists, in that firefighters and EMS personnel have experience in managing confidential information (Cloud, 2008, p. 58). This area warrants further research because firefighters are

traditionally regarded as some of the most trustworthy public servants. To erode that public confidence might diminish the argument for a collaborative information sharing process.

The *National Strategy for Information Sharing* acknowledges that homeland security activities and counterterrorism have become a daily activity within local response agencies. The *Strategy* specifically states, "they require access to timely, credible, and actionable information and intelligence about individuals and groups intending to carry out attacks within the United States" (National Strategy for Information Sharing, 2007, p. 17).

C. RESEARCH QUESTION

How can information and intelligence be better disseminated to local first responders to enhance situational awareness, provide a higher degree of responder safety, and better protect the public? To answer this question, this thesis examines existing models being used to disseminate intelligence to first responders in a timely and efficient manner. After examining the existing models in a comparative analysis, recommendations are developed for an improved model.

D. SIGNIFICANCE OF RESEARCH

The fire service's evolving role in the intelligence process presents unprecedented challenges. This expanded role has presented an opportunity to contribute to the homeland security prevention and protection mission in addition to their traditionally recognized role in response and recovery. As rich sources of expertise, fire service personnel can assist law enforcement in identifying possible threats. Becoming effective consumers of intelligence, firefighters can better protect themselves from the risks associated with terrorist attacks and major disasters.

Law enforcement and the intelligence community have begun to recognize the benefit of fire service experience. Efforts have started to formalize the information and intelligence sharing relationship and to build a more collaborative information-sharing network. Recent federal, state, and local information sharing initiatives have been major steps forward in the process. The goal of these initiatives is to achieve widespread and meaningful fire service integration in state and local fusion centers, and other information sharing networks, by establishing protocols and standards to support federal, state, and local efforts. By identifying best practices, more fire service agencies might begin the process of developing partnerships with their local fusion centers and intelligence/law enforcement professionals. It would be a significant accomplishment to contribute to the development of a fire service model of information sharing; specifically, a model for timely and effective dissemination that can be used throughout the United States. The purpose of this thesis is to recommend an effective model for dissemination of intelligence that can be used as a reference for fire service agencies if they make a decision to invest in an intelligence enterprise within their organizations.

E. HYPOTHESIS

This thesis hypothesizes that in order for the nation's fire service to continue to evolve as a valuable partner with the IC, it needs to take the steps required to participate in the information sharing process and become better consumers of intelligence.

Closing this gap is important so that the fire service can reduce risk to its members and be better prepared in advance of a terrorist attack, or any other disaster situation confronted. Enhanced preparedness is essential to the core mission of the fire service, as it contributes to its ability to save the most lives.

The process of improving the sharing of intelligence has begun at the federal, state, and local levels through multiple initiatives developed in recognition that the fire service is a valuable partner in every phase of the intelligence cycle by virtue of their duties at fires, emergencies, and medical responses everyday nationwide.

It is important for the IC and law enforcement to have the ability to communicate terrorism/criminal related information and intelligence to the fire service to enhance their level of preparedness, inform their response operations, and support the protection of first responder personnel. This two-way process is still evolving, and continues to evolve as information-sharing initiatives become more mature and better support the development of communities of interest at the federal, state, and local levels. Currently, 72 established intelligence fusion centers exist in the United States. A recent report by the DHS indicates that the integration of the fire service into this information and intelligence-sharing network is progressing. As of October 2009, varying degrees of fire service participation occurred in 48 out of 72 fusion centers (DHS I&A Report, 2009).

As fire service participation expands, and the macro level sharing of intelligence between the fire service and the intelligence/law enforcement communities becomes more recognized as a matter of course, it is then necessary for fire service agencies to develop internal mechanisms of disseminating intelligence to field level personnel. If they do not receive timely, credible, and actionable information, driven by the intelligence process, prior to and during response operations to all hazards incidents, their lives, as well as the lives of the public they are trying to help, can be jeopardized. Situational awareness of incidents is critical to responder and public safety.

Two areas of concern need to be addressed when developing the capability of sharing sensitive or classified information as determined by the producers of intelligence:

- The need for fire service personnel at different levels of command within an organization to possess a security clearance. Classified Information may contain information relevant to firefighters and/or EMS personnel at the executive levels and in the field. Relevant fire service personnel need to be trained on how to handle this type of intelligence and must possess the necessary clearances to access it. Fire service personnel also need to be cognizant of the dangers related to compromising law enforcement investigations. Law enforcement relies on sources for information. It also needs to protect its sources from media exposure during investigations. Fire service personnel trusted with handling this type of intelligence should receive training in this regard. An alternative to requiring security clearances may be to train analysts to sanitize intelligence to lower classifications for consumption, being mindful to keep it actionable.
- For the fire service to be effective participants in the intelligence process, it must be aware that its typical good standing with the public can become compromised. Fire service personnel given intelligence responsibilities need to be aware of the constitutional boundaries surrounding these issues in the performance of this new activity. If the fire service becomes identified as being a part of the intelligence process, what traditionally has been viewed as a trustworthy relationship, can be eroded. If firefighters become perceived as engaging in what has typically been a law enforcement capacity during the course of their duties, the public may be less willing to allow them access to their premises.

By analyzing a sample of fire service agencies around the country that have made efforts to participate in the intelligence process, the author can then research the hypothesis that, in order for the nation's fire service to continue to evolve as a valuable partner with the IC, it needs to take the steps necessary to participate in the information sharing process and become better consumers of intelligence.

II. LITERATURE REVIEW

The IC and the law enforcement community have only recently realized the value of the fire service as a partner in the intelligence discipline. Due to this new and emerging relationship, relatively little literature or scholarship about how information should be shared between the intelligence/law enforcement communities and the fire service exists. The literature review includes the following sections.

- ***Identifying Intelligence Requirements*** discusses current initiatives to determine what and how information should be shared between the intelligence/law enforcement communities and the fire service.
- ***Application of Intelligence for Planning and Operations*** presents the intelligence cycle as a tool to be used for creating intelligence products for a wide range of public safety and emergency services organizations.
- ***Mechanisms for Disseminating Information and Intelligence*** covers existing mechanisms to deliver intelligence to the firefighters.
- ***Information/Intelligence Classification Barriers*** discusses understanding the process of security clearances and how information is categorized.
- ***The Role of Training Programs*** explains the need for training for this new and non-traditional relationship between the fire service and the intelligence/law enforcement communities, including the appropriate stages of the intelligence cycle for fire service participation.

A. IDENTIFYING INTELLIGENCE REQUIREMENTS

Work has commenced at the federal, state, and local levels to identify the intelligence needs of the fire service.

The process for disseminating intelligence to the fire service can only be successful if the fire service can identify what type of information and intelligence it needs, as well as the importance of participating in the analysis stage of the intelligence cycle. This participation assists in the production of intelligence reports relevant to the fire service.

In April of 2009, DHS Office of Intelligence and Analysis (I&A), Office of Infrastructure Protection (IP), and the U.S. Fire Administration (USFA) held a workshop to discuss emergency services sector information and intelligence requirements. Participants were from a cross-section of emergency services disciplines including fire, rescue, hazardous materials, law enforcement, emergency medical service, and emergency management personnel. The after action report of the workshop revealed several issues.

- It was recognized, that at present, a universal lack of understanding of what each discipline within the emergency services does, and what exactly the IC does exists. What should the relationship look like? Many cross-disciplinary intelligence requirements abound, but each discipline also has unique requirements for intelligence.
- It was articulated that intelligence analysts generally do not understand the role of those in the emergency services and how the emergency services can be a valuable partner in the fusion process (DHS Workshop 2009, p. 7). This represents a serious gap in the ability of the IC to become a producer of intelligence useful to the emergency services.

B. APPLICATION OF INTELLIGENCE FOR PLANNING AND OPERATIONS

The role of the fire service is relevant in every part of the intelligence cycle. Intelligence requirements are defined in the planning phase, and then the corresponding information needs identified. Collection is relevant for suspicious activity reporting (within the confines of the law), and sharing of internal fire department information, such as information obtained from performing building inspections or what is observed during the course of normal response activities. Fire service personnel can provide their subject matter expertise to produce more

relevant intelligence products for fire service personnel consumption. Dissemination is relevant because fire service personnel are intelligence customers and consumers and may be able to identify other important consumers to enhance responder and public safety. Evaluation of intelligence products is critical to let analysts know if the fire service is obtaining what it needs.

A recent report published by DHS, “Fire Service Integration for Fusion Centers” (April 2010), explains how intelligence and information are now important elements to support fire service preparedness for response and recovery missions (Security, 2010). To take advantage of intelligence products for planning and operations, first responders also need to understand clearly what intelligence can actually do for them. The Intelligence Guide for First Responders lists some valuable uses for intelligence.

- Provide decision advantage, by improving the decision-making of consumers
- Warnings of potential threats
- Insight into key current events
- Situational awareness
- 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 (ITACG, 2009).

While the above points illustrate the value of intelligence, first responders should also have realistic expectations; intelligence can assist with preparing and responding but cannot predict nor prevent everything that may be confronted.

Intelligence can also provide a mitigation function for first responders. Mitigation is typically the process of reducing or eliminating risks. Intelligence-led policing, which originated in the United Kingdom during the 1990s, has been suggested as the model for what is termed intelligence-led mitigation. In a recent white paper (February 2010) Townsend, Sullivan, Monahan, and Donnelly present a case that intelligence-led policing and intelligence-led mitigation use

the intelligence cycle as a basic tenet. The authors cite the New Jersey State Police Practical Guide to Intelligence–Led Policing, which states that the intelligence cycle "seeks to set appropriate tasking priorities for the colllection of basic data, process that data into an easy useable format, analyze it to create situational awareness through intelligence products that support tactical, operational and strategic needs, then disseminate those products to customers who provide feedback on what additional or new intelligence requirements remain. The cycle begins anew as new requirements are again balanced against command guidance, operational needs, and resource constraints" (Townsend, Sullivan, Monahan, & Donnelly, 2010). Their claim is that intelligence-led mitigation uses the same cycle but provides products and support to a larger group of stakeholders, which includes all public safety and emergency services entities.

C. MECHANISMS FOR DISSEMINATING INFORMATION AND INTELLIGENCE

In order for the information sharing process to be meaningful, a mutual understanding must exist between the intelligence/law enforcement communities and the fire service that there is value added in this relationship, which is evolving because of the work being done through numerous federal, state, and local efforts. The IC is also being encouraged to change its way of thinking as it relates to information sharing. Lee Hamilton, former Vice Chair of the 9/11 Commission stated, "we have made minimal progress toward the establishment of a seamless information sharing system. You can change the law, you can change the technology, but you still need to change the culture; you need to motivate the institutions and individuals to share information" (CRS Report, 2006). The Intelligence Reform and Terrorism Prevention Act of 2004 required that the president establish an Information Sharing Environment (ISE) "for the sharing of terrorism information in a manner consistent with national security and applicable legal standards relating to privacy and civil liberties." The ISE mainly

focuses on how to coordinate access to and the sharing of protected terrorism information (Program Manager, 2006). In December 2005, President Bush issued a presidential memorandum titled “Guidelines and Requirements in Support of the Information Sharing Environment.” In the memorandum, he clearly defines the guidelines for information sharing to be used at all levels of government.

The fire service in the United States may not have to start from scratch when trying to determine how to disseminate intelligence to field forces. In his thesis for the Naval Postgraduate School (NPS), Bryan Heirston describes how the United Kingdom’s Civil Contingencies Act of 2004 included a significant role for the fire service in the intelligence cycle, specifically related to information sharing to prevent terrorism.

One of the primary concerns about sharing information, as noted by Heirston, pertains to the sharing of sensitive information. Sometimes, intelligence contains information that can compromise sources or ongoing investigations. The United Kingdom model of sharing sensitive information uses fire liaisons (battalion level chiefs in the United States), and executive-level officers (deputy or staff chiefs in the United States). The fire liaisons have advanced security clearances and have direct contact with the intelligence community to receive intelligence. If sensitive information is contained in the intelligence product, the liaisons have the training to be able to share the relevant information with the field forces without compromising the sensitive/classified nature of the information (Heirston, 2009, p. 63).

As of 2010, 72 DHS designated state and major urban fusion centers operated throughout the United States, with many additional local and regional fusion centers also operating throughout the country. Their existence is a testament to the fact that homeland security leaders have recognized the value of centralizing intelligence gathering and analysis to assist in preventing and responding to terrorist threats (CRS Report, 2006). The fire service integration

into state and major urban area fusion centers is showing some promise. The latest report (October 2009) released by the DHS, regarding the status of fire service integration within state and major urban area fusion centers, shows that 48 of the 72 established fusion centers (67%) are performing outreach to state and local fire service organizations and/or looking at options for integration in the future (DHS Report, 2009).

D. INFORMATION/INTELLIGENCE CLASSIFICATION BARRIERS

In order for fire service personnel to integrate fully into the intelligence process and be able to disseminate information, the literature indicates that the issue of security clearances must be addressed. What constitutes “classified” information? Can Unclassified/For Official Use Only (U/FOUO) information be vetted to extract what is needed by fire service personnel to protect its members? Information labeled law enforcement sensitive (LES) is generally considered not consumable by other than law enforcement personnel. How can that information-sharing barrier be overcome?

Presidential Executive Order 13356 of August 2004, Strengthening the Sharing of Terrorism Information to Protect Americans, requires that records and reports related to terrorism information be made available at an unclassified level as much as possible to allow personnel with the appropriate training, access for sharing with their agencies (Executive Order 13356, 2004).

In his 2002 article, “Bridging the Intelligence Gap,” David J. Rothkopf acknowledges that the culture of secrecy in the intelligence community has slowed its growth and caused distrust to develop between the IC and the newly recognized collectors and consumers at the state and local level. He brings attention to the importance of meeting the new challenge of collaboration among all participants in the process.

An interesting perspective to the security clearance issue is highlighted in a special report by the U.S. House of Representatives Committee on Homeland Security, which includes a recommendation by the Heritage Foundation for the federal government to declassify as much information as possible instead of requiring security clearances for intelligence consumers. This recommendation asserts that the cost of obtaining security clearances is an undue burden for state and local entities when they are trying to assist the federal government in protecting the nation (House of Representatives Report, 2005, p. 17).

E. THE ROLE OF TRAINING PROGRAMS

Training fire service personnel in the intelligence discipline helps to formalize the relationship with IC members and other homeland security partners. Programs already exist in Colorado, Arizona, and Indiana, among others that can be used as models for training program development. For example, the Terrorism Liaison Officer (TLO) program in Arizona incorporates fire service personnel and includes a state certified 40-hour training program and a security clearance to have full access to intelligence products produced at the state fusion center (Salyers & Lutrick, 2007).

The Global Justice Information Sharing Initiative, *Fusion Center Guidelines, Developing and Sharing Information and Intelligence in a New World*, offers in guideline #13 recommendations for multidisciplinary awareness and education. The guideline specifically states, “provide a multi-tiered awareness and educational program to implement intelligence-led policing and the development of sharing of information” (Global Justice, 2005, p. 67). The key point made is to include non-traditional partners in intelligence, which includes the fire service.

THIS PAGE INTENTIONALLY LEFT BLANK

III. RESEARCH METHODOLOGY

As illustrated in the literature review, very little documented evidence exists of how the fire service is participating in the intelligence sharing business to date. The establishment of the FSIE has increased the awareness of the IC, law enforcement, and fire service of the need to continue developing this new partnership but more needs to be done. There are approximately 33,000 fire service agencies in the United States. Only 15 agencies initially participated in the FSIE. This low number indicates that the fire service has much work to do if it is going to increase its ability to assist in the prevention of terrorist acts, as well as provide enhanced safety to its members while performing their routine daily duties or when responding to major disasters resulting from a natural calamity or that may have a nexus to terrorism. This thesis evaluates methods used to overcome the challenges of information and intelligence sharing to develop recommendations for better dissemination mechanisms that fire service agencies can use to improve relationships with the intelligence/law enforcement communities.

How can information and intelligence be better disseminated to local first responders to enhance situational awareness, provide a higher degree of responder safety, and better protect the public? To answer the research question, several steps were taken to gather information for analysis.

A combination of methods was used to gather and analyze information. First, structured interviews were conducted with subject matter experts from the fire service and homeland security disciplines to determine what methods already exist for disseminating intelligence and information to first responders. The interviews were conducted by telephone. Second, a six-question survey was developed using an online service and was distributed to 40 first responder fire chiefs, including career and volunteer fire service agencies. (See Appendices A and B for a list of the interview and survey questions used for the research). The

survey was conducted to solicit information from field responders on what type of intelligence would be most helpful to them in the field, and how they would like to receive the intelligence, to enhance safety before, during and after a response to a significant event. The survey was designed and conducted using methods described in Survey Research Methods (Third Edition, 2001) by Floyd J. Fowler Jr. The survey questions were presented in an open-ended format to allow respondents to answer without limits or restrictions. The answers were analyzed and the results summarized as illustrated in Figures 2 through 7 in the analysis chapter. Knowing what field responders want and/or need can assist in developing the best tools needed to disseminate the information.

In addition to conducting the interviews and survey, additional information was gathered by researching fire service agency and DHS websites, and fire service trade magazines for technological initiatives that have been researched and developed for assisting with the dissemination of intelligence and information. The intent of the additional research was to gather additional data to support recommendations on how to disseminate intelligence and information efficiently to field responders to enhance their decision-making before, during, and after an incident.

Eighteen people were interviewed for this thesis. Interview subjects were chosen for their involvement in the FSIE initiative, their work within the DHS Intelligence Enterprise. Others were selected to obtain a law enforcement perspective on intelligence and information sharing.

Nine fire service representatives were interviewed. Of the nine, six represented fire departments that were original participants in the FSIE initiative; two were fire service representatives currently working with the National Counterterrorism Center's Interagency Threat Assessment and Coordination Group (ITACG), and one was the director of a large urban Fire Department Operations Center. The remaining interview subjects were representatives from DHS, including the United States Fire Administration, the Office of Intelligence

and Analysis State and Local Program Office, the Emergency Services Sector of the Infrastructure Protection Office, two law enforcement officials with intelligence backgrounds, and two fire service graduates of NPS. The assumption was that the subject matter expertise of all the interview subjects provided for a valuable comparative analysis.

After all data were collected, a qualitative analysis was conducted to understand what is being done in different agencies to identify best practices in the dissemination of intelligence down to the local level. Best practices are identified on the FEMA website, Lessons Learned Information Sharing (www.llis.gov), as exemplary, peer-validated techniques, procedures, good ideas, or solutions that work and are solidly grounded in actual operations, training, and exercise experience.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. ANALYSIS

A. STRUCTURED INTERVIEWS

Interview subjects were asked a series of open-ended questions to determine what is currently being done within their organizations regarding the identification of and the use of intelligence, as well as how and if they prepare their personnel for this new role. Once the interviews were completed, a qualitative analysis was performed using a manual data coding process to identify the key themes from the interviews and provide a detailed narrative related to the interview questions.

1. Responses and Analysis to Question 1

- What is the role of intelligence within your organization?

The overarching answer to this question was that intelligence is used to provide situational awareness for first responders. What actually is situational awareness? Situational awareness was most commonly defined as knowing what is going on around you. Most fire department training programs often incorporate references to situational awareness. This phrase has become one of the new buzzwords in the fire service. Firefighters and other first responders are constantly reminded to know where they are, observe what is going on around them and to be diligent in reporting anything unusual. In the context of firefighting and emergency operations, it is a matter of life and death. When a firefighter is crawling around a building that is on fire, they must rely on their training and experience to perform their assigned tasks safely. In addition, they must perform an adequate size-up while responding to an incident, when they arrive at an incident and throughout the incident until the incident is deemed to be under control. They must anticipate what may happen next. A difference exists between static situational awareness and dynamic situational awareness. Static situational

awareness means an assessment at a particular moment in time of an incident. Dynamic situational awareness is an evolution of scene size-up. It not only involves understanding the current situation, it allows a responder to anticipate how the situation might change and to be able to react to the changing environment (Townsend, Sullivan, Monahan, & Donnelly, 2010, p. 5). Understanding dynamic situational awareness is the framework for a better-informed decision-making process at an incident. One of the interview subjects defined intelligence as “information that is relevant to your decision making process” (T. Herlocker, personal communication, April 28, 2010).

Another factor that is a consideration regarding the role of intelligence is how intelligence products are used. Interview subjects indicated that the intelligence products could be used in three ways.

- They can be used to discuss emerging trends to develop training programs to increase the awareness of responders.
- In real time, as an incident is evolving, intelligence can be used to make deployment decisions. As an example, one interview subject reported that if his organization receives intelligence that identifies a credible threat to first responders, it might direct its field personnel to enhance security on fire apparatus and in fire department facilities. Another example provided speaks to the importance of cooperation between law enforcement and the fire service. If a fire department were responding to a house fire that local law enforcement knew was under surveillance for suspicion of containing bomb-making materials, it would be critical for that to be communicated to the responding units. Prior to the incident, that information may not have to be given to the firefighters or fire officers in a local station, but it probably should be given to the individuals responsible for making the strategic and tactical decisions in the event of a response to that location. It would be their decision on how to make the local firefighters and fire officers aware.
- Intelligence is utilized to analyze threat assessments to facilitate the strategic planning processes. For example, if threat assessments indicated that improvised explosive devices (IED) in combination with radiological materials are a concern, a priority in planning may be to invest money in purchasing detection equipment and developing training programs to educate and protect first

responders on this particular hazard. During the World Trade Organization (WTO) conference in Seattle in 1999, the role of intelligence was to inform local first responders of what groups might be coming into their jurisdiction to be able to understand the threat element, what kind of tactics and techniques they used, and what potentially could be the effect on local first responders. "If there were anarchists who would blow things up or set fires, the fire department would want to know" (M. Washington, personal communication, June 14, 2010).

2. Responses and Analysis to Question 2

- What effect has the FSIE had on intelligence and information sharing for the fire service?

The FSIE has been a DHS management initiative to reach out to subject matter experts within the fire service to discuss the fire service information and intelligence sharing issue. The intent was to get buy-in from the fire service in understanding the benefits of intelligence and information sharing for their stakeholders. Representatives interviewed for this thesis claimed that the FSIE put the fire service "on the map recognizing that we need to be a player in the intelligence world" (T. Herlocker, personal communication, April 28, 2010). It has recently been described as "more of an ad-hoc group that gets together and discusses specific issues" (personal communication, June 14, 2010). A new focus has been to change the face of the FSIE by removing the word "intelligence" from the initiative and using "fire service information sharing" as the public face for the effort.

The FSIE has been the catalyst for getting the fire service involved in the intelligence business. One interview subject believes that a key aspect of the FSIE is to enable the sharing of best practices among and between fire service organizations. Another interview subject stated that he was not sure that there actually has been a one to one relationship between the FSIE and the actual sharing of information and intelligence. He feels that other initiatives happened parallel to its formation, in particular, the development of fusion centers. The

recently published appendix to the Baselines Capabilities for State and Major Urban Area Fusion Centers, Fire Service Integration for Fusion Centers, is a key doctrinal piece to continue the development of the fire service information sharing initiative. However, as stated by one interview subject, “it is a good start, but the proof will be when and if we actually get fire service representatives into the fusion centers” (M. Washington, personal communication, June 14, 2010). At present, fire service representation in fusion centers is on a broad spectrum, ranging from no representation to very intricate relationships. In Arizona, fire and police are tightly woven in the Arizona Counterterrorism Intelligence Center (ACTIC). In another large U.S. city, the fire service representative is not even allowed inside the fusion center, he may get a phone call or an e-mail with information, if he is lucky.

To demonstrate how the FSIE has highlighted the importance of fire service participation in fusion centers, one of the interview subjects cited attendance at some of the recent fusion center conferences. At the very first conference, 25 fire service personnel attended out of 900 attendees. The following year, roughly 100 fire service personnel attended. At the most recent conference, approximately 200 fire service personnel attended (R. Palestrant, personal communication, April 29, 2010).

3. Responses and Analysis to Question 3

- Does your agency have trained Terrorism Liaison Officers (TLO)? If so, how and where do they receive their training? What are their duties and how do they interact with field responders?

Only a few of the organizations represented by the interview subjects have TLO. All acknowledged that the program could benefit the intelligence and information sharing process but also commented, “one size does not fit all.” The general consensus was that if a TLO program were to be adopted, it should be customized to the needs of the jurisdiction and that it also be dependent on the existing relationship with the law enforcement community.

What is a TLO? It is an individual trained in handling and processing intelligence documents and information. Different models of TLO programs exist as described by the interview subjects. Some of the organizations represented have several TLO while others that also have them only have one. Other organizations used other personnel as “TLO” without the particular title. In fact, some even suggested that a different name be utilized for the job duties to reflect the all-hazards nature of fire service work more accurately. Other suggested titles were Fusion Liaison Officer or Field Intelligence Officer.

Representatives from the organizations that do have TLO indicated that the duties and responsibilities, as well as the training, varied. One west coast department has essentially one TLO who represents fire departments in fifteen separate counties. He describes himself as more of a facilitator for disseminating information. He has built a core network of fire chiefs who receive information from him but, according to him, they may or may not disseminate the information any further. The network he developed enables him to offer TLO training in several formats. His state has a state certified TLO program, which is eight hours, or one day of training. This is considered an introductory program. There is a three-day intermediate program (twenty-four hours) and an advanced (forty-hour) program. He also provides what he describes as a mini-TLO program; a three hour presentation tailored for the line firefighter and fire officer, essentially an awareness level program on terrorism, which covers indicators and warnings, legalities, how to report suspicious activity, and a familiarization with the regional fusion center; what it is and how to contact them. His biggest challenge is marketing the value of these programs and getting the buy-in from the fire chiefs (S. Francisco, personal communication, April 17, 2010).

Another fire chief interviewed, from a major city on the east coast, claimed he uses a hybrid TLO program. They have one trained TLO on duty, their special operations chief who is the first point of contact for reporting suspicious activity, and is the liaison with other agencies in the city. His suggestion is that if a jurisdiction were to endorse and adopt a TLO program, it needs to be built for the environment that it is in (J. Donnelly, personal communication, April 26, 2010).

In a large southeast city, the fire department representative uses what he describes as administrative TLO's. They use a tiered approach to delivering TLO training, and they first trained all of their civilian employees with a TLO awareness program. This included administrative employees, fire inspectors and facilities personnel. The intent was to enable them to recognize and be able to report suspicious activity. He highlighted that this training was done at no cost to the organization because it was done while the employees were working and required no expense to backfill their positions. His hope is to acquire funding in the future to train the "boots on the ground" battalion chiefs, fire officers, and firefighters in a minimum eight-hour program, with a goal of eventually developing a thirty-two to forty-hour program. Currently, he has administrative TLO's working in the regional fusion centers that have developed an excellent working relationship with fusion center personnel. With the additional training to field personnel, his vision is to expand the TLO program to have both administrative TLO's and on-scene response TLO's (R. Palestrant, personal communication, April 29, 2010).

All of the fire service representatives interviewed emphasized one TLO model that, in their views, represented what some of them termed as the "Cadillac" model for TLO programs. This program is in the state of Arizona in the Phoenix metropolitan area. The representative from this program provided a comprehensive description of their program. The TLO program in this region is a forty-hour DHS approved program, which allows them to compete for grants to fund the program. It is also approved by the state of Arizona, which enables law

enforcement personnel to obtain continuing education credit hours for completion. The backbone of the program is about intelligence and information sharing; however, the curriculum is specific for their jurisdiction. The unique component of the Arizona program is that most of the value comes from the focus on the response mission. Response TLO's actually become the Intelligence Section within the Incident Command System (ICS) and respond with a laptop computer, and are able to share relevant information from the Arizona Counterterrorism Intelligence Center ACTIC with the incident commander. Literally, they are able to show the incident commander (IC) what they can bring to the table relative to intelligence, whether it is criminal in nature, a person or location that might pose a threat to firefighters; or something about the structure they are operating in that poses a threat. An extremely important aspect of this program is that no difference exists between a police department intelligence officer and a fire department intelligence officer other than one carrying a gun and the other a hose. In fact, the TLO's in this region are actually referred to as "guns and hoses." The fire TLO has the clearance and capability to obtain criminal intelligence if needed and pass it on to the IC. As an example, if the fire department were to make entry into a building after it was deemed safe by the police resources on scene, and there was a need for them to recognize a perpetrator, the TLO has the capability to receive a photograph of the person and brief the firefighters on the scene before making entry. Another example of the excellent working relationship that exists is regarding SWAT team operations. When the Special Weapons and Tactics (SWAT) team is being deployed to a location, the fire department TLO is notified and responds. Fire department emergency medical units are staged in the area in the event a police officer is injured, for a quick deployment. In addition, the TLO is able to advise the dispatch center that police department activity is occurring in the area so that units that might be responding to other alarms in the area are aware. The TLO gives clearance to those units when it is safe to respond. This also prevents the other responding units from warning the perpetrators prior to the police

department deploying their personnel. The TLO advises them to respond without lights and sirens when entering the area (R. Salyers, personal communication, June 14, 2010).

4. Responses and Analysis to Question 4

- How does your agency disseminate intelligence?

This question also presented a variety of responses. The most frequent responses were that the represented organizations prepared and disseminated weekly bulletins. One department disseminates a daily bulletin to all staff level chiefs.[2] Some departments circulate information only as needed or depending on if specific intelligence requires action for dissemination.

The representative from a mid-west department that disseminates a daily bulletin explained that the staff level chiefs receive it, and only if something is applicable to a local area or specific unit, is it disseminated. If that becomes the case, it requires approval from a deputy commissioner or a staff chief. It was interesting to note that he mentioned that the police department shares information with local emergency medical response (EMS) units regarding gang activity. They do this through the local district fire battalion chiefs and not through fire department headquarters. Other information disseminated is mined from special reports from DHS. No analysis is provided; just raw information, which is usually sent to special operations units or bureaus, such as the fire marshals or hazardous materials response units (J, Dennis, personal communication, April 2, 2010).

[2] Staff level chiefs are usually the senior management of a department. An example would be the Fire Commissioner, the Fire Chief, and the Chief of Operations. It may be different in a smaller department.

Those departments that published weekly documents claim that a daily brief may tend to desensitize the average first responder and they may not read it regularly. The consensus was that a weekly document provides a reasonable frequency that can provide the necessary information, such as significant events that can affect fire department activities. Most of those producing a weekly bulletin include local, national, and international information.

One department provides a weekly Monday morning brief via an e-mail to a secure folder on the fire department Intranet, which is a read only document that cannot be copied or printed. Fire department units are required to use the information from the brief for drill purposes for the succeeding four days to cover all shifts of personnel. In addition, a weekly conference call briefing is conducted on Monday mornings with the special operations units (J. Donnelly, personal communication, April 26, 2010).

The New York Fire Department (FDNY) produces a weekly bulletin called Watchline, which is department-wide and addresses all-hazard FDNY specific mitigation and response missions “to keep members abreast of new dangers and guard against complacency in the absence of new incidents” (FDNY, 2007). Watchline is the specific mechanism for disseminating all hazards information to the field. It is circulated via e-mail to all units through their e-mail accounts. The bulletin contains relevant and current unclassified information with recommendations to review specific department publications and training bulletins depending on the events described. Watchline is categorized as Unclassified/For Official Use Only (U/FOUO). No requirement exists to use the information contained in Watchline for drill purposes. It is available to chiefs and officers if they choose to do so.

The Seattle Fire Department has no formal product within for disseminating intelligence. If a threat exists, an informal method is used. As an example, if a dangerous situation occurs relating to a particular building, such as a structural problem, the local responding stations are notified via internal

communications. Regarding a terrorist threat, the local battalion is briefed by senior staff and sometimes invited to a Joint Terrorism Task Force (JTTF) meeting to receive unclassified information that can be shared with responding units (M. Washington, personal communication, June 14, 2010).

One other department utilizes conference calls with their on duty chiefs to disseminate intelligence that is time sensitive for them to be able to advise their responding units. The information is carefully vetted to provide only what they need to know to keep their members safe (J. Donnelly, personal communication, April 26, 2010).

5. Responses and Analysis to Question 5

- Are you aware of any models, other than your own agency, for intelligence sharing and dissemination currently being used in the fire service that have been successful?

Most of the interview subjects again mentioned the Arizona program but other examples were highlighted as well for specific parts of their programs. FDNY representatives discussed the state of New Jersey fusion center, the Regional Operations Intelligence Center (ROIC), as a good example for disseminating intelligence because it provides an all hazards approach and not an all crimes approach to producing and sharing intelligence (personal communication, April 28, 2010). The fusion center in the National Capital Region (Washington, D.C.) uses a model where distribution is to a single point of contact within each of the participating fire service agencies. Each agency has a designated point of contact responsible for making the information pertinent to their agency and disseminating it according to their protocol. Their regional fire intelligence group is encouraging fire departments to push the information into secure folders on their Intranets accessible to all personnel in the agency, mostly FOUO information. If the information is of higher classification, then conference calls are conducted with the intelligence-working group with those possessing the security clearances. The next evolution in the National Capital Region is to avoid

individual internal dissemination and instead have the fusion center push the information into the Homeland Security Information Network (HSIN) and have the approved personnel establish HSIN accounts. The intent is to warehouse the data in one central location for access. The process for obtaining HSIN accounts is not very complicated as long as the agency sponsors its personnel. In this system, an added benefit is that when something of interest is posted, all participating partners receive an e-mail. The only concern with this type of mechanism is the issue of being comfortable with the federal government becoming the main point of distribution (J. Donnelly, personal communication, April 26, 2010).

6. Responses and Analysis to Question 6

- Does your agency have a representative in the local/regional fusion center? If not from your agency, is there a fire service representative? Is that person well received and a respected partner?

Of the fire service representatives interviewed, only three had representatives in the fusion centers. Washington, DC Fire/Rescue has a fire service analyst in the fusion center funded through a grant. Their representative is very well received and was described as “an integral part of the fusion center.” They also have a fire lieutenant with intelligence responsibilities who has full access to the fusion center (J. Donnelly, personal communication, April 26, 2010).

A different model exists in Miami-Dade Fire/Rescue. Three people from their Terrorism Response Bureau are assigned to the fusion center, who are members on light duty assignment and have been very well received by their counterparts in law enforcement. This relationship is two years old and continues to evolve. Their fusion center is divided into sectors representing some of the critical infrastructure sectors, such as transportation, public health, chemical/biological, banking/finance, and energy. They also have a sector for

Weapons of Mass Destruction (WMD). Analysts are assigned to each sector, and the three fire department representatives are assigned between one and three sectors as areas of responsibility. One of the unique features about Miami/Dade's regional fusion center is that the law enforcement and fire representatives assigned not only work together in the fusion center but they also interact out in the field by making visits and establishing relationships with representatives working in the various sectors. This allows them to better understand what the issues are from a security standpoint in each sector (R. Palestrant, personal communication, April 29, 2010).

The Phoenix metropolitan area also has fire service representatives in the fusion center, which is a well-developed relationship through the TLO training program that they provide.

Seventy-two fusion centers are up and running throughout the United States. Their existence is a testament to the fact that homeland security leaders have recognized the value of centralizing intelligence gathering and analysis to assist in preventing and responding to terrorist threats (CRS Report, 2006). Having trained people integrated into a fusion center provides a greater opportunity for this information exchange to occur in a timely manner. The fire service integration into state and major urban area fusion centers is showing some promise. The latest report (October 2009) released by the DHS I&A, regarding the status of fire service integration within state and major urban area fusion centers, shows that 48 of the 72 established fusion centers (67%) are performing outreach to state and local fire service organizations and/or looking at options for integration in the future (DHS I&A Report, 2009).

7. Responses and Analysis to Question 7

- Does your local fusion center produce intelligence that is valuable for the fire service?

Most of the interview subjects could not answer this question in the affirmative. What they did state was that most of the products produced are law enforcement centric. One interview subject made a key point regarding the ability of a fusion center to produce a product relevant for the fire service, “it cannot be done in a vacuum. The fusion center acts on the intelligence requirements that we provide them” (J. Donnelly, personal communication, April 26, 2010). The FSIE working group has reportedly developed a currently unapproved list of national fire service requirements. The goal is to be able to give the requirements to the state and major urban area fusion centers so that analysts are aware of the fire service’s needs (J. Dennis, personal communication, April 2, 2010).

8. Responses and Analysis to Question 8

- What type of intelligence should be shared with first responders?

The answer to this question ranged from anything that can influence tactical decision making to enhance safety to as narrow as only terrorism-related information. The sense was that it depended on if those interviewed believed in an all-hazards or a terrorism-only approach to intelligence and information sharing. What was evident was that whatever was shared and disseminated would drive training and preparedness efforts.

9. Responses and Analysis to Question 9

- What would your recommendation be for an effective model for disseminating intelligence to field responders in a fire department?

The consensus was that the model should be discipline specific, in other words, tailored to the requirements of the discipline. Fire service requirements are very different from law enforcement requirements. We need to know what and where. Law enforcement needs to know who. Another suggestion was that

the model be layered depending on the size of the organization. In larger departments, the model using secure folders on an Intranet could provide security and also allow wide access within the agency. In a smaller department, personal communication from the hierarchy might be more timely and efficient. One key issue raised was the need to establish controls on the members of the respective departments to maintain security and sustain a good intelligence and information flow.

10. Responses and Analysis to Question 10

- What is your opinion on the issue of security clearances for members of the fire service with intelligence responsibilities? Are security clearances necessary?

The responses to this question were varied. Most thought that clearances were necessary for those individuals who work in the fusion centers or for those who attend regular briefings that contain intelligence that may be marked secret or top secret. Clearances are not necessary to have access to LES or FOUO intelligence. The consensus was that field responders did not require clearances; most of what they would receive or have access to generally becomes open source.

One interview subject commented that clearances do not necessarily facilitate inclusion in meetings but are used “as a crutch by other agencies to keep you out” (J. Donnelly, personal communication, April 26, 2010). Another interview subject stated that he has not used his clearance once in two and a half years, although now that he is working with the local Joint Terrorism Task Force (JTTF), he will probably have more use for it. He also stated that in his experience, the longer that he has worked face to face with law enforcement and the more their working relationship has developed, a sense of trust has been developed, which can enhance information sharing (S. Francisco, personal communication, April 17, 2010).

The most frequent comment to this question was the sense of frustration in the length of time it requires to obtain a security clearance, from either DHS or the Federal Bureau of Investigation (FBI).

11. Responses and Analysis to Question 11

- What is the range of classifications or sensitive markings for the intelligence products you receive?

The majority of the responses cited FOUO and LES. Some responses stated secret, and top secret but they were qualified by explaining that most of what the fire service needs is not at this level; however, there is value in some people possessing these clearances who have the ability to sanitize the intelligence to make it actionable.

12. Responses and Analysis to Question 12

- Are you aware of any specific programs to train fire service personnel in the intelligence process?

Currently, no fire service centric training programs exist to train fire service personnel in the collection of or the use of intelligence to enhance their mission to prevent, protect, respond and recover from terrorist, accidental, or natural disasters. A general consensus by some of the interview subjects indicated that most fire service chemical, biological, radiological, nuclear, and explosive (CBRNE) training classes contain terrorism-related information, and if modified to include the intelligence cycle and recognition of suspicious activities and how to report them, could become somewhat of an intelligence class. Some of the federal programs on response to terrorist incidents also could be modified in a similar fashion. One interview subject suggested that a definite need existed to train fire service personnel on information security and he claimed that it could be included in firefighter basic training programs and then tailored for the different

supervisory levels. He stated that this would be a significant step in being able to change this culture as far as information sharing was concerned (J. Donnelly, personal communication, April 26, 2010).

Another interview subject advised that training programs are available through the DHS/DOJ Fusion Process Technical Assistance Program and Services that, although not specifically for the fire service, acknowledge the fire service as a partner with a need for this type of training. As an example, one of the programs offered is Fusion Center and Fire Service Information Sharing and Coordination. This course as described provides support for jurisdictions as they consider coordination with and/or integration of the fire service into existing information sharing initiatives and assists fire service personnel to engage in existing fusion center information sharing processes (DHS/DOJ Fusion Process Brochure, 2008). Another available training opportunity to the fire service is through the Federal Law Enforcement Training Center (FLETC) in Georgia. One of the interview subjects suggested that training available at the FLETC would be valuable, particularly to train fire service personnel as analysts. His claim was that a fire service analyst adds value when interacting with law enforcement analysts; they would bring the fire service perspective to the table so that relevant products are produced for fire service consumption (R. Palestrant, personal communication, April 29, 2010).

B. SURVEY OF FIRST RESPONDER FIRE CHIEFS

A six-question survey was developed using an online service and was distributed to 40 first responder fire chiefs, including career and volunteer fire service agencies. The intent of the survey was to ascertain what their needs were regarding the type of intelligence or information they would prefer to receive, how they prefer to receive it, and if their agencies provide terrorism awareness training.

Of the 40 fire chiefs requested to participate in the survey, 30 completed the survey, a 75% response rate (see Figure 1). This response rate is consistent with what academic survey organizations are often able to achieve with general household surveys (Fowler, 2001, p. 42).

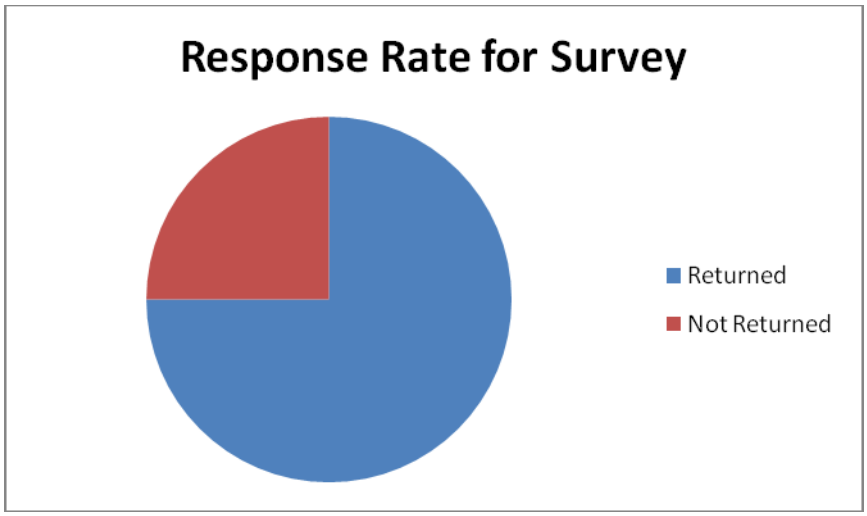

Figure 1. Response Rate for Survey

1. Response to Survey Question 1

- Question 1: What type of terrorist related intelligence do you think firefighters and EMS personnel need in order to more safely perform their jobs?

As shown in Figure 2, 11 (37%) of the 30 respondents stated they would want intelligence that briefs them on current threats and recent events.

Eight respondents (28%) wanted intelligence regarding what types of materials are being used by terrorists.

Five respondents (17%) wanted to know the modalities and tactics being used by terrorists.

Four respondents (13%) wanted information on potential targets in their jurisdictions.

One respondent (1%) wanted information on how to mitigate a current threat.

One respondent (1%) wanted to know the scope of local activity.

What is evident by the responses to Question 1 is that eighty-three percent (83%) of the respondents are interested in receiving intelligence that can assist them in preparation activities. Receiving information on specific threats, the types of materials used, and the modalities and tactics used, allows responders to develop appropriate training programs and purchase equipment that enables them to minimize risks to responders and the public.

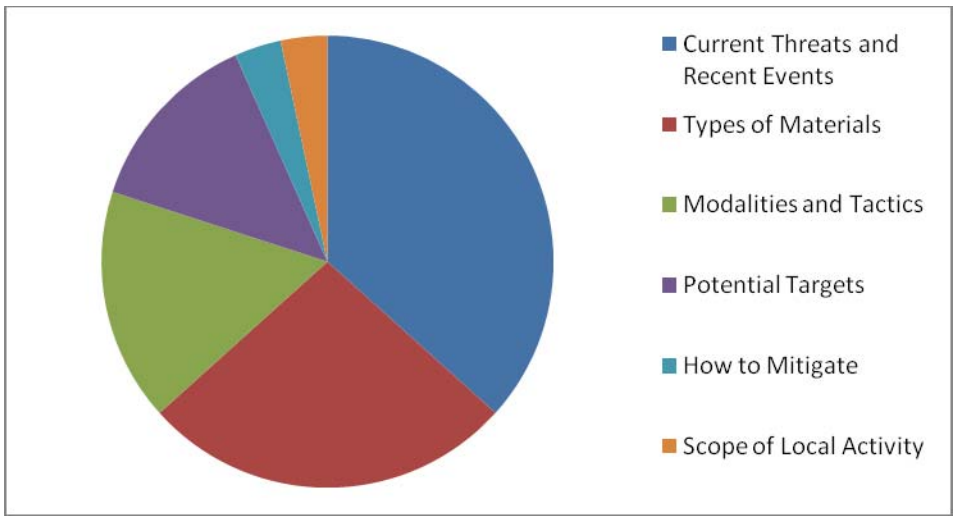

Figure 2. Responses to Question 1, "What type of terrorism related intelligence do you think firefighters and EMS personnel need in order to more safely perform their jobs?"

2. Response to Survey Question 2

- Question 2: Do you feel that it would be valuable to receive intelligence briefings regularly and from whom?

All of the respondents answered that they would benefit from regular intelligence briefings. Regarding from whom they would prefer receiving them, they answered as follows.

Seventeen of the respondents (57%) stated they wanted to receive the briefings from law enforcement officials.

Five of the respondents (17%) wanted to receive the briefings from their immediate superiors through the chain of command.

Three of the respondents (10%) wanted to receive the briefings from homeland security officials.

Three of the respondents (10%) wanted to receive the briefings from a fire service intelligence representative.

Two respondents (6%) wanted to receive the briefings from whoever had the most reliable and up to date intelligence.

An interesting result from Question 2 is that the fire chiefs want to receive their information from law enforcement officials. This reinforces the need for fire service agencies to develop effective information sharing relationships with their local law enforcement personnel.

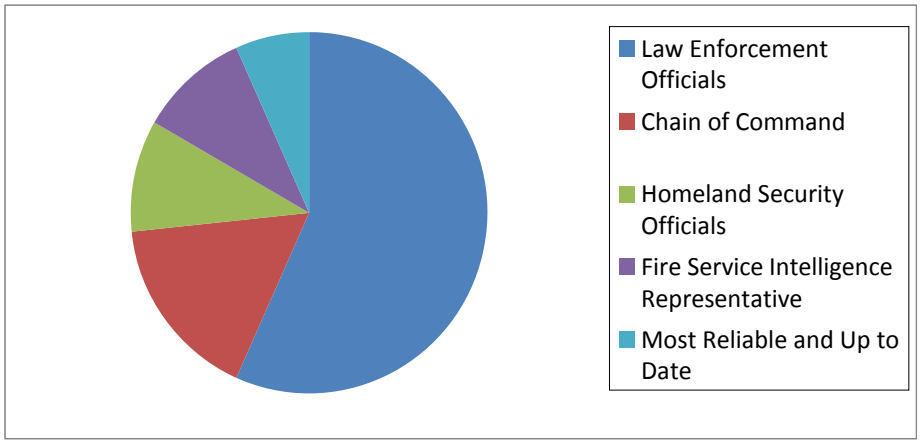

Figure 3. Responses to Question 2, "Do you feel that it would be valuable to receive intelligence briefings regularly and from whom?"

3. Response to Survey Question 3

- Question 3: How would you prefer to receive intelligence briefings, estimates, and assessments?

Sixteen of the respondents (53%) preferred to receive briefings via e-mail.

Eleven of the respondents (37%) preferred the briefings to be done at a group meeting or conference in person with those providing the briefing.

Three of the respondents (10%) wanted to receive the briefings in a written format, such as a bulletin.

Many of the interview subjects indicated that they either published or received a written document providing intelligence and/or information related to terrorism. Question 3 clearly indicates that most of the fire chiefs surveyed (90%) would rather have information provided in an e-mail or in person by a subject matter expert. A conclusion might be made that if written intelligence products were provided to first responders, they needed to be concise, providing actionable information that could be quickly digested.

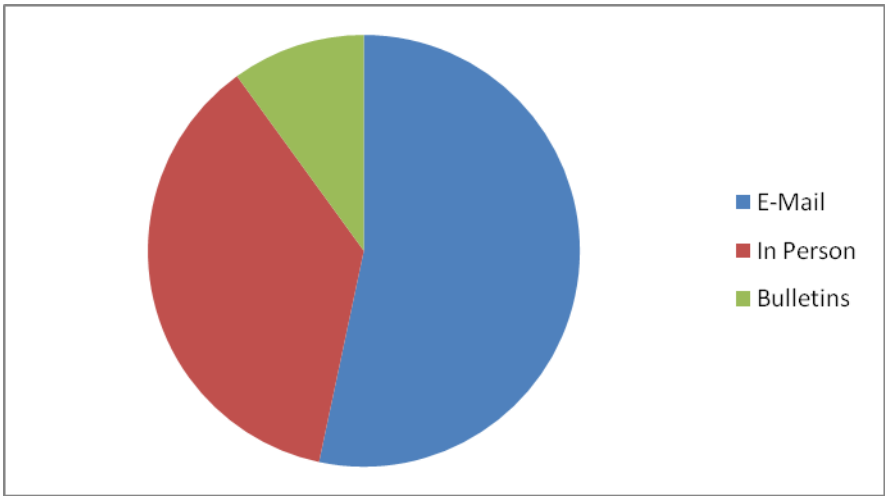

Figure 4. Responses to Question 3, "How would you prefer to receive intelligence briefings, estimates, and assessments?"

4. Response to Survey Question 4

- Question 4: What would work best in your agency to disseminate intelligence to members in the field?

The intent of this question was to determine what medium would actually be preferred to obtain intelligence down to the line unit level for the fire officers, firefighters, and EMS personnel.

The respondents had several answers to this question.

Ten (30%) of the respondents indicated that group conferences with chief officers would work the best. The chief officers could then disseminate the intelligence to the members in their commands personally.

Five (16%) of the respondents would like daily video conferences to have the information disseminated to the fire stations.

Five (16%) of the respondents wanted to use agency e-mail systems to disseminate the intelligence.

Five (16%) respondents preferred having intelligence sent directly to the computers in the fire apparatus and the ambulances in the field.

Three (10%) of the respondents would like to see a specific software program on a fire station computer to obtain the intelligence to the field responders.

Two (6%) respondents felt that it would best to disseminate intelligence in a classroom training session style.

What is important to note with the responses to Question 4 is that personal contact is the preferred method. This mechanism works well in the fire service at the line level for sharing information because in most fire service agencies, the local level fire chief has daily contact with subordinates several times during a shift.

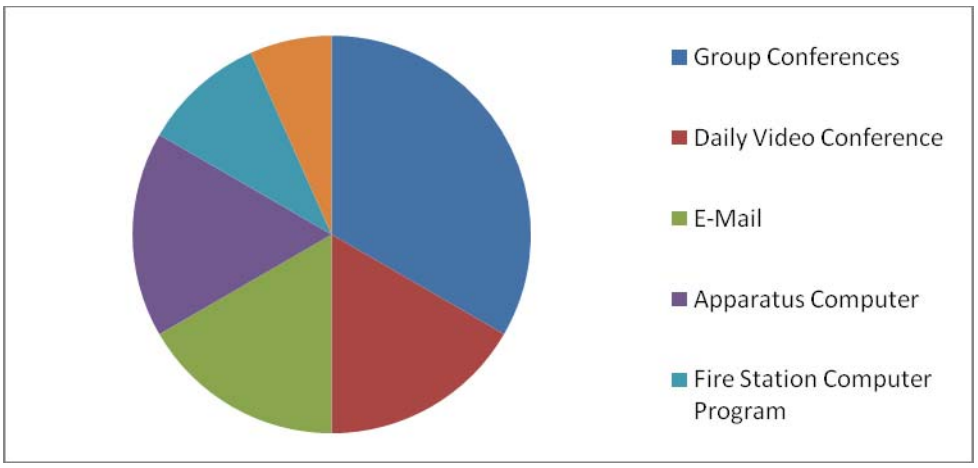

Figure 5. Responses to Question 4, "What would work best in your agency to disseminate intelligence to members in the field?"

5. Response to Survey Question 5

- Would regular intelligence briefings affect your daily operations?

Twenty-seven (90%) of the indicated that regular briefings would affect their daily operation and three (10%) indicated that they would not.

Although it is clear from the responses to Question 5 that regular briefings would affect their daily operations, several of the interview subjects cautioned that the briefings needed to be substantive; in other words, contain relevant and actionable information. If briefings were conducted just for the sake of conducting them, they risked becoming ineffective and could lead to desensitization to the information provided.

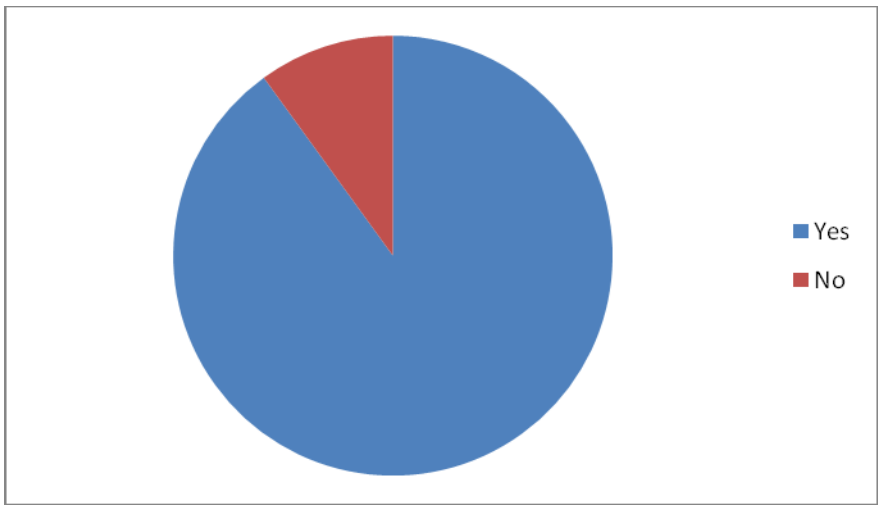

Figure 6. Responses to Question 5, "Would regular intelligence briefings affect your daily operations?"

6. Response to Survey Question 6

- How many hours of terrorism awareness training does your agency provide to personnel?

The responses to this question resulted in three categories for the number of hours that personnel receive terrorism awareness training.

Thirteen (42%) of the respondents reported that their members receive between eight and twelve hours of terrorism awareness training.

Nine (31%) reported that their members receive between one and four hours of terrorism awareness training.

Eight (26%) reported that they provide no terrorism awareness training.

It was encouraging to note that nearly seventy-five percent (75%) of the respondents are providing some level of terrorism awareness training to their personnel. Further research is warranted to analyze the curriculum of these training programs. The number of respondents not providing any terrorism

awareness training is a cause for concern. It is clear that most of the respondents consider terrorism awareness training necessary. Including this type of training in basic training programs for firefighters and then reinforcing it at supervisory levels could be effective in developing an adequate level of preparedness at the line level.

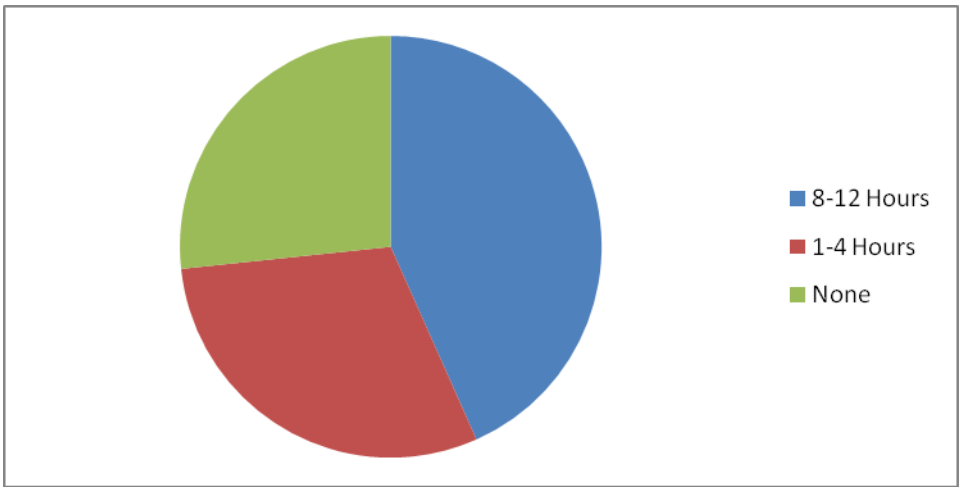

Figure 7. Responses to Question 6, "How many hours of terrorism awareness training does your agency provide to personnel?"

V. BUILDING EXECUTION INTO THE STRATEGY

The Fire Service Intelligence Enterprise (FSIE) is an initiative to incorporate the fire service into national standards, protocols, and mechanisms for homeland security information and intelligence sharing. The FSIE is the value innovation for the fire service in becoming an important component of the intelligence process. Instead of focusing on how to overcome the cultural barriers of information sharing between the law enforcement community and the fire service, the FSIE makes the competition (law enforcement) irrelevant, concentrating on demonstrating the fire service's value to participation in the intelligence process. This is a new and uncontested market space within the intelligence community, a Blue Ocean Strategy (Kim, 2005, p. 12). The FSIE represents a collaborative effort of several U.S. Department of Homeland Security (DHS) entities; the Office of Intelligence and Analysis, State and Local Program Office (I&A/SLPO) and the U.S. Fire Administration, with support from the Federal Emergency Management Agency, National Preparedness Directorate (FEMA/NPD). The FSIE was created to provide organized federal support for incorporating the fire service disciplines in the gathering, analysis, and dissemination of homeland security related information and intelligence at the federal, state, local, tribal, and territorial levels. The major goal of the FSIE is to facilitate fire service integration within state and major Urban Area Fusion Centers, and to facilitate the identification and development of information and intelligence sharing requirements, mechanisms, and training for fire service personnel (FSIE Concept Plan, 2009, p. ii). In essence, the FSIE has become what is described by Bryson as the "dominant coalition" or "coalition of the willing" to champion the strategy of including the fire service in the intelligence process (Bryson, 2004, p. 34). The end result of a successful partnership should be enhanced situational awareness for emergency responders, which translates into improved safety during preparedness and response activities. The strategy

already exists as developed by DHS, the USFA and the creation of the FSIE; the mission should now become how to execute the strategy effectively. This chapter discusses the methodology for executing the strategy by first discussing how and if the FSIE has been successful and then by outlining an execution plan by providing a stakeholder analysis to continue building and sustaining the effort.

A. UNITED STATES FIRE ADMINISTRATION AND THE FSIE INITIATIVE

The intelligence community and the fire service have recognized that improvement is necessary in communications and information sharing (FSIE Concept Plan, 2009). This has been a significant step in broadening the role of the fire service in the homeland security discipline. Our front line firefighters and emergency medical personnel are being recognized as "first preventers" or "first responders who are able to recognize telltale signs of danger to homeland security and report the suspicious activity and preserve the scene until proper authorities arrive" (FDNY, 2007). In his thesis for NPS, Deputy Chief Bryan Heirston of the Oklahoma City Fire Department, explains that the FSIE has continued to evolve and the draft concept plan (FSIE CONPLAN) was released in December 2008. The document, according to Heirston, clarifies "the role of the fire service in preventing terrorism through information sharing with local, state, and federal homeland security partners and is based on four pillars" (Heirston, 2009).

- Identification of the types of intelligence and dissemination mechanisms that the fire service needs to enhance all-threat/all-hazard preparedness and to support fire service response and recovery operations.
- Identification of the way in which the fire service can contribute to local and national homeland security all-threat/all-hazard prevention and protection efforts.
- Collaborative development of an information/intelligence-sharing network within the fire service, and between the fire service and the homeland security/intelligence community, while ensuring the protection of citizen privacy and civil rights/civil liberties.

- Identification of a pool of fire service subject matter experts to serve as advisors for DHS initiatives that involve or affect fire service interests (Heirston, 2009).

The collection of intelligence by the fire service is important to the IC and law enforcement to identify any possible nexus to terrorism. It is equally important for the IC and law enforcement to have the ability to communicate terrorism/criminal related information to the fire service for the protection of their personnel. This two-way process is still evolving, as the FSIE becomes more mature and develops into a larger community of interest.

1. Where Does the Fire Service Fit in the Intelligence Cycle?

The role of the fire service is relevant in every part of the intelligence cycle. Intelligence requirements are defined in the planning phase, and then the corresponding information needs are identified. Collection is relevant for suspicious activity reporting, within the confines of the law, and sharing of internal fire department information, such as information obtained from performing building inspections or what is observed during the course of normal response activities. Analysis occurs when fire service personnel can provide their subject matter expertise to intelligence analysts who can then produce more relevant intelligence products for fire service personnel to consume. Dissemination is relevant because fire service personnel are intelligence customers and consumers and may be able to identify other important consumers to enhance responder and public safety. Evaluation of intelligence products is critical to let analysts know if the fire services' needs are being met.

2. Is the FSIE Working?

The mission statement of the FSIE directly supports an effort to assist first responders in maintaining dynamic situational awareness by establishing that its main goal is to foster the integration of the fire service into state and major urban area fusion centers. The FSIE mission as stated is:

> Institutionalize the integration of the fire service into Federal, State, local, Tribal, and Territorial information and intelligence sharing networks—including State and Major Urban Area Fusion Centers—to enhance preparedness and operations of fire service organizations across the country, while supporting the prevention, protection, response, and recovery efforts of all homeland security partners (FSIE Concept Plan 2009, p. 6).

Seventy-two fusion centers are up and running throughout the United States. Their existence is a testament to the fact that homeland security leaders have recognized the value of centralizing intelligence gathering and analysis to assist in preventing and responding to terrorist threats (CRS Report, 2006). Having trained people integrated into a fusion center provides a greater opportunity for this information exchange to occur in a timely manner. The fire service integration into state and major urban area fusion centers is showing some promise. The latest report (October 2009) released by the DHS I&A, regarding the status of fire service integration within state and major urban area fusion centers, shows that 48 of the 72 established fusion centers (67%) are performing outreach to state and local fire service organizations and/or looking at options for integration in the future (DHS I&A Report, 2009). The degree of the FSIE success is also dependent on the political environment at the federal, state, and local levels. The integration process does not necessarily mean that fire service personnel have to be physically sitting in the fusion centers, but at a minimum, analysts within the fusion centers should have the training to accomplish fire service intelligence analysis. The degree of education that the fire service, law enforcement, and intelligence communities have received on what the objectives of integration are is an important factor.

In conducting interviews for this thesis, several fire service subject matter experts have indicated that the FSIE initiative has lost momentum. The current management of this initiative has shifted almost solely to the United States Fire Administration, which has resulted in what may be termed a “stovepipe initiative.” Prior to this, the DHS Office of Intelligence and Analysis (DHS I&A) had the lead.

More emphasis has been placed on building consensus within the fire service. The claim is that more of the national fire service organizations, the International Association of Firefighters (IAFF), International Association of Fire Chiefs (IAFC), and the National Volunteer Fire Council (NVFC), have become involved, each bringing their own interests to the process. This has created difficulty for the original FSIE participants to build a consensus. The aforementioned organizations, IAFF, IAFC, and NVFC, represent 33,000 fire service agencies collectively with over 1 million firefighters in the United States. It was indicated that the financial aspect of the FSIE, namely the grant process, might be the motivation for these other organizations becoming involved. The view of some of the interview subjects is that if the FSIE is going to move forward in representing the fire service interest in the intelligence business, it must be done in a smaller working group. The recommendations in this thesis actually counter that claim by citing the momentum that the FSIE has established, and thus, demonstrating an impact among the fire service community with regard to improved intelligence support.

3. Has the Intelligence Community Welcomed the Effort?

One of the main reasons for the FSIE initiative occurred because a significant gap existed in the intelligence products needed by the fire service to support the decision making process at the strategic and tactical levels. This gap exists all across the country and at all levels of government. The National Intelligence Strategy of the United States of America (2005) indicates that the IC needs to "establish policies that reflect need-to-share (versus need-to-know) for all data, removing the "ownership" by agency of intelligence information." The Intelligence Reform and Terrorism Prevention Act of 2004 requires the Director of National Intelligence (DNI) to "ensure maximum availability of access to intelligence information" (Intelligence Strategy, p. 14). It also recommends developing networks capable of distributing intelligence in an unclassified form to non-traditional consumers at the state, local, and tribal levels of government. One

of the mechanisms established to allow better sharing of terrorism-related information is the Interagency Threat Assessment and Coordination Group (ITACG) within the National Counterterrorism Center. The intent is to assist in the production of "federally coordinated" terrorism-related information products for dissemination to state, local, and tribal officials (Information Sharing 2007, p. 18). Fire service personnel participate and serve on the ITACG.

In February 2008, the DNI published the United States Intelligence Community Information Sharing Strategy, which includes a quote from President Bush stating the following:

> I have asked [Director McConnell] to improve information sharing within the intelligence community and with officials at all levels of our government, so everyone responsible for the security of our communities has the intelligence they need to do their jobs. (Intelligence Sharing Strategy 2008, p. 3)

Director McConnell boldly claimed that the IC must transform its culture to one where the "responsibility to provide" information is a core mission (Intelligence Sharing Strategy 2008, p. 3). It is implied that firefighters and other state and local government personnel are not only "first responders" but also the first line of defense and an asset to information gathering. In summary, it seems as though the IC has welcomed the new challenge of creating a much more collaborative information-sharing environment.

B. STAKEHOLDER MANAGEMENT

Considering the FSIE mission a value innovation to establish a strategy for better information and intelligence sharing, the fire service could take what Kim and Mauborgne call a "reconstructionist" view, and assist in reconstructing the boundaries and structure of the current information and intelligence sharing "market" (Kim, 2005, p. 17). To be able to accomplish this, careful analysis should be made of the stakeholders in the process. Figure 8 depicts the current

stakeholders in the FSIE initiative. The next section provides a stakeholder analysis and highlights the key stakeholders that support the recommendations of this thesis.

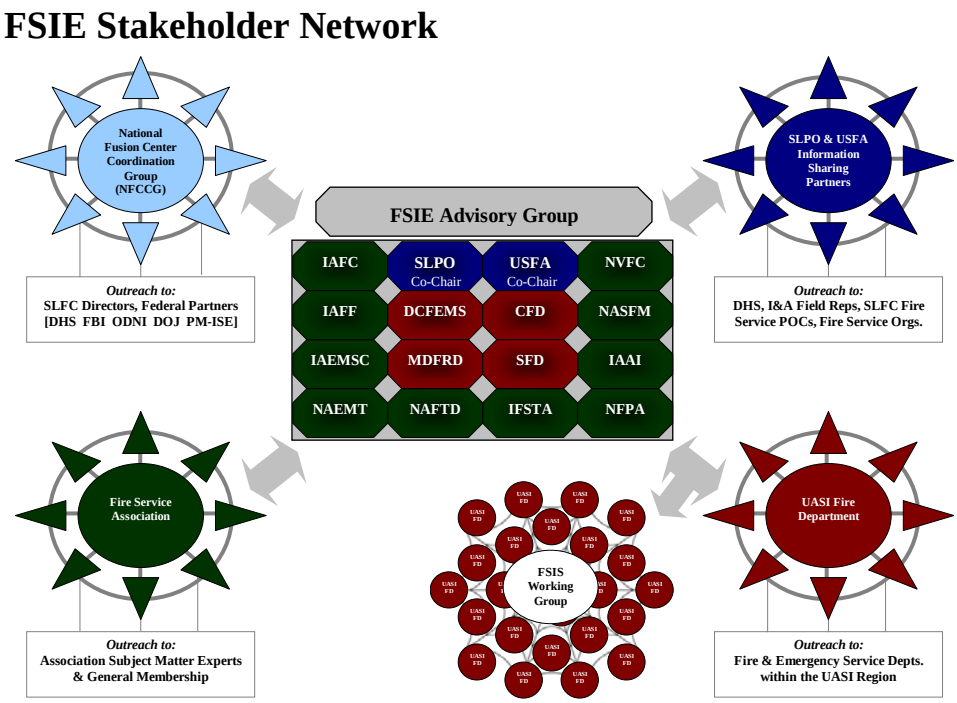

Figure 8. FSIE Stakeholder Network (From: Fire Service Intelligence Enterprise Concept Plan, 2009)

C. PRIORITIZING THE STAKEHOLDERS

The stakeholder analysis process is a three-step process. The main advantage of the process is to obtain a clearer picture of the players and where they actually fit into what can be termed the "stakeholder map." The first step is to identify the stakeholders. The FSIE Concept Plan as depicted in Figure 8 provides that information. The second step is to determine the needs of the stakeholders as they relate to the larger strategy. The interviews and survey for this thesis have assisted in accomplishing this step. Once the needs of the stakeholders have been identified, the next step is to develop a mechanism for

feedback to determine if the selected strategy is working and producing what the stakeholders need. The recommendations in Chapter VI of this thesis present a framework to develop an evaluation process by providing tools to the stakeholders to participate in a meaningful way in the intelligence and information sharing process. In addition to the above three steps, it is equally important to understand exactly how the stakeholders influence the intelligence and information sharing process. If all members of the stakeholder network understand the interrelationships of how they can influence the process, it is likely that the process will succeed (Kim, 2005, pp. 111–112).

1. Power/Interest Grid

According to Kim and Mauborgne, analysis of a stakeholder network using a power versus interest grid can assist an organization in plotting the stakeholders according to their power within and on an organization in relation to their interests to determine how they influence the organization, as well as determining what the organization needs from each stakeholder group. It helps in identifying the importance of each group to the organization or mission to help execute the overall strategy (Kim, 2005). The use of a power versus interest grid in the context of this thesis can help to answer the research question, “how can information and intelligence be better disseminated to local first responders in order to enhance situational awareness, provide a higher degree of responder safety, and better protect the public?” According to Bryson, the power versus interest grid results in the establishment of four categories of stakeholders. Stakeholders with high power and high interest are categorized as players. Stakeholders with high power and low interest are categorized as context setters. Those with high interest and low power are categorized as subjects; they are subject to the power of other stakeholders. The remaining category are those categorized as having low power and low interest; they are called the crowd

(Bryson, 2004, p. 112). Figure 9 shows a model power versus interest grid. It is a subjective depiction by the author as determined from the research completed for this thesis.

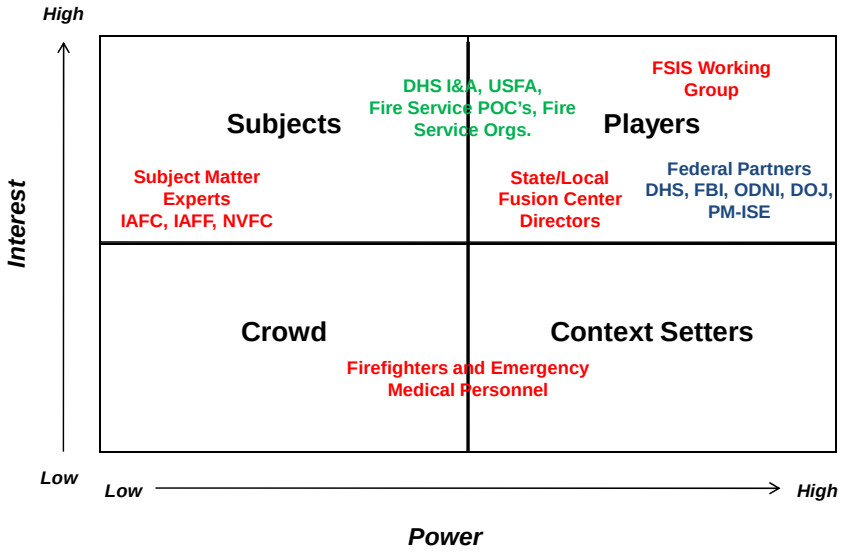

Figure 9. Model Power Versus Interest Grid

The grid as illustrated by the author identifies the groups whose interest and power bases should be considered to execute the overall strategy of intelligence and information sharing between the fire service and the law enforcement/intelligence community. Two key points can be extrapolated from the grid, First, the subject matter experts in the ***subject*** quadrant (high interest/low power) need to be shifted to the ***players*** quadrant (high interest/high power). Their continued participation in the FSIE Stakeholder Network can facilitate the shift, but to accomplish this, more emphasis must be placed on prioritizing the needs of entire fire service. The fire service associations participating have the ability to reach out to literally tens of thousands of fire service personnel to determine what their issues are concerning intelligence and information sharing. These associations cannot operate in a vacuum; they need to develop partnerships between themselves, which should result in a greater

power base causing a shift from subjects to key players. The second key point relates to the "boots on the ground" fire and EMS personnel, who are depicted on the grid as part of the ***crowd*** and ***context setters***. The average firefighter and EMS person probably have little interest in the importance of intelligence and information sharing mainly due to a lack of training in this new discipline for the fire service. Providing the necessary training to enhance their awareness of how important this initiative can be to improve safety and situational awareness, can allow a shift to occur whereby firefighters and EMS personnel move on the power grid from the ***crowd*** and ***context setters*** to a more valuable role as ***subjects*** and ***players***. If the entire fire service can be engaged in understanding the critical role that intelligence can play in the course of their duties, particularly during and after a significant event, the more likely that the strategy initiated by the formation of the FSIE will be executed. Some of the research for this thesis indicated that fire service personnel could be trained initially in basic training school, as well as including more advanced levels of intelligence training in promotional curricula, as people progress in their careers.

D. BUILDING AND SUSTAINING THE NETWORK

To build execution into the strategy of developing a meaningful intelligence and information sharing environment, buy-in must occur from those participating in the process. According to Kim and Mauborgne, it is only when all members of an organization are aligned around a strategy and supports it, that execution of the strategy can be accomplished. They claim that a culture of trust and commitment must be created and that "people's minds and hearts must align with the new strategy so that at the level of the individual, people embrace it of their own accord and willingly go beyond compulsory execution to voluntary cooperation in carrying it out" (Kim, 2005, p. 171). Using the concept of fair process can enable the success of building, sustaining, and executing the strategy.

1. The Power of Fair Process

Kim and Mauborgne discovered the concept of fair process by researching social science literature. They developed what they term a managerial expression of fair process from the concept of procedural justice as described by two social scientists, John W. Thibaut and Laurens Walker in the 1970s. Thibaut and Walker claimed that people care as much about the justice of the process through which an outcome is produced as they do about the outcome itself (Kim, 2005, p. 175). Kim and Mauborgne assert that fair process builds execution into strategy by getting buy-in from people up-front in the process. Fair process results in building a sense of trust, which leads to voluntary cooperation (Kim, 2005).

Fair process consists of three elements: engagement, explanation, and expectation clarity. Engagement is the process of involving people in the decisions that affect them and allowing them to have input as the strategy is developed. Trust and commitment are outcomes of including the stakeholders early and often in the process. Explanation involves ensuring that the stakeholders are made aware of why and how decisions are made, which also builds trust between the decision makers and the stakeholders. It illustrates that all input has not only been solicited, but also utilized in the decision-making process. This also allows for feedback and evaluation, which enhances the strategic learning process and results in a better product. Expectation clarity means that once the strategy is in place, then all stakeholders understand how the strategy is implemented and what standards are used to gauge success or failure (Kim, 2005).

An important complementary note to why fair process matters in the strategic development process concerns intellectual and emotional recognition theory as discussed by Kim and Mauborgne. If people are recognized during the process for their intellectual worth, they are more willing to share their knowledge and ideas. If they are recognized emotionally, the claim is that they feel

emotionally tied to the strategy and aspire to contribute everything they can to make it successful. Knowledge and ideas not valued result in people not sharing their best critical thinking and creative ideas, which leads to reduced investment and counterproductive behavior.

The author can share a personal example of the power of fair process. In 1998, the FDNY made a strategic decision to enhance its response capabilities to terrorist incidents. Five new response units, called “squad” companies were formed and strategically located around the city to decentralize the response to hazardous materials and chemical, biological, radiological, nuclear, and explosive (CBRNE) incidents. The initiative required the selection of new company commanders and unit personnel to staff these units. All new personnel would be receiving several hundred hours of training to be able to execute the new mission. It required the selection of highly motivated individuals committed to success. Personal experience, as one of the new company commanders taught the author, that once the personnel were selected, a different style of leadership was required to be successful. Early in the process, all new personnel in the unit were included and engaged in the decision-making process of how the unit would be managed. This was a significant change from the hierarchical structure typical in the fire service. The unit personnel developed all internal unit policies with final review by the unit leaders. In particular, the senior veterans in the unit were given the authority and responsibility to make policy. This process resulted in a level of trust and commitment that, until then in the author’s career, had not been experienced. Members of the unit made a significant investment simply because they were made part of the process. The assignment was one of the most rewarding in the author’s career.

Figure 10 shows the execution consequences of the presence and absence of fair process in strategy making (Kim, 2005).

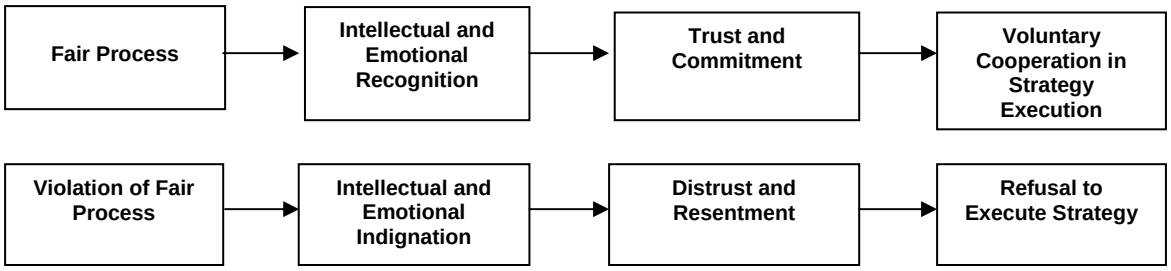

Figure 10. Execution Consequences of the Presence and Absence of Fair Process (From: Kim, 2005, p. 183)

The inclusion of fair process in the stakeholder analysis helps to build the "coalition of the willing" and by developing commitment, trust and voluntary cooperation as important capital in moving forward with the fire services' involvement in intelligence and information sharing. As demonstrated by the author's personal example, the level of commitment by fire service personnel can be enhanced by those in leadership roles; developing a high level of trust with subordinates. This is true for the formal leaders, as well as the informal leaders in the rank and file. Thirty years of experience, twenty as a supervisor, enables the author to observe that it is noticeable when entering a fire station, if a sense of ownership, pride, and commitment exists within a unit. The appearance of the unit apparatus, station quarters and the personnel tells a story. This can be seen from the new recruit up to and including the senior member of the unit. No matter what the mission may be, a unit with those qualities can build and sustain any given strategy. If that can transcend an entire organization, the mission will succeed.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. RECOMMENDATIONS AND CONCLUSIONS

The research for this thesis has shown that an ongoing effort exists within the fire service to progress toward full integration in the fusion center process. This continues to be a work in progress. While this is a significant step in providing the fire service access to homeland security intelligence and information, a standardized model for disseminating the intelligence and information to the "boots on the ground" first responders is still needed. A standardized method of dissemination can be included in intelligence training curriculums at all levels. Firefighters are trained to follow standard operating procedures beginning in recruit level training, which enables them to make decisions more efficiently to accomplish whatever they are tasked with at a fire or emergency. As an example, firefighters assigned to perform a search at a residential structure fire are taught basic search techniques that allow them to move through a structure with speed and efficiency, covering the most area in the shortest amount of time possible, minimizing the risk of being in the structure for too long and running out of air in their breathing apparatus. If firefighters are trained at an early stage and refreshed throughout their careers to receive intelligence that can affect theirs and the public's safety in a standardized format, their decision-making capacity is improved, and therefore, the level of risk may be reduced. The Times Square car bomb incident in New York City in May 2010 provides a good example. If a quick and efficient method of dissemination was predetermined to notify fire units throughout the city of the incident, once it was confirmed, situational awareness would be enhanced for all responders, allowing them to use caution and make better decisions, when responding to similar type incidents.

This chapter presents a model for disseminating intelligence and information to the fire service. It is multi-phased and allows for modification by individual fire service organizations based on their financial and personnel

resources. The model is based on the definition of intelligence as all-threat/all-hazard information that has been gathered and vetted through the intelligence cycle to generate products that can be used to guide fire service decisions at the strategic, operational, and tactical levels.

A. A NEW MODEL FOR THE FIRE SERVICE

The recommendations are based on the October 2009 report of Fire Service Integration within State and Major Urban Area Fusion Centers by the DHS Office of I&A, as a basis for developing the new model. The report provides a nationwide picture of fire service involvement in the intelligence- and information-sharing evolution through fusion center participation. Three metrics in particular influenced the recommendations.

- Fire service coordination at the state level, a point of contact (POC) for coordination between the fusion center and the fire service. Out of seventy-two fusion centers, thirty-two reported having this capability (44%).
- Fire Service Fusion, Terrorism, Intelligence Liaison Officers (FLO, TLO, ILO) in states or major urban areas with fusion centers. Eighteen states out of seventy-two fusion centers reported having FLO, TLO, or ILO (23%).
- Point of contact on the FSIE distribution list. Thirty-eight states reported that they had a POC for the FSIE (53%) (DHS I&A Report, 2009)

1. Fire Service Coordination at the State Level

Each of the fifty states has a fire chief's association whose membership consists of the fire chiefs from all areas of the state. Most of the associations also have regional and county representatives throughout the state for disseminating general fire service information to the fire chiefs in that state, which is a good existent network for sharing information. The International Association of Fire Chiefs network is divided into eight regional divisions that represent the states in the associated divisions. The regional associations are typically the

communications link from the IAFC to the state fire chief's associations. The IAFC has a Terrorism and Homeland Security Committee with representatives from around the country. The IAFC has been identified as a stakeholder with a supporting function by the FSIE. Efforts have begun recently at the executive level to develop the relationship further to obtain more involvement from the fire service in the information sharing initiative (J. Donnelly, personal communication, July 28, 2010). The IAFC could be the main point of contact for the FSIE to connect with the states, and in turn, the counties within the states. Each fire chief's association should have a formal point of contact with the FSIE and those states with either state or major urban area fusion centers should have the same. This is a matter of educating the IAFC leadership and committee leaders on the value of the fire service information sharing initiative. The IAFC already has an established relationship with the USFA so developing this new initiative should not pose a particular problem. The establishment of a secure portal on the IAFC website for disseminating unclassified information and/or intelligence would be a pragmatic method and would support what interview subjects identified as a key way to disseminate intelligence and information. Interview subjects and survey respondents identified electronic means of communication as a quick and easy method for information sharing. In addition, weekly bulletins were identified as the most frequently used mechanism for providing information affecting fire department activities. Posting a weekly bulletin in a standardized format, similar to the FDNY Watchline, in a secure folder on the IAFC website, can be a logical solution and provide a type of "one stop shopping" for relevant intelligence and information.

The IAFC could be the ideal organization to sponsor the Fusion Center and Fire Service Information Sharing and Coordination Workshop program offered through the DOJ Fusion Process Technical Assistance Program. The purpose of this program is to facilitate discussion between fire service personnel and their respective fusion centers. It also assists fire service personnel in learning how they can engage in the information sharing processes. Participation

in this program can begin to assist fire service organizations in improving their operational information sharing abilities. The state, regional and/or county fire chief's associations can sponsor these workshops to solicit more participation in this important endeavor. Perhaps an alternative to providing fire service intelligence training can be for the National Fire Academy (NFA) to offer the educational platform and develop a fire service intelligence curriculum. The NFA supplies a recognized physical location to conduct the training as well. Having both the IAFC and the NFA as training advocates working together can be a valuable partnership in this type of initiative. The challenge is to obtain the funding to support the program.

2. FLO, TLO, ILO Training Programs

A Terrorism Liaison Officer (TLO) is an individual trained in handling and processing intelligence documents and information. When asked if their organizations have TLO's, all of the interview subjects that answered yes described them as significant in being able to receive intelligence and information that could improve firefighter and public safety. The research indicated that the key to developing a successful program was to customize it to fit the jurisdiction it served. Having trained TLO's in a fire department could allow for the following.

- Any relevant terrorism-related intelligence to be disseminated quickly and efficiently.
- Pertinent intelligence/information from DHS or other federal and state resources could be analyzed and provided to members of the organization.
- Threat and vulnerability assessments to be performed.
- Review of current terrorism-related events in the United States and abroad that could have implications in the local jurisdiction.
- Developing of local area training needs based on risk assessments.

A program successfully adopted in Arizona can serve as a model for developing this area of expertise and training for use throughout the fire service. Arizona's program is a statewide program that incorporates law enforcement,

military, federal, and fire service agencies. Fire service personnel can formally receive terrorism-awareness and prevention training through this mechanism. DHS, through the formation of the FSIE, has already established that firefighters and emergency medical workers have access to many buildings and locations during the course of their routine duties and are able to notice suspicious activity by passively observing their surroundings. The Arizona TLO program provides a more advanced level of training than just basic awareness and trains each TLO to perform in three mission areas during a forty (40) hour training program.

- Criminal intelligence collection and dissemination
- Building intelligence collection (threat and vulnerability assessments)
- On-scene response to significant events

a. Criminal Intelligence Collection

The training received in criminal intelligence enables the individual to receive, process, and distribute information to appropriate personnel. The training program participants all receive an FBI secret clearance after an extensive background check to facilitate the performance of their assigned duties. In Arizona, a certified TLO, in collaboration with the Arizona Counterterrorism Information Center, can reclassify documents for dissemination as “public safety sensitive” rather than “law enforcement sensitive,” and thereby, increase the number of first responders who can be informed (Salyers, 2007). This ability within the fire service can increase the amount of information shared to line first responder units when necessary. By decentralizing the consumption of information to meet a particular area’s risk profile, first responders may be more inclined to react to and implement the recommendations.

In his thesis, Heirston compares England’s sensitive information-sharing system with that of the United States. He explains that the fire service and intelligence community use a network of what they call fire liaisons (battalion chief level in the United States) along with executive-level officers (fire chief and

deputy chief level in the United States) who have higher security clearances to share sensitive information. The sensitive information can only be seen by the members with the advanced clearances who decide on how and what to disseminate (Heirston, 2009). A TLO, FLO, or ILO can have this capability if necessary.

b. Building Intelligence

A designated TLO can identify target hazards, critical infrastructure and key assets within their response area for the need to perform threat and vulnerability assessments. As an example, the FDNY has a Critical Information Dispatch System (CIDS), a computer database that recognizes the unique hazards present in certain occupancies.[3] Local fire companies generate and input the data. This system is successful for two reasons. First, local units usually have intimate knowledge of the types of buildings to be assessed and already have relationships with building owners, managers, and personnel. Salyers and Lutrick indicate that those relationships are important due to the concern by building owners that intimate information about their facility be collected and used. Second, a TLO can have advanced training in performing threat and vulnerability assessments. As force multipliers assisting in assessment completion, TLO's can increase the number of structures and locations to be entered into a database and be available at a dispatch or operations center for dissemination to the first responders when an incident occurs. A local TLO can be the point of contact (POC), and thus, eliminate any confusion in the process.

[3] Critical Information Dispatch System (CIDS) is a computer database that contains specific information on a building or occupancy for the attention of responding units. Tactical information that can be helpful to firefighters is included. Most, if not all identified critical infrastructure is already in the system.

c. On-Scene Response

Having response TLO's with specialized training and access to specific terrorism-related or all-hazards information puts the information closer to what Salyers and Lutrick describe as "boots on the ground" personnel. They describe this as closing the loop from collection to dissemination. The FDNY already has in place several specially trained chiefs in the field in a variety of training disciplines. They have battalion chiefs trained as safety chiefs, hazardous materials technicians, foam coordinators, transit liaisons, and air reconnaissance chiefs. Depending on the type of incident, a specially trained chief is assigned to respond to assist the incident commander in the particular specialty. Having fire chiefs trained as TLO's can enhance capability in a terrorism-related event in providing real time information at the command post. The TLO can provide human intelligence and interpret the information on scene for the incident commander.

3. Designated Points of Contact for the FSIE

Ideally, it is beneficial for all U.S. fire service organizations to have a POC for the FSIE. As a working group, the FSIE has made progress in developing their stakeholder network as evidenced in Figure 8. The interview subjects described the FSIE as the catalyst for the fire service involvement in intelligence and information sharing. One interview subject noted that a key objective of the FSIE should be to facilitate the sharing of best practices for intelligence and information sharing between fire service organizations. State fire chiefs associations, in collaboration with the FSIE, should advertise the benefits of participating as working partners in the initiative to expand the network and to continue developing a culture of information sharing. "Fire service organizations and personnel should make information sharing an institutionalized part of their normal operations" (USFA Fire Service Information Sharing—Message Guide, 2010). The fire service has been acknowledged as a provider of information to

fusion centers, as collaborators by virtue of their training and experience, making them important subject matter experts who can greatly contribute to the development of intelligence products, and finally, as consumers of information and intelligence to assist in preparedness, as well as enhancing responder safety during response and recovery operations. Simply having a POC to receive relevant information significantly enhances the dissemination of information. The fire service represents a community of interest that can both contribute and benefit from a wide-reaching information-sharing environment.

B. TECHNOLOGY AND DISSEMINATING INTELLIGENCE

The advancements in technology in sending and receiving information are constantly evolving. Disseminating intelligence to enhance dynamic situational awareness and responder safety should be accomplished in a timely and secure fashion. Interview subjects maintained that intelligence products can be used in three ways: to discuss trends, make deployment decisions, and analyze threat assessments, which are all elements of determining dynamic situational awareness to assist first responders in adapting to a changing response environment. Receiving the information quickly and securely makes it actionable in real time. Currently, some very useful internet-based methods exist for first responders to acquire timely and relevant intelligence to assist them in the performance of their duties. First responders have the ability to subscribe to these sites to receive real time homeland security related information and intelligence.

The Homeland Security Information Network (HSIN) is a national secure and trusted web-based portal for information sharing and collaboration between federal, state, local, tribal, territorial, private sector, and international partners engaged in the homeland security mission.

The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) is a web-based initiative established to support the critical infrastructure protection of emergency services sector departments and agencies nationwide.

Fire service agencies should strive to develop a network command capability, which is a new information-sharing framework using voice, video, and data to connect first responders for situational awareness and improved incident management (Pfeiffer, 2009).

Finally, fire service agencies need to have an internal mechanism to advise field units of situations t occurring in real time while they are on duty. The method chosen must be able to communicate with responders in the fire stations, as well as in the fire apparatus either while on the road at or while returning from an incident.

1. Homeland Security Information Network (HSIN)

HSIN is comprised of a growing network of communities, called Communities of Interest (COI), which are organized by state organizations, federal organizations, or mission areas, such as emergency management, law enforcement, critical sectors, and intelligence. Users can securely share within their communities or reach out to other communities as needed. HSIN provides secure, real-time collaboration tools, including a virtual meeting space, instant messaging and document sharing. HSIN allows partners to work together instantly, regardless of their location, to communicate, collaborate, and coordinate (DHS website).

In addition to the above capabilities, HSIN provides geospatial tool for use in establishing enhanced situational and strategic awareness. The Integrated Common Analytical Viewer (iCAV) is a secure, web-based, geospatial visualization suite of tools that integrates commercial and government-owned data and imagery from multiple sources. When the data layers and information

feeds are overlaid with imagery, iCAV users are able to view the impact of threats, natural and man-made disasters, population centers that can be impacted, and the resources available to respond to and recover from an event. The iCAV program was initiated as mandated by HSPD-7 to map, image, analyze, and sort geospatially the nation's critical infrastructure and key resources and is a critical component capability in assisting DHS and its mission partners to prepare for, prevent, respond to and recover from natural and man-made disasters better.[4]

HSIN has not been without criticism. A 2007 Government Accountability Office (GAO) report suggests that HSIN may not be facilitating effective information sharing, and in fact, may be duplicating efforts of state and local authorities. The assertion is that HSIN is not providing anything new. The report claims it uses similar user groups, such as emergency management agencies, and provides similar methods for information sharing, such as electronic bulletin boards, “chat” tools, and document libraries. The suggested remedies by the GAO are for HSIN to take steps to improve coordination with state and local initiatives to reduce redundancy and to use the key initiatives from the state and local programs to recommend best practices for more effective coordination and collaboration for information sharing at the federal level (GAO, 2007). As a result of some of the criticisms, DHS is taking steps to enhance HSIN by developing what they are calling HSIN Next Generation (NextGen).[5] The current HSIN is a

[4] Membership in HSIN is COI-based. It is available to fire service members on a subscription basis. To become a member, a subscriber must first decide which COI(s) meets their needs. Once the COI has been identified, a subscriber needs to be nominated and vetted into the COI. Once nominated, the COI Validating Authority reviews the membership application and approves or denies admission to the COI. If the application is approved, the subscriber receives an e-mail with instructions on how to log onto HSIN for the first time. Fifty three percent (53%) of survey respondents for this thesis indicated that they wanted to receive intelligence via electronic means, such as e-mail.

[5] The next generation network will provide DHS, its partners and stakeholders information management capabilities and services including a portal, search, collaboration, enterprise content management, and service oriented architecture-based information integration and analysis functions to facilitate collaboration and information sharing needs for sensitive but unclassified (SBU) data (Digital Communities 2008, accessed August 1, 2010).

computer-based counterterrorism communications system connecting all 50 states, five territories, Washington, D.C., and 50 major urban areas. It allows all states and major urban areas to collect and disseminate information in real time between federal, state, and local agencies involved in combating terrorism. It also provides capabilities to help analyze that information. The network also gives states and major urban areas real-time interactive connectivity with the National Operations Center (NOC). The NOC is the main hub at the federal level for providing situational awareness and coordination. It operates twenty-four hours a day, seven days a week monitoring threat and hazard information from sources all across the country and provides spot reports, and situation reports to provide a common operating picture for incident commanders and response personnel. Maintaining the NOC capabilities are a high priority as described in the National Response Framework (NRF) (NRF, 2008). Participation by first responder agencies in HSIN is a valuable tool for disseminating real time actionable intelligence and information.

2. Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC)

The goals of the EMR-ISAC are the following.

- Promote awareness of the threats to and vulnerabilities of emergency services sector (ESS) critical infrastructures.
- Encourage ESS prevention, protection, and resilience actions for all disasters.
- Enhance the survivability, continuity, and “response-ability” in all-hazards environments (EMR-ISAC Brochure).

To accomplish its goals, the EMR-ISAC publishes products available to subscribers, which provide information relevant to the ESS. CIP (FOUO) notices are published periodically and disseminated that contain actionable information regarding threats and vulnerabilities potentially affecting emergency plans and operations. CIP Infograms are published weekly, which contain information about protecting critical infrastructures of emergency responders and their

communities. CIP Bulletins, also published as needed, contain homeland security information involving infrastructure protection of the emergency services (EMR-ISAC Brochure) (See appendices for examples).These products are delivered via e-mail to subscribers and access to them by first responders can obviously contribute to better planning and operational decision making. At a minimum, mid-level chief officers and line officers should subscribe. Subscribing requires sending an e-mail request to emr-isac@dhs.gov and providing the requested information.

3. Network Command

The FDNY has been developing a system of network command, which includes the use of voice, video and data to enhance situational awareness and provides the incident commander with a better decision-making framework. A "web-like structure of networks connects to different informational sources to enhance command capacity" (Pfeifer, 2009). The network is formed by using technology to create enhanced on-scene capabilities for information sharing by being able to connect multiple organizations at the scene to enable better collaboration and information exchange. This network command is managed through the development and deployment of electronic command boards. Electronic command boards are essentially touch-screen computers with software designed and installed to allow for managing resources on the scene of a fire or emergency and also have the capacity through a secure wireless network to receive information from multiple sources in real time during a fire or emergency.

A key finding of the research relative to TLO's was illustrated in the Arizona model described earlier. A TLO responding with a laptop computer could complement the information being received on the electronic command board, becoming a critical component within the network command, particularly as it relates to the ability to receive sensitive and/or classified information.

The hub of the network command structure is the Fire Department Operations Center (FDOC), which is the FDNY's high tech Emergency Operations Center possessing the ability to receive and transmit information in all three domains: voice, video and data. The FDOC can monitors communications, reviews video images, and searches multiple databases to feed the incident commander important information for decision-making purposes. The FDOC is essentially a data mining apparatus that can produce timely, relevant and actionable products for the incident commander. The director of the FDNY FDOC stated, "information needs to be departed meaningfully and very briefly" to be useful. In most cases, there is a five to fifteen minute window to provide critical information downrange to the incident commander to make better decisions. He also commented that if information or intelligence can be graphically oriented, it can be much more impactful, being able to "jump out" to the decision makers, which is one of the key benefits of the electronic command boards (T. Herlocker, personal communication, April 28, 2010). In addition to the internal benefit of the FDOC to the FDNY, it provides information to external partners. As an example, in October 2006, New York Yankees pitcher Cory Lidle accidentally crashed his private plane into a Manhattan high-rise residential building. During the initial stages of the incident first responders needed to know if this crash might have had a nexus to terrorism to make appropriate strategic and tactical decisions. Homeland security officials in Washington, D.C. were interested in receiving information from the scene to develop situational awareness at the federal level. The FDOC was able to connect multiple agencies in the local metropolitan area for briefings and also posted situation and progress reports on HSIN so that responders all across the nation who access HSIN could be informed about the situation in New York. This mechanism was also used for the "Miracle on the Hudson" in January 2009, when U.S. Airways Flight 1549 made an emergency landing in the Hudson River (Pfeifer, 2009).

The above incidents provide evidence that contrasts what occurred on 9/11 at the World Trade Center where police department helicopters, from their

vantage point, were able to assess that the towers were in imminent danger of collapse. At that time, no formal procedure existed for that information to be shared with fire department incident commanders. If that information could have been shared quickly and efficiently, it is possible that more first responder's lives could have been saved. "Possessing information has been a traditional sign of power, which has led to information silos. In a network world, however, power is attained not by hoarding information, but by distributing accurate information to many organizations as quickly as possible. This paradigm shift is vital during fires and disasters, where emergency responders depend on a network command to connect to information systems and other organizations to assist in incident management" (Pfeifer, 2009, p.18).

This complex and expensive model of network command may not be attainable by most fire service organizations due to fiscal constraints. It is presented to illustrate what is possible when intellectual talent and technological advances are joined in the interest of public and emergency responder safety. Perhaps on a regional or county level with funding through grant programs, similar models can be developed and implemented. (See Appendix C for an example of the information sharing capabilities of electronic command boards).

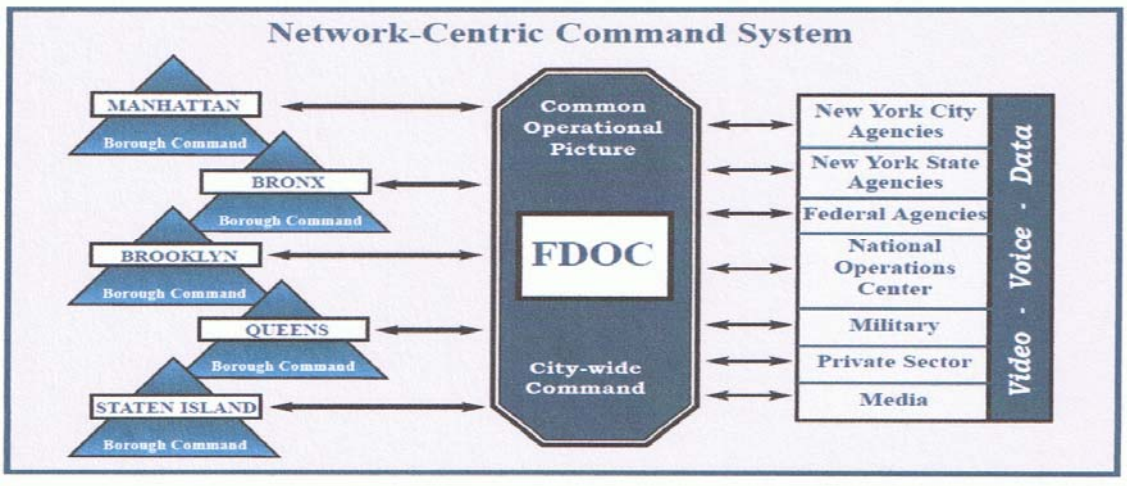

Figure 11. Network-Centric Command System (From: Pfeifer, 2009)

4. Internal Dissemination Mechanisms

When information or intelligence suggests a credible threat exists to a jurisdiction or region, a method is needed to disseminate that to responders in the field quickly. Similarly, when an incident is happening in real time or has already happened, responders should be made aware to have a heightened state of alert when responding to other incidents.

The FDNY has recently drafted a policy to accomplish this. The Phoenix, Arizona Fire Department uses a similar method. The methodology is termed an “Emergency Action Message” (EAM). The intent is to disseminate information to responders in the field prior to or post event of serious concern or of a nature of which all field units should be aware. The The on-duty citywide tour commander will order and draft the EAM, and it will be disseminated to all field units and other designated employees as necessary. The message will provide unclassified information to field units as a means to enhance their situational awareness during their daily activities and responses. It will be delivered via e-mail format over the fire department Intranet. This method allows for tracking and also allows for the local battalion and division chiefs to monitor and see if the message has been opened and read by each unit. Disseminating the message via e-mail over the Intranet provides a secure portal for the message relayed as FOUO. Units will be notified that an EAM is pending in their e-mail accounts via a message on the apparatus mobile data terminal (MDT) if out of quarters, or via the alarm teleprinter in quarters, voice intercom system, or fax machine. When receiving the message, the officer on duty will be directed to check the unit’s e-mail account to view the EAM. The message will not be announced on any radio frequency for security purposes. If the message is not read in a reasonable amount of time, the local battalion chief will follow up and ensure compliance. The EAM will be generic in nature to preclude a review of the material for sensitive content. As an example, the Times Square car bombing attempt in May 2010 would result in a message to units about the incident and to be alert for

responses in high profile areas and to review standard operating procedures for responses to hazardous materials incidents or incidents involving improvised explosive devices (IED) (FDNY EAM Draft Policy, 2010).

This methodology is very simple and quick to accomplish once accurate information is received and verified. E-mail was the preferred method identified by survey respondents for receiving intelligence and information quickly in the field. Most fire service organizations have this capability. Even in a volunteer fire department, the assumption can be made that e-mail is a contemporary way of communicating with responders (See Appendix D for a summary of recommendations).

C. FUTURE RESEARCH

This thesis has addressed the need for methodologies to disseminate intelligence and information to first responders to improve decision making and to enhance responder and public safety. Recommendations have been made on how this can be accomplished. Additional research areas exist. The development of training programs for fire service personnel in the field of intelligence warrants further research and development. Intelligence training for firefighters can enhance the response mission by providing them with the tools to receive intelligence products, which can enhance their understanding of the operational environment, and which should result in better decision-making, leading to increased safety and survival. The use of social networking to communicate during emergencies is also a technological medium for further exploration. The public has been engaged to provide real time information to emergency response organizations. How can social networking be utilized effectively by first responders during major disasters? How can funding be made more available to emergency service organizations for technology upgrades to more easily receive and disseminate information? Future research projects are limited to the imagination of the researcher interested in information sharing and collaboration.

D. CONCLUSION

The sharing of terrorism-related information has become a priority to the fire service. Stakeholders have recognized that one of the most effective ways to improve homeland security efforts is to create an environment in which external and internal information sharing are occurring at regular intervals. Recognition now exists that firefighters and emergency medical personnel are valuable assets in being able to collect information during the course of their daily duties. Representation at the federal level is occurring because of the FSIE initiative to ensure the receipt of intelligence and information to increase situational awareness to be better prepared to prevent and respond to terrorist incidents.

The issues raised in this thesis related to information sharing and dissemination focus not on the ability to collect information but on the ability to properly and expeditiously disseminate it to the consumers of the information in the field. Fire chiefs, fire officers, firefighters, and emergency medical personnel all have the need to receive this type of information to remain vigilant and safe in the performance of their duties. Weaknesses exist in the methods by which relevant information is shared with first responders in the field. Historically, the fire service has relied on the chain of command for receiving and sharing information with field responders, which can create a barrier in the ability to have creative and viable problem solving ideas become good policy. To remove the barriers to solving problems, the fire service must be open to allowing a non-traditional model of bottom up thinking and problem solving to occur.

First responders need to be empowered and trusted with the ability to use new resources to increase the level of safety and situational awareness in the field. The recommendations proposed are practical solutions to assist in solving the identified challenges. One of the challenges for first responders on every response is that of the unknown. They rarely know exactly to what they are responding. They typically have information as to location and to what they are supposedly responding. If first responders can reduce the risks posed to them by

the unknown factors, their safety and the safety of the public can be improved. Receiving intelligence and information in a timely, simple and meaningful way before, during, and after an incident, increases the chances of making more informed decisions to bring an event to a successful conclusion.

APPENDIX A. STRUCTURED INTERVIEW QUESTIONS

1. What is the role of intelligence within your organization?

2. What effect has the FSIE had on intelligence and information sharing for the fire service?

3. Does your agency have trained Terrorism Liaison Officers (TLO)? If so, how and where do they receive their training? What are their duties and how do they interact with field responders?

4. How does your agency disseminate intelligence?

5. Are you aware of any models, other than your own agency, for intelligence sharing and dissemination currently being used in the fire service that have been successful?

6. Does your agency have a representative in the local/regional fusion center? If not from your agency, is there a fire service representative? Is that person well received and a respected partner?

7. Does your local fusion center produce intelligence that is valuable for the fire service?

8. What type of intelligence should be shared with first responders?

9. What would your recommendation be for an effective model for disseminating intelligence to field responders in a fire department?

10. What is your opinion on the issue of security clearances for members of the fire service with intelligence responsibilities? Are security clearances necessary?

11. What is the range of classifications or sensitive markings for the intelligence products you receive?

12. Are you aware of any specific programs to train fire service personnel in the intelligence process?

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. SURVEY QUESTIONS

1. What type of terrorism-related intelligence do you think firefighters and EMS personnel need in order to more safely perform their jobs?

2. Do you feel that it would be valuable to receive intelligence briefings regularly and from who?

3. How would you prefer to receive intelligence briefings, estimates and assessments?

4. What would work best in your agency to disseminate intelligence to members in the field?

5. Would regular intelligence briefings affect your daily operations?

6. Does your agency provide terrorism awareness training to its personnel? If so how many hours?

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. ELECTRONIC COMMAND BOARD (ECB)

The ECB enables the Incident Commander (IC) to have better situational awareness by showing graphic displays of the fire/emergency location within a building, floor plans, and mapping capabilities showing the surrounding structures and topography. Electronic command boards are essentially touch-screen computers with software designed and installed to allow for managing resources on the scene of a fire or emergency and also have the capacity through a secure wireless network to receive information from multiple sources in real time during a fire or emergency. The following screen shots are some examples of what the IC can display. In addition, the FDNY Fire Department Operations Center has the capability to send the IC graphically-oriented intelligence/information to enhance decision making.

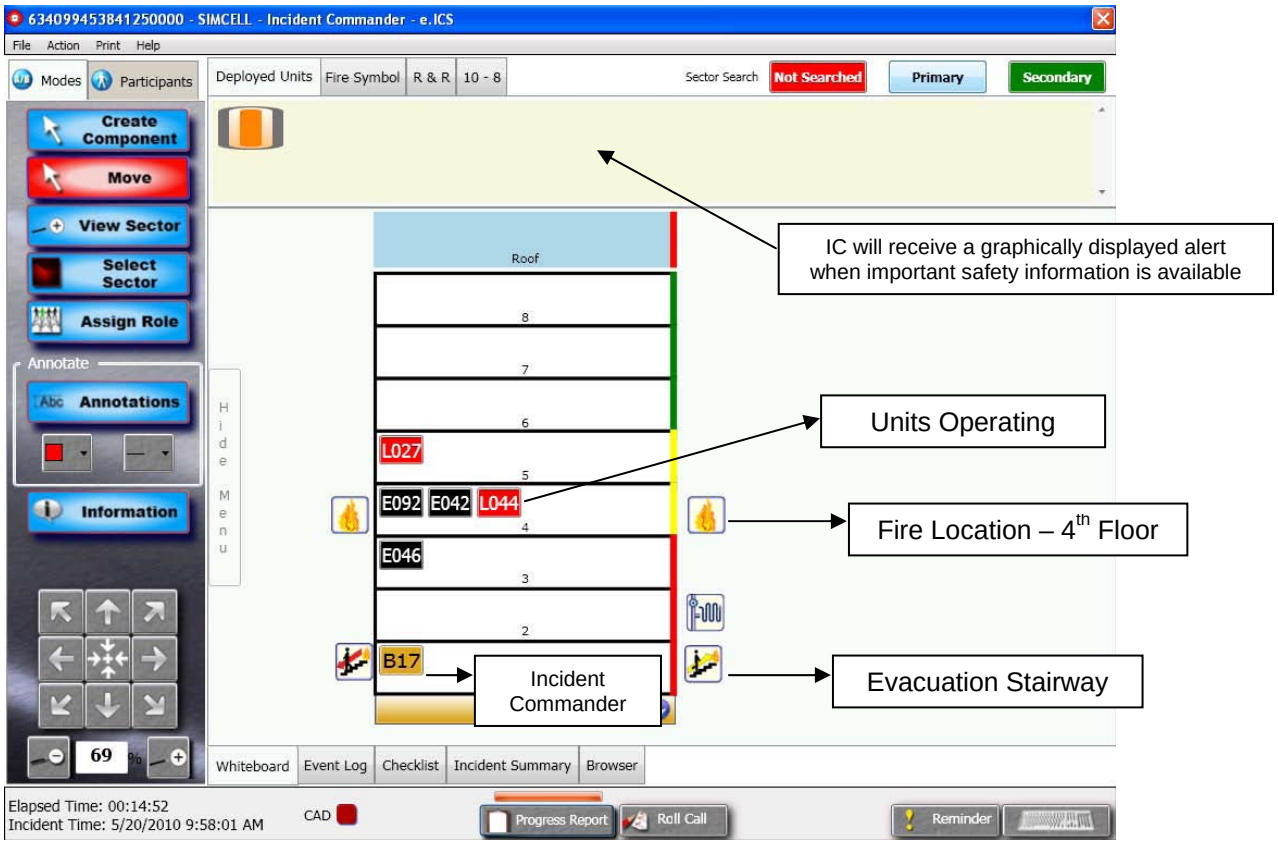

Figure 12. Managing an Incident and Resources (From: Prototype of FDNY ECB)

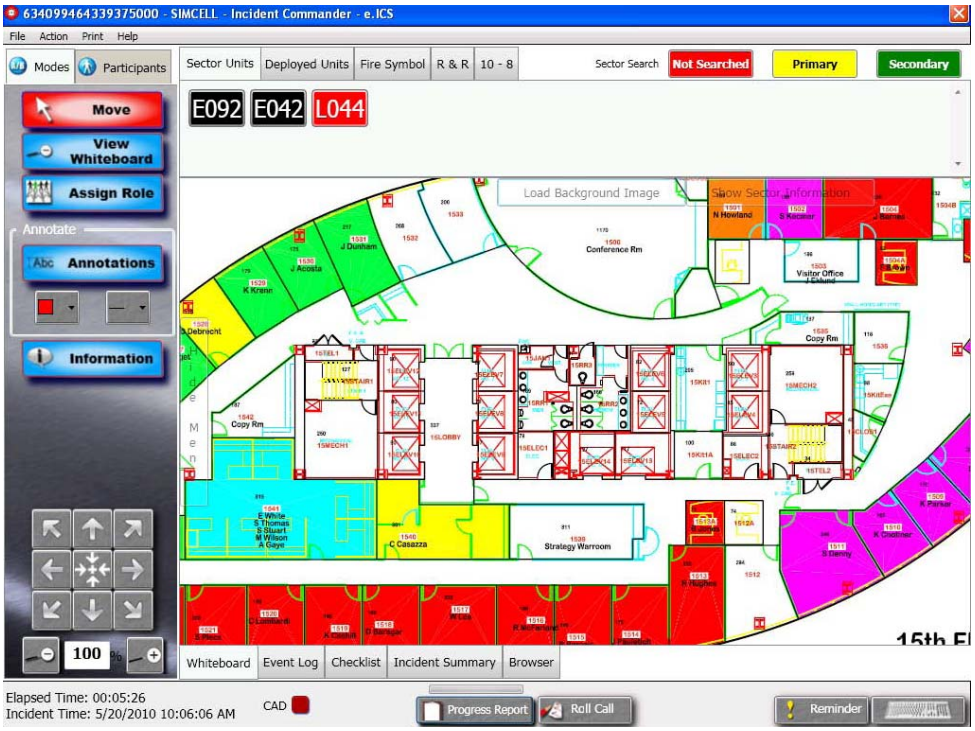

Figure 13. Floor Plans (From: Prototype of FDNY ECB)

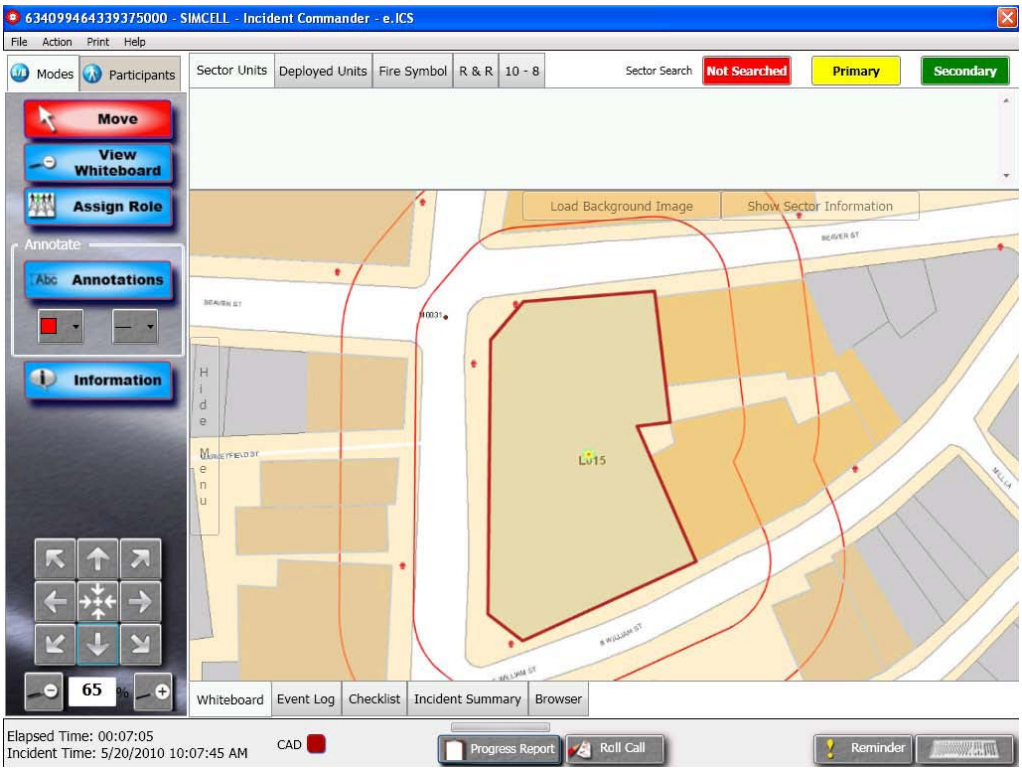

Figure 14. Overhead View of the Structure and Surrounding Structures (From: Prototype of FDNY ECB)

APPENDIX D. SUMMARY OF RECOMMENDATIONS

- Establish secure portal on IAFC website
- IAFC and NFA sponsored intelligence training
- Develop TLO, FLO, ILO training programs
- Provide fire department points of contact for FSIE
- Use of technology for disseminating intelligence
    - HSIN
    - EMR-ISAC
    - Electronic Command Boards
- Internal dissemination mechanisms
    - Emergency action messages

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Bryson, J. M. (2004). *Strategic planning for public and nonprofit organizations, a guide to strengthening and sustaining organizational achievment.* San Francisco: Jossey-Bass.

Bush, George W. (2005). Presidential memorandum: Guidelines and requirements in support of the information-sharing environment. Retrieved July 15, 2010, from http://www.fas.org/sgp/news/2005/12/wh121605-memo.html

Cloud, R. (2008). *Future role of fire service in homeland security.* Monterey, California: Naval Postgraduate School.

Congress, C. R. (2006). *Homeland security intelligence:perceptions, statutory definitions, and approaches.* Washington, D.C.: Congressional Research Service.

Department of Homeland Security. (2008). National response framework. Washington, D.C.

Department of Homeland Security. Homeland Security Information Network. Retrieved August 10, 2010, from http://www.dhs.gov/files/programs/gc_1156888108137.shtm

Department of Homeland Security. (2009, October). Office of intelligence and analysis report on the status of fire service integration within state and major urban area fusion centers.

Digital Communities. (2008, June). DHS to upgrade homeland security information network. Retrieved August 1, 2010, from http://www.govtech.com/dc/369046

FDNY. (2007). *FDNY terrorism and disaster strategy.* Brooklyn, NY: FDNY.

FDNY. (2010). Emergency action message draft policy.

FEMA. Lessons learned information sharing. Retrieved March 21, 2010, from www.llis.gov

Fowler, Floyd J. (2001). *Survey research methods*. Thousand Oaks, CA: Sage Publications, Inc.

Group, I. T. (2009). *Intelligence guide for first responders.* Washington, D.C.: National Couterterrorism Center.

Heirston, B. (2009). *Terrorism prevention and firefighters: Where are the information sharing boundaries.* Monterey, CA: Naval Postgraduate School.

Kim, W. C. (2005). *Blue ocean strategy.* Boston: Harvard Business School Press.

National Intelligence Strategy of the United States of America. (2005).

National Strategy for Information Sharing. (2007, October).

Office of the Director of National Intelligence. (2008). United States Intelligence Community Information Sharing Strategy.

Pfeifer, J. (2009). Network command:The high-tech future of incident management. *WNYF*, pp. 14–18.

Presidential Executive Order 13356. (2004). *Strengthening the sharing of terrorism information to protect Americans.* Washington, D.C.

Program Manager, I. S. (2006). *Information sharing environment implementation plan.* Washington, D.C.: Office of the Director of National Intelligence.

Representatives, U. H. (2005). *Beyond connecting the dots, a vital framework for sharing law enforcement intelligence information.* Washington, D.C.

Rothkopf, D. J. (2002). Bridging the intelligence gap. *Blueprint Magazine*.

Salyers, R. A., & Lutrick, T. (2007, February). Best defense. *Fire Chief*, pp. 48–53.

Security, D. O. (2005). *Global justice information sharing initiative, fusion center guidelines, developing and sharing information and intelligence in a new world.* Washington, D.C.: Department of Homeland Security.

Security, D. O. (2008). DHS/DOJ Fusion Process, Technical Assistance Program and Services Brochure. Washington D.C.

Security, D. O. (2009). Emergency services sector information and intelligence requirements workshop. *Emergency Services Sector Information and Intelligence Requirements Workshop.* Emmitsburg, MD: Department of Homeland Security.

Security, D. O. (2009). *Fire service intelligence enterprise concept plan.* Washington, D.C.: Department of Homeland Security.

Security, D. O. (2010). *Fire service integration for fusion centers.* Washington, D.C.: United States Department of Justice.

Townsend, K., Sullivan, J. P., Monahan, T., & Donnelly, J. (2010). *Intelligence-led mitigation.* Washington, D.C.

United States Fire Administration. (2010). Fire service information sharing—message guide.

United States Fire Administration Response Section. *Emergency management and response-information sharing and analysis center brochure*. Retrieved August 2, 2010, from www.usfa.dhs.gov

United States Government Accountability Office. (2007). Testimony before the Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment, Committee on Homeland Security, House of Representatives. Information Technology: Homeland Security Information Network Needs to Be Better Coordinated with Key State and Local Initiatives. Washington, D.C.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Know Library
   Naval Postgraduate School
   Monterey, California

3. Chief of Department Edward S. Kilduff
   Fire Department New York
   Brooklyn, New York

4. Assistant Chief Joseph Pfeifer
   Center for Terrorism and Disaster Preparedness
   Fire Department New York
   Queens, New York

5. Mand Library
   Fire Department New York-Bureau of Training
   New York, New York