NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

ESTABLISHING THE INTELLIGENCE REQUIRED BY THE FIRE DEPARTMENT CITY OF NEW YORK FOR TACTICAL AND STRATEGIC DECISION MAKING

by

James W. Kiesling

March 2016

Thesis Advisor: Robert Simeral
Second Reader: Christopher Bellavita

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** March 2016	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE ESTABLISHING THE INTELLIGENCE REQUIRED BY THE FIRE DEPARTMENT CITY OF NEW YORK FOR TACTICAL AND STRATEGIC DECISION MAKING	**5. FUNDING NUMBERS**
6. AUTHOR(S) James W. Kiesling	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB protocol number ____N/A____.

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

13. ABSTRACT (maximum 200 words)

Following the tragic events of September 11, 2001, numerous reports came to the same conclusion: there was an urgent need to enhance information sharing throughout the homeland security community (HSC). The report of the National Commission of the Terrorist Attacks upon the United States set forth numerous failures of information sharing that occurred throughout the HSC involving events leading up to 9/11, the attacks, and the response. The necessity of information to enable the fire service (FS) to make proper decisions is clear. Groups working on how to best provide the FS with intelligence believe that in order to assist the Intelligence Community (IC) in providing the intelligence, a specific list should be developed. This has become the goal of this thesis. In analyzing what intelligence is required by the FS, it has become apparent that there are a vast number of variables. Taking into account these variables and the dynamic environment has revealed that compiling a list of specific requirements is not practical. In lieu of a specific list, a better option would be to make available to the IC an understanding of the operations of the FS. By providing an explanation of the information that the FS utilizes to respond to emergencies, an understanding, as opposed to a stagnant list, of the intelligence needs of the FS could be established. To accomplish this, a guide for the IC could be established—a guide similar to those available to the FS explaining the IC. This guide could explain the intelligence needs of the FS at a level that is understandable and pertinent to those tasked with fulfilling them. A draft guide is included in the appendix of this thesis.

14. SUBJECT TERMS emergency response, fire, fire department, Fire Department City of New York, FDNY, fire service, firefighters, first responders, homeland security, information sharing, intelligence, intelligence needs, prevention, response, Fire Service Intelligence Enterprise, network fusion	**15. NUMBER OF PAGES** 115
	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

ESTABLISHING THE INTELLIGENCE REQUIRED BY THE FIRE DEPARTMENT CITY OF NEW YORK FOR TACTICAL AND STRATEGIC DECISION MAKING

James W. Kiesling
Captain, Fire Department City of New York, Special Operations Command
B.A., John Jay College of Criminal Justice, 2009

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
March 2016**

Approved by: Robert Simeral
Thesis Advisor

Christopher Bellavita
Second Reader

Erik Dahl
Associate Chair of Instruction
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Following the tragic events of September 11, 2001, numerous reports came to the same conclusion: there was an urgent need to enhance information sharing throughout the homeland security community (HSC). The report of the National Commission of the Terrorist Attacks upon the United States set forth numerous failures of information sharing that occurred throughout the HSC involving events leading up to 9/11, the attacks, and the response. The necessity of information to enable the fire service (FS) to make proper decisions is clear. Groups working on how to best provide the FS with intelligence believe that in order to assist the Intelligence Community (IC) in providing the intelligence, a specific list should be developed. This has become the goal of this thesis. In analyzing what intelligence is required by the FS, it has become apparent that there are a vast number of variables. Taking into account these variables and the dynamic environment has revealed that compiling a list of specific requirements is not practical. In lieu of a specific list, a better option would be to make available to the IC an understanding of the operations of the FS. By providing an explanation of the information that the FS utilizes to respond to emergencies, an understanding, as opposed to a stagnant list, of the intelligence needs of the FS could be established. To accomplish this, a guide for the IC could be established—a guide similar to those available to the FS explaining the IC. This guide could explain the intelligence needs of the FS at a level that is understandable and pertinent to those tasked with fulfilling them. A draft guide is included in the appendix of this thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CIA	Central Intelligence Agency
CPT	Center for Policing Terrorism
CTDP	Center for Terrorism and Disaster Preparedness
DHS	U.S. Department of Homeland Security
DOHMH	NYC Department of Health and Mental Hygiene
DOJ	U.S. Department of Justice
EMP	electromagnetic pulse
EMS	emergency medical service
EOC	emergency operations center
ERPs	emergency response plans
FBI	Federal Bureau of Investigation
FDNY	Fire Department City of New York
FDOC	Fire Department Operations Center
FEMA NPD	FEMA's Office of National Preparedness
FEMA	Federal Emergency Management Agency
FF	firefighter
FS	fire service
FSIE	Fire Service Intelligence Enterprise
GIS	geographic information systems
GPM	gallons per minute
HSC	homeland security community
HSIN	Homeland Security Information Network
HSPD-8	*Homeland Security National Presidential Directive 8: National Preparedness*
HVAC	heating ventilating and air conditioning
I&A	DHS Office of Intelligence and Analysis
IC	Intelligence Community

IED	improvised explosive device
IP	Office of Infrastructure Protection
ITACG	Interagency Threat Assessment and Coordination Group
JCAT	Joint Counterterrorism Assessment Team
JFK	John F Kennedy
JTTF	Joint Terrorism Task Force
LE	law enforcement
LEC	law enforcement community
NCTC	National Counterterrorism Center
NFPA	National Fire Protection Association
NIPP	*National Infrastructure Protection Plan*
NPG	*National Preparedness Goal*
NPS	*National Planning Scenarios*
NPS: AT	*National Planning Scenarios: Attack Timelines*
NSIS	*National Strategy for Information Sharing*
NYC	New York City
NYPD	New York City Police Department
OI&A	Department of Homeland Security Office of Intelligence and Analysis
PPD	presidential policy directive
PPE	personal protective equipment
RATH	Risk Assessment and Target Hazard Unit
ROCIC	Regional Organized Crime Information Center
SCBA	self-contained breathing apparatus
SNRA	*Strategic National Risk Assessment*
SOC	FDNY Special Operations Command
SOP	standard operating procedure
START	National Consortium for the Study of Terrorism and Responses to Terrorism
Stratfor	Strategic Forecasting Inc.

TATP	triacetone triperoxide
TRIPwire	DHS technical resources for incident prevention
UA	universal adversary
USFA	U.S. Fire Administration
USS	United States ship
VBIED	vehicle-borne improvised explosive device
WMD	weapon of mass destruction

THIS PAGE INTENTIONALLY LEFT BLANK

DEDICATION

I would like to dedicate this thesis to:

My mother, Grace M. Kiesling, who passed away during the writing of this thesis.

My wife, Gayl E. Kiesling, who married me during the writing of this thesis.

The members of my family that have served or serve:

My father, Joseph J. Kiesling (deceased), battalion chief FDNY, F2 U.S. Navy, who served in WWII aboard the USS *Ault*.

My brother, Joseph J. Kiesling, fireman FDNY (retired).

My nephew, Joseph J. Kiesling, firefighter FDNY.

My sister, Patricia Hantsis, major, U.S. Air Force Reserve, who served in Iraq during the Iraq War.

My nephew, Kevin Miller, fire marshal FDNY.

The 343 members of FDNY who gave their lives responding to the attacks on September 11, 2001; 93 of whom were my Special Operations brothers.

> Go tell the Spartans, Passerby, That here, obedient to their laws, We lie
>
> — Simonides, Greek poet (556 BC–468 BC),
> epitaph for the Spartans who fell at Thermopylae

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank my thesis advisor, Captain Robert Simeral, and second reader, Dr. Christopher Bellavita, not just for their help, but also for the extreme patience they exhibited throughout the writing of this thesis. In addition, I would like to thank the many other members of the Naval Postgraduate School and my cohorts who helped me in so many ways during my time here.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT—BACKGROUND

In the aftermath of the tragic events of September 11 2001, numerous reports from various government agencies and committees culminated in the same conclusion: There was an urgent need to enhance information and intelligence sharing throughout the homeland security community (HSC). The *Final Report of the National Commission on Terrorist Attacks upon the United States* offered numerous recommendations designed to promote information sharing in an attempt to restore a balance between security and the sharing of intelligence (National Commission on Terrorist Attacks upon the United States [9/11 Commission], 2004).

In evaluating the progress made by the HSC, the U.S. Homeland Security Council believes that it has made great strides within the Intelligence Community (IC) to improve internal and external communication but that more remediation was needed, stating, "While our information sharing capabilities have improved significantly, substantial obstacles remain. We must continue to break down information barriers among Federal, State, local, and Tribal partners and the private sector" (as cited in Heirston, 2009, p. 5). The fire service (FS) was thus directed to persevere in efforts to improve communications at all levels and within all exigencies. However, the IC has often been reluctant to share information with those considered outside (and sometimes within) the information sharing community. There have been numerous examples of this reported by the 9/11 Commission among others. While operating jointly to investigate leads on the USS Cole bombing, the CIA and FBI withheld information from each other on several occasions and at times failed to provide reports on information that was initially provided to both agencies jointly (9/11 Commission, 2004, pp. 266–269). This reluctance to share intelligence is somewhat understandable as intelligence not closely guarded could compromise methods and sources. Often, intelligence would not be disseminated unless specifically requested due to an absence of a requirement that agencies share information.

Since the FS is outside the normal intelligence loop, the command elements often do not receive necessary intelligence because officers may not know what types of intelligence to request ahead of time. In addition to an historical reluctance to share intelligence, the IC has limited awareness of the intelligence needs of the FS, as do administrators within the FS. Without background knowledge about the manner in which intelligence is sought and handled within the FS, the IC cannot produce and disseminate actionable intelligence to the FS community.

The FS has a definite need for accurate and timely intelligence. This intelligence can be utilized to minimize the danger to FS personnel during the preparatory and the response phases of a terrorist attack as well as for preventing such an attack. This intelligence can also be used to protect the lives of other first responders as well as the civilians that they are seeking to protect. At present, the FS does not consistently receive the information that it needs in order to accomplish its missions and protect its personnel.

B. RESEARCH QUESTIONS

The research questions posed here focus on the intelligence requirements of Fire Department City of New York (FDNY) but can be applied throughout the FS.

1. Primary Question

With regard to the mission of the FDNY to prevent, prepare for and respond to terrorist attacks; what specific intelligence and/or information is required by the FDNY?

2. Secondary Questions

What intelligence and/or information are not pertinent to the mission of the FDNY?

How will intelligence and/or information provided to the FDNY be utilized to accomplish its mission?

C. SIGNIFICANCE OF RESEARCH

To assist in breaking down the barriers to effective sharing, one of the preliminary steps for the FS to take is to determine exactly what information it does and does not

need to carry out its mission. Additionally, the FS should also establish other parameters regarding the intelligence required for effective action. In addition to the specific intelligence requirements, the FS would have to establish other standard operating procedures (SOPs) regarding information handling such as: developing the appropriate training for those handling the intelligence; if applicable, obtaining the appropriate clearances for those with a need to know; regarding the dissemination of information including not just who requires what level of information but also the technology required to provide it; for reporting information obtained by the FS; and establishing a method of providing feedback.

If the FS can establish these parameters beforehand with a comprehensive list that details what is needed, why it is needed, and how it will be protected, the ability of the FS to obtain the necessary intelligence would be greatly enhanced. This enhanced capability has the potential to save the lives of both responders and civilians.

The intent of this thesis is that it will produce data that will prove useful toward enhancing the intelligence capabilities of the FDNY Center for Terrorism and Disaster Preparedness (CTDP). A consequence of the attainment of the main goal is that the information provided to FDNY's partners in the IC will further enhance its ability to deliver the necessary intelligence to other first responders. In addition a potential long-term byproduct is that some variant of this information would be of some use to the FS as a whole.

A secondary purpose for this thesis is that by documenting the basic structure of the FDNY CTDP, the concept of fusion by networking will prove to be adaptable toward fulfilling the intelligence needs of those fire departments that do not have access to a state or major urban area fusion center.

D. HYPOTHESIS

The necessity of timely, actionable intelligence to enable the FS to make appropriate tactical and strategic decisions is clear. In order to assist the IC in providing the appropriate information and to aid those compiling the information, a standardized set of the required information should be developed. This would include what information is

necessary and what information is not. In addition, it would offer a basic description of why it would be required, and how it would be handled and disseminated. Including the explanation of why the intelligence was necessary and what should be done with it, would assure the IC that the intelligence requested was necessary and that it would be safeguarded. In addition, by providing an explanation of the intelligence that is not required, the flow of focused information should be expedited; as much of the most sensitive information, while important to the military and law enforcement (LE), has no practical application for the FS.

E. METHOD

The intent of this thesis is to conduct a policy analysis utilizing a policy options analysis methodology. The goal of the thesis analysis is to identify the positive and negative aspects of each policy in terms of potential adaptability, both practically and financially, and also in terms of operational impact.

There are policies that are commonly used to provide the FS with intelligence, and the FDNY has developed its own policies. While these policies can provide a consistent flow of intelligence to those departments that have adapted them; this flow is delivered either unanalyzed or typically analyzed by analysts trained for LE intelligence analysis and not fire intelligence. This thesis employs a policy options analysis to analyze a common method of providing intelligence to the FS by comparing it to an analysis of the method currently in use by the FDNY and to the analysis of the model of a potential policy option.

F. CRITERIA FOR JUDGING SUCCESS

With the stated goal of FS being able to obtain and disseminate the intelligence that is necessary to prevent, prepare for, and respond to terrorist attacks, it is extremely difficult to develop a tangible criteria for judging success. This is in part because goal is one of negative results. Success cannot be measured when no untoward incidents occur. If nothing happens, it is difficult to attribute the lack of incident directly to the policies that were implemented. This is compounded by the fact that such events such as the

attacks on 9/11, tend to be rare and unique, which makes it difficult to establish a baseline from which to evaluate newly implemented policies.

It is not practical to comparatively judge the final outcome of these policies, which is the prevention of, preparation for, and the response to terrorist attacks. However, we can judge the individual policies' ability to provide the intelligence that the end users deem essential to their mission. The FS and FDNY collectively have experience in dealing with the intelligence provided by policy options, identified as A and B, as well as what is required to establish and maintain these policies. What is required for this policy options analysis is to compare policy options A and B to policy option C.

To accomplish a comparison, it is first be necessary to establish a set of intelligence requirements for the FS, referred to as policy option C. This policy prototype would be provided to members of the IC, such as fusion centers and LE intelligence. Those receiving this policy prototype would examine the intelligence requirements that were provided to them to ascertain if the guidelines set forth in the prototype are understandable and if they able to provide the requirements as listed.

If the requirements meet the approval of the selected members of the IC (e.g., DHS and FBI) the next step is to use these requirements (designated as policy option C) to obtain intelligence reports from the same LE sources utilized to evaluate the prototype. These reports would then be compared to intelligence reports that have been provided under policies A and B. The final criteria for success would be does the end product yield more actionable intelligence and/or reduce the amount of irrelevant data?

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

A. INTRODUCTION

After 9/11, there emerged a large body of literature dedicated to ascertaining just how such a tragedy was allowed to happen and how to prevent a tragedy of this magnitude from happening again. Much of this literature is dedicated toward intelligence operations and information sharing. The first part of the literature review traces the literature that accompanied the evolving efforts to strengthen information sharing in the HSC. These efforts were initially were focused on the military, CIA, and FBI and later, as these efforts began to be realized, efforts shifted to local LE and the development of fusion centers. While this shift resulted in intelligence being disseminated to the level of local LE, this intelligence was not widely disseminated amongst local first responder communities. The progression of literature began to address in a more specific manner the dissemination of information to first responders and the FS. This section of the literature review examines FS intelligence operations today, focusing on the current status of the FS's pursuit to fulfill its intelligence requirements. In addition this section examines the involvement of the FS in fusion centers and the efforts of the Fire Department, City of New York (FDNY) to develop an effective intelligence network. The above mentioned body of literature represents the progression and current status of efforts to provide the FS with the intelligence necessary to fulfill its counterterrorism mission.

The next section of the literature review covers the literature that was utilized to ascertain what specific intelligence would be required be the FS and the FDNY to fulfill their HS mission. The first portion covers literature examining the various stages of a terrorist attack, beginning with the inception of the attack, through the attack itself, and finally examining the aftermath. The following portion covers the capabilities of the FS to respond to the attack throughout the various stages.

B. OVERVIEW AND CURRENT STATUS OF EFFORTS TO PROVIDE INTELLIGENCE TO THE FS POST-9/11

In response to 9/11, the IC and HSC have been tasked with improving their ability to provide intelligence to emergency responders including the FS.

1. Overview of Intelligence, and the National Intelligence and Homeland Security Communities

The catastrophe that occurred on September 11, 2001 staggered the nation and shocked the IC. As a consequence of these events and the accompanying need to understand what went wrong, numerous agencies launched in-depth studies to ascertain what could have been done to prevent this tragedy. The most comprehensive of these studies was the *9/11 Commission Report.* This study reported numerous failures of information sharing that occurred throughout the IC involving events leading up to 9/11, the attacks on 9/11, and the response to these attacks (9/11Commission, 2004). The commission offered numerous recommendations regarding information sharing, such as providing various incentives to promote information sharing in an attempt to restore a balance between security and the sharing of intelligence (9/11 Commission, 2004, p. 417). These recommendations included every level of government to the president and stated the president should lead a government-wide effort to promote information sharing between agencies (9/11 Commission, 2004, p. 418).

While the *9/11 Commission Report* was the government's attempt to understand the events of 9/11, the *United States National Strategy for Homeland Security* was the formal government response to these events and represented a strategy aimed at mobilizing and organizing the entire nation against terrorist attacks. Several sections of the strategy pertain to the IC. For instance, the intelligence and warning section explains the necessity of implementing a system with the capacity to detect a terrorist attack before it occurs. The information sharing and systems portion pertains to the technology of sharing information between the various agencies. The domestic counterterrorism segment of this thesis examines the need to specifically improve communication and coordination between law enforcement agencies, and enhances the joint terrorism task forces (JTTFs) (Office of Homeland Security, 2002).

For this thesis, an overview of the IC was obtained through the examination of Mark Lowenthal's text, *Intelligence: From Secrets to Policy*, first published in 1999 and currently in its sixth edition. This text is considered by many in the HSC to be essential reading on the topic of the IC. Moreover, Lowenthal defines intelligence and covers such topics as: the intelligence cycle, the intelligence community, gathering and analyzing intelligence, intelligence policy and accountability, and the U.S. policy on national security and intelligence. Lowenthal's book provides a thorough overview of the IC; however, it offers nothing new in regard to intelligence operations at a state or local government level (2006). The summations of the literature covered in this section, as well as the findings of many other studies conducted at that time are essentially identical. They all establish the necessity for the IC to share intelligence, yet they provide few specific details in regard to the systems necessary to accomplish this and generally do not specify the required participants.

2. Local Law Enforcement Involvement in Information Sharing

At the local level, LE has become the focus of the information sharing efforts. This is characterized by the publication in 2005 of documents such as *Intelligence-Led Policing: The New Intelligence Architecture, New Realities, Law Enforcement in the Post-9/11 Era* (Bureau of Justice Assistance, 2005) and the *Fusion Center Guidelines* (U.S. Department of Justice [DOJ] & U.S. Department of Homeland Security [DHS], 2005) developed by the DOJ in collaboration with the DHS. As the titles of these documents indicate, the focus is on intelligence for LE with an emphasis on terrorism prevention. To illustrate this point in the section of the *Fusion Center Guidelines* (DOJ & DHS, 2005, p. 3) that defines a fusion center, the guidelines state that they are a conduit to implement portions of the *National Criminal Intelligence Sharing Plan*, embracing such concepts as intelligence-led policing and community policing.

In 2006, the DHS published the *Department of Homeland Security Intelligence Enterprise Strategic Plan*. While this document contains multiple references to LE and the LE role in the DHS intelligence plan, references to all other agencies at the local level were indiscriminately referred to by such blanket terms as stakeholders or customers and

were not provided with specific roles (U.S. Department of Homeland Security [DHS], 2006a).

3. The Fire Service Involvement in Information Sharing

While the previously reviewed documents express the necessity to establish reliable information sharing within the established IC, they do little to establish an intelligence conduit between the IC and local stakeholders. As the U.S. Homeland Security Council argued, "While our information sharing capabilities have improved significantly, substantial obstacles remain. We must continue to break down information barriers among Federal, State, local, and Tribal partners and the private sector" (Heirston, 2009, p. 5).

When the *National Strategy for Information Sharing* (*NSIS*) was released in 2007, one of the stated goals was to help ensure that "those responsible for combating terrorism must have access to timely and accurate information regarding those who want to attack us, their plans and activities, and the targets that they intend to attack" (U.S. White House Office, 2007, p. 2). In the *NSIS*, the IC continues to be the primary source for information; however, the IC must adapt to enable it to interact with non-traditional partners, at all levels of government, with roles in prevention and response. The *NSIS* also stated that the IC could obtain important information regarding possible terrorist attacks from partners outside the IC (U.S. White House Office, 2007).

The DHS Office of Intelligence and Analysis (I&A) held a workshop in 2009 in conjunction with the Office of Infrastructure Protection (IP), and the U.S. Fire Administration (USFA) (DHS, 2009a, p. 1). The purpose of this workshop was to ascertain the intelligence requirements of emergency responders. In attendance at the seminar were representatives from fire, rescue, hazardous materials, law enforcement, emergency medical service, and emergency management Those in attendance found that analysts in the IC generally do not have an understanding of the roles of those in the emergency response community or its intelligence requirements. Those in attendance also remarked that they did not possess a good understanding of the role that the IC could play in regard to first responders (DHS, 2009a, p. 7).

The majority of information written at this time, in reference to enhancing the FS interaction with the IC, addresses the Firefighter as an intelligence gatherer. A report published by the Center for Policing Terrorism (CPT), *Firefighters' Developing Role in Counterterrorism*, recommended that the FS serve a preventive intelligence role (Gartenstein-Ross & Dabruzzi, 2008). According to the authors, firefighters have an exceptional access to the buildings of the nation and could act as sensors of opportunity to report any suspicious activity they observed. In addition, they reported that the FS's excellent standing in the community would enable it to develop community networks and educate the public on how to recognize potential terrorist activity (Gartenstein-Ross & Dabruzzi, 2008).

The documents reviewed express an awareness that the information barriers between the IC and first responders need to be broken down, and they even encourage and have begun the framework for information sharing among federal, state, local, and tribal officials, and the private sector. The literature indicates that while the IC is beginning to recognize the FS, the IC does not have a good understanding of the FS's intelligence requirements and mostly regard the FS as a force multiplier to gather intelligence. Absent from this body of literature are any specific recommendations to break down the barriers between the IC and first responders. In addition, the literature offers little more than an acknowledgement of the IC's lack of understanding of the FS.

4. Fire Service Intelligence Operations Today

The literature reviewed in this portion examines the current status of the FS's attempts to acquire the intelligence necessary to make sound decisions. To accomplish this, literature chosen focuses on the current status of fusion centers and on the FDNY. The FDNY is representative of the portions of the FS without practical access to a fusion center.

In response to the need to develop actionable intelligence at a local level, in 2005 the U.S. Department of Justice (DOJ) and the U.S. Department of Homeland Security (DHS) released the previously mentioned *Fusion Center Guidelines*. This paper was the result of a focus group composed of representatives from law enforcement agencies at the

federal, state, and of local levels. In addition, this document provides solid guidelines for those seeking to establish a fusion center to institute an information sharing environment down to the local level (DOJ & DHS, 2005). While the basic concept of this text is sound and designed to get intelligence to the local law enforcement community (LEC), it contains no specific provisions to incorporate the FS into these centers.

The procedures for incorporating the FS into fusion centers is covered in *Fire Service Integration for Fusion Centers* published by the DOJ in 2010. *Fire Service Integration for Fusion Centers* is an appendix to the DOJ Global Justice Information Sharing Initiative's, *Baseline Capabilities for State and Major Urban Area Fusion Centers*. According to the U.S. Department of Justice, "The document identifies how fusion centers can effectively integrate the FS into their existing analysis and information/intelligence sharing processes" (U.S. Department of Justice, 2010, p. 1). The document points out some of the advantages of having FS personnel in the center, such as their contributions of raw information, or serving as subject matter experts. It also explains how intelligence is an important component of the FS mission (U.S. Department of Justice, 2010). This is a very useful document but still it does not address all the issues involved in providing consistent intelligence to the FS. The specific intelligence requirements are not addressed, and SOPs for receiving and disseminating intelligence are only addressed in that the document states that the FS constituent of the fusion center should participate in developing the various procedures.

In response to the expanding need for intelligence in the first responder community, the Interagency Threat Assessment and Coordination Group (ITACG) of the National Counterterrorism Center (NCTC) published the first edition of *Intelligence Guide for First Responders* in 2009 (Interagency Threat Assessment and Coordination Group, 2009). This guide is now in its third edition, which was published by the Joint Counterterrorism Assessment Team (JCAT), the successor to the ITACG (Joint Counterterrorism Assessment Team [JCAT], 2015). This guide was developed by LE at the federal, state, and local levels and the FS and DHS "to assist state, local, and tribal first responders in accessing and understanding Federal counterterrorism, homeland security, and weapons of mass destruction intelligence reporting" (ITACG, 2009, p. 2).

This guide offers a synopsis of intelligence, handling intelligence, the IC, the varieties of intelligence reports obtainable by first responders, and an explanation of the language utilized by the IC (ITACG, 2009). This guide contains valuable information for those in the FS trying to understand intelligence operations. It does not contain specifics on the intelligence that is required by the FS or the procedures to handle it, other than explaining the classifications of intelligence.

In 2007, FDNY and the DHS hosted the inaugural Fire Service Intelligence Enterprise (FSIE) conference. This conference consisted of a working group of 15 of the nation's largest fire departments: Baltimore, Boston, Chicago, Denver, District of Columbia, Houston, Las Vegas, Los Angeles City, Los Angeles County, Miami-Dade, New York, Philadelphia, Phoenix, San Francisco, and Seattle. Major federal stakeholders in the FSIE include the Department of Homeland Security's Office of Intelligence and Analysis (OI&A), FEMA's Office of National Preparedness (FEMA NPD), the United States Fire Administration (USFA), the Department of Justice (DOJ), and other federal, state, and local stakeholders (Cruthers, 2008, pp. 22–23). The *Fire Service Intelligence Enterprise Concept Plan*, published by the DHS in 2009, defined as a mission essential task of the FSIE the necessity to "define fire service intelligence requirements, including types of intelligence the fire service needs and how that intelligence enhances preparedness and/or operations" (DHS, 2009b, p. 6).

That same year the Emergency Service Sector Information and Intelligence Requirements Workshop was conducted at the National Emergency Training Center on the U.S. Fire Administration's campus in Emmitsburg, Maryland. The purpose of the workshop was to bring together a cross section of state and local stakeholders to begin the process of defining the intelligence needs of first responders, including the FS as well as other stakeholders. The record of their efforts was published in the *Emergency Service Sector Information and Intelligence Requirements Workshop after Action Report* (DHS, 2009a).

Many of the FDNY's post 9/11 rebuilding efforts were directed toward developing the FDNY's intelligence capabilities. In 2006, these efforts led to the creation of the FDNY Center for Terrorism and Disaster Preparedness (CTDP). The CTDP took

the lead in writing the FDNY's terrorism strategy, the *Fire Department City of New York, Terrorism and Disaster Preparedness Strategy*, which outlines much of the department's intelligence operations. This document outlines some of the FDNY's procedures for obtaining, handling, and disseminating intelligence but lacks specifics in regard to intelligence requirements (Fire Department City of New York [FDNY], 2007b, p. 10).

FDNY has further developed its ability to disseminate information through the weekly publication of *Watchline*, its flagship intelligence product (Pfieifer, 2011, p. 10). This publication reaches 50,000 readers every week, including readers beyond the fire service (FDNY, 2013a, p. 20). In addition, the FDNY has implemented such policies as those outlined in *All Unit Circular 342, Sensitive but Unclassified Information Policy*, which sets the mandatory requirements regarding the identification, access, dissemination, storage, and destruction of documents (FDNY, 2009, p. 1).

C. EXAMINING THE STAGES OF A TERRORIST ATTACK AND THE CAPABILITY OF THE FS TO RESPOND

There has been a large body of work done on both potential terrorist attacks and attacks that have occurred or been planned since 9/11 as well as the ability of the nation to respond to terrorist attacks.

1. Anatomy of a Terrorist Attack

The *National Planning Scenarios* (NPS) consist of 15 all-hazard scenarios for use in homeland security preparedness activities and are products of a working group consisting of the DHS and the Homeland Security Council. The *National Planning Scenarios: Attack Timelines* (NPS: AT) are an addition to the *National Planning Scenarios* (DHS, 2006b). These are all-hazard planning scenarios for use by all levels of government in planning for potential terrorist attacks and natural disasters. In NPS, the scenario begins from the time of the attack and was intended to aid in planning the response phase. In contrast, the scenarios in the *National Planning Scenarios: Attack Timelines* (also known as attack prequels) begin with the conception of the attack and end with the culmination of the attack. Additionally, the prequels offer a scenario for each of

the terrorist attacks listed in the NPS.[1] Furthermore, these scenarios are designed to aid in, prevention, and preparation planning.

The Universal Adversary (UA) Program provides the analytical framework in these scenarios for conducting exercises against potential criminal and terrorist adversaries. It builds a complex fictional picture of potential adversaries based on the motivation, capability, and intent of real-world adversaries; while utilizing realistic tactics, techniques, and procedures (U.S. Federal Emergency Management Agency, 2009). The scenarios consist of a data sheet of potential damage, a general overview of the scenario, a universal adversary (UA) group (terrorist group) profile, a list of UA operatives, a detailed attack scenario, and the UA execution timeline. In addition to being a tool to assist in planning for the prevention and preparation stages of an attack, the NPS and NPS: AT, utilized with information from the UA databases, is intended to be used in designing exercises and in the deployment of red teams (DHS, 2006b).

The special report, *60 Terrorist Plots Since 9/11: Continues Lessons in Domestic Counterterrorism,* published by the Heritage Foundation, examines all of the terrorist attacks that have been attempted within the U.S. since 9/11/2001 until the time of its publishing in July of 2013 (Zuckerman, Bucci, & Carafano). This report lists four of these attacks as successful. In addition, the paper finishes with a section deconstructing the terror data to establish lessons learned. Building on this, the Heritage Foundation has published several other special reports documenting domestic terrorist attacks the most recent of which, *67 Islamist Terrorist Plots Since 9/11: Spike in Plots Inspired by Terrorist Groups, Unrest in Middle East* was published in April of 2015 (Inserra, & Phillips).

Whereas the Heritage Foundation's report focuses on terrorist attacks within the U.S. since 9/11 (Inserra & Phillips, 2015), the *2010 NCTC Report on Terrorism*, published by the National Counterterrorism Center, focuses on terrorist attacks worldwide that occurred in 2010 (National Counterterrorism Center, 2011). This report contains many useful breakdowns of this data such as: by region, by attack types, victim

[1] Due to the fact that there are no universal adversary groups involved in natural disasters; there is no additional information in this document pertaining to the natural disaster scenarios.

category, and perpetrator category. The final section of the paper is a chronological listing of terrorist attacks that killed 10 or more people in 2010, complete with a brief description of the attack.

2. Capability of the FS to Respond to a Terrorist Attack

Homeland Security National Presidential Directive 8: National Preparedness (HSPD-8) of 2003 was the impetus for this portion of the research (White House, 2003). Issued by the president "This directive establishes policies to strengthen the preparedness of the United States to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies" (White House, 2003, sec. 1). In response to this directive, in March 2005, the Department of Homeland Security (DHS) released the *Interim National Preparedness Goal* (2007, p. iii). This goal established a national vision and priorities to guide efforts to strengthen the nation's preparedness and was intended to be utilized in conjunction with the *National Planning Scenarios* (DHS, 2005b) and the *Target Capabilities List* (DHS, 2005b, p. iii).

The *Strategic National Risk Assessment* was written by U.S. Department of Homeland Security (2011b) to support the establishment of the *National Preparedness Goal*. Its purpose is "to inform homeland security preparedness and resilience activities," this assessment "evaluated the risk from known threats and hazards that have the potential to significantly impact the Nation's homeland security" (DHS, 2011b, p. 1). Publication of the *National Preparedness Guidelines* (*Guidelines*) in 2007 completed development of the national goal. It supersedes the *Interim National Preparedness Goal* and defining "what it means for the Nation to be prepared for all hazards" (DHS, 2007, p. iii). The *National Preparedness Guidelines* were developed through several sub-components. These consisted of the *Universal Task List*, *Target Capabilities List*, and *National Planning Scenarios*. The *Universal Task List* is a list consisting of over 1,600 distinctive tasks. Each of these tasks is an important component toward preventing, protecting from, responding to, and recovering from the scenarios that are put forth in the *National Planning Scenarios* (DHS, 2007, p. iii). The *Target Capabilities List* defines 37 specific capabilities that organizations must as a group obtain in order to respond

successfully to disasters and provides guidance on building and maintaining these capabilities (DHS, 2007, p. iii). The *Fire Department City of New York, Terrorism and Disaster Preparedness Strategy* identifies the FDNY's function in relation to each of the target capabilities as either a leader or in a support role (FDNY, 2007b, pp. A-1–A-3).

D. CONCLUSION

In examining the IC's ability to fulfill the intelligence requirements of the FS brought on by the events of 9/11, I first examined literature pertaining to the structure of the IC and the background of the events of 9/11 that established intelligence sharing as a priority. This literature contains no direct connections between the FS and any members of the IC. The recommendations contained in these writings are mostly general in nature, encouraging information sharing and providing a foundation for future efforts. The next section of literature establishes the requirement of the IC to get first responders the information they need to fight terrorism. While most of the writing examined pertains to LE, there is some mention of the FS. When the FS is mentioned, it is noted that the IC does not understand the intelligence needs of the FS. In addition, the majority of the literature that mentions the relationship between the FS and the IC addresses potential that the FS has to provide intelligence to the IC. In the final section, the literature establishes a methodology to transfer information to the local level and provides some guidelines on how different segments of the FS can access this information, and basic instructions on how to use it once obtained. In the final analysis of the literature, all of the groups working toward establishing a reliable FS intelligence apparatus expressed similar findings. In the *Fire Service Integration for Fusion Centers*, it advises, "Fire service constituents should participate in the identification of the roles and responsibilities of the fusion center's fire service stakeholders, including their needs as a customer of the center" (DHS, 2010, p. 10). Participants in the Emergency Service Sector Information & Intelligence Requirements Workshop reported that a comprehensive list of information and intelligence requirements, including general applications for each, would be a valuable tool for intelligence analysts (DHS, 2010, p. 7). Finally, the FSIE listed one of its overarching goals as facilitating the "identification and development of information and intelligence sharing requirements" for FS personnel (DHS, 2009b, p. ii).

Assistant Chief Joseph Pfeifer (2012), the FDNY's Chief of Counterterrorism and Emergency Preparedness, elaborates on some of the problems the FS experiences in obtaining intelligence in his article, "Network Fusion: Information and Intelligence Sharing for a Networked World," published in *Homeland Security Affairs*. Chief Pfeifer writes of the dangers of information originating from a place of limited perspective, with the information only being pushed when the originating agency deems it necessary (2012, p. 5). He also writes of various types of organizational bias that can hinder the dissemination of appropriate intelligence, including an in-group bias toward LE as well as another form of bias, mitigation neglect. Mitigation neglect is a bias toward intelligence required to prevent a terrorist attack, neglecting the intelligence that is necessary to mitigate such an attack (Pfeifer, 2012, pp. 7–8). These phenomena can be overcome by clearly establishing the intelligence requirements of the FS.

III. POLICY OPTIONS ANALYSIS

In choosing the appropriate policies to analyze, I considered representations from a full spectrum of options. At one end of this spectrum are fusion centers, which are considered the upper end in regard to providing intelligence. At the other end is the more traditional method of having local LE provide intelligence to the FS. The fusion center option was discounted due to the fact that this is not an option that is available to FDNY. Network fusion employed by FDNY to procure intelligence is utilized as one of the policy options because the desired outcome of this thesis is obtaining the best intelligence possible for the FDNY and therefore its current policy had to be included in the analysis. Finally, the central premise of the thesis, the policy option of establish fire service intelligence requirements, was included. This provided the following policies for analysis:

- Policy Option A: Traditional intelligence methods
- Policy Option B: Network fusion
- Policy Option C: Establish fire service Intelligence requirements

A. POLICY OPTION A: TRADITIONAL INTELLIGENCE METHODS

An option widely used by the FS to obtain intelligence is from the local law enforcement community. In this method, local LE passes on the intelligence it has received to the local fire department. There are no nationally recognized standards by which intelligence is required and should be provided to the FS. This method places the decision about what information to provide to the FS into the hands of the LE intelligence personnel. In general, the IC is structured around military and LE intelligence requirements. The intelligence that is necessary to identify and arrest a suspected terrorist in order to prevent a terrorist attack is very different from the intelligence necessary to respond to a successful chemical attack on a subway system. By leaving the decision in the hands of someone or some group trained to provide intelligence to LE, there is a danger of receiving either insufficient intelligence for the FS or an intelligence overload. That being said, the intelligence that would be obtained would certainly contain the immediately critical intelligence, such as information regarding an impending attack that

would be deemed important to everyone. Some advantages of this system are that much of the local LEC already has an established intelligence pipeline, and generally, local law enforcement has a preexisting relationship with the local FS. This allows a local fire department to relatively easily establish a source of intelligence for minimal costs.

B. POLICY OPTION B: NETWORK FUSION

The option that is currently in use by the FDNY is called network fusion. During the rebuilding efforts in the aftermath of 9/11, the FDNY sought to develop its intelligence capabilities. This rebuilding process has led to the creation of the FDNY Center for Terrorism and Disaster Preparedness (CTDP), which acts as a hub for the FDNY's intelligence activities. Presently, the FDNY CTDP does not assign personnel to a traditional fusion center to fulfill its intelligence needs. The CTDP functions on the principles of the fusion center without actually being a fusion center; it refers to how it operates as network fusion. Assistant Chief Joseph Pfeifer, the FDNY's Chief of Counterterrorism and Emergency Preparedness, defines network fusion as an "innovative design for sharing information and intelligence," "which encourages collaboration across multiple disciplines be leveraging technology to connect the unconnected at classified and unclassified levels" (2012, p. 1).

The CTDP staff attends weekly briefings with various agencies and has contacts in other fusion centers that send them information of interest. Members of the CTDP monitor the information that is available on various intelligence networks such as: Homeland Security Information Network (HSIN) and DHS Technical Resources for Incident Prevention (TRIPwire). In addition, there are many members who hold secret and top secret clearances and who assigned to different FDNY commands and units. The information obtained through these varied channels is consolidated (fused) at the CTDP. In the absence of a fusion center, this effort has proven largely successful (J. Esposito, personal communication, February 7, 2011; T. Carroll, personal communication, February 8, 2011). The possibility of missing a piece of intelligence is greatly reduced by receiving intelligence from a variety of agencies and centers as well as from the various intelligence networks. The disadvantage is that in order to collect, consolidate, and

evaluate information from a variety of sources, a dedicated staff is necessary. This may not be an option for some (particularly smaller) departments.

C. POLICY OPTION C: ESTABLISHING FIRE SERVICE INTELLIGENCE REQUIREMENTS

Another method for the FS to obtain the intelligence necessary to carry out its mission would be to develop a standardized set of information indices that the DHS IC would be required to supply to the FS. This information, or a list of intelligence requirements, would include explanations with a degree of precision of why this particular intelligence is pertinent to the FS in regard to its role in preventing, preparing for, and responding to terrorist attacks. If these parameters could be established beforehand, intelligence sharing should be greatly enhanced. Not only would this expedite the dissemination of intelligence, it would assist intelligence agents during information analysis. This program should also include a methodology of how to disseminate the various classifications of intelligence throughout the agency in question. The negative aspect of this approach is the need to establish the necessary requirements and to develop a more interactive relationship with the IC. The benefits that the FS would receive from establishing a reliable intelligence source far outweigh the cost. In addition, the cost that would be incurred to accomplish this would be minimal compared to the expense that the IC incurs in gathering and analyzing the intelligence that it could make available to the FS. This option can be used in conjunction with either of the previously mentioned options.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. INTELLIGENCE FDNY REQUIRES TO REALIZE ITS MISSION

The intelligence cycle consists of developing raw information into finished intelligence for consumers of intelligence to use in their decision-making process (ITACG, 2009, p. 10). The first step of this cycle is "establishing the intelligence requirements of the consumer of intelligence" (JCAT, 2015, p. 30). To determine the intelligence requirements of the FDNY, it was first necessary to determine the mission requirements in regard to national preparedness of the HSC, in general, and the FS and FDNY, specifically.

A. FDNY'S ROLL IN THE FIVE PREPAREDNESS MISSIONS

Presidential Policy Directive (PPD) 8: National Preparedness "was released in March 2011 with the goal of strengthening the security and resilience of the United States through systematic preparation for the threats that pose the greatest risk to the security of the Nation" (DHS, 2014, p. 1). This document was the impetus behind a succession of documents that direct the national preparedness efforts. PPD-8 defines five preparedness missions: prevention, protection, mitigation, response, and recovery. One of the documents called for was the *National Preparedness Goal* (NPG). In order to develop the NPG, the *Strategic National Risk Assessment* (SNRA) was conducted (DHS, 2011b). This risk assessment looked at risks that would have a major impact on the nation's homeland security. The list of risks consisted of 23 national-level events divided into three categories: adversarial/ terrorist, natural, and technological (DHS, 2011b). For purposes of assessing the HS mission of the FDNY, it could be argued that all of the risks in the technological category and the majority of those in the natural category could be the result of terrorism. Two examples would be: wildfires, which have become a potential terrorist weapon, and space weather, which has similar effects to those of an electromagnetic pulse (EMP) attack. These events can be considered opposite ends of the spectrum. EMP attacks are often considered low probability, high consequence events that would require a high level of expense and expertise to carry out. In contrast wildfires, which have been advocated by *Inspire* (the Al Qaeda produced magazine), are

low risk, inexpensive, and require limited technical expertise. All of the events examined have the potential to warrant some level of response by the FDNY. The development of core capabilities was mandated in PPD 8. These core capabilities are essential components required to realize national preparedness. Groups of these 31 core capabilities make up the five preparedness missions (prevention, protection, mitigation, response, and recovery) (DHS, 2014, p. 1).

The five missions are clearly established in these documents, along with the core capabilities required to carry them out. Next, I examined each mission area along with core capabilities in order to determine what the potential role of the FDNY would be in fulfilling the mission requirements. To facilitate this, I conducted a comparison of the FDNY CTDP's *Counterterrorism and Risk Management Strategy* and the preparedness missions. This strategy lists specific examples of the FDNY's potential role in fulfilling each of the preparedness missions. In the analysis of each of the mission areas, specific examples of the FDNY's use of intelligence to fulfill that mission area have been provided.

1. Prevention

Prevention is defined as preventing or circumventing a potential terrorist attack (DHS, 2011a, pp. 4–6). The prevention mission has a unique characteristic when compared to the other missions. While all of the other missions and their accompanying core capabilities are based on an all-hazards approach, the prevention mission is specific to terrorism.

The seven prevention core capabilities are:

1. Planning
2. Public information and warning
3. Operational coordination
4. Forensics and attribution
5. Intelligence and information sharing
6. Interdiction and disruption

7. Screening, search, and detection (DHS, 2011a, pp. 4–6)

An example of prevention efforts, which were initiated in response to intelligence provided to the FS regarding the potential for a nuclear or radiological attack, is the FDNY's radiological detection program. As has been observed in the prevention mission, the FS can serve as not only consumers of intelligence but also as providers of intelligence. Firefighters (FFs) can serve as sensors of opportunity during the normal course of daily operations. The effectiveness of this program is in part due to the extraordinary access afforded to the FS to numerous structures on a daily basis. According to the FDNY, during fiscal year 2014, the FDNY responded in part to 503,668 fire incidents and 1,323,198 emergency medicine services (EMS) incidents in addition to conducting 190,346 fire prevention inspections and 7,206 fire investigations (FDNY, 2015).

A feature of the radiological detection program is that it takes advantage of FDNY member capabilities as roving sensors of opportunity. This program is intended not only as a means of detection but also as a deterrent due to the random nature of the monitoring. As part of this program field units are required to record the normal background levels of radiation in their areas of operation. To accomplish this program sensors are deployed in three ways:

1. Personal radiological sensors are worn by the officers of field units whenever they leave quarters. This policy causes the random monitoring of any structure entered throughout the course of the tour. This monitoring can take place while conducting routine errands, performing building inspections, or responding to fires and emergencies. (FDNY, 2007a, p. 2)
2. In addition to being worn by members, radiological sensors are also deployed on the apparatus of all FDNY fire companies. These sensors are constantly monitoring the atmosphere as fire companies travel throughout the city. (FDNY, 2007a, pp. 1, 7; 2006b, p. 1)
3. As well as monitoring operations on land, FDNY fireboats provide radiological monitoring while conducting routine patrols as well as during choke-point operations conducted in cooperation with law enforcement. (FDNY, 2010, p. 13)

In addition to this prevention by detection program, the FDNY also has several training programs, both in house and federal utilized to train members to recognize

various weapons of mass destruction (WMD), their components and WMD labs. The information in these programs is based on the most current intelligence available.

2. Protection

Protection is defined as protecting our population and infrastructure against potential threats and hazards in a way that allows our nation to prosper (DHS, 2011a, pp. 6–9). The 11 protection core capabilities are:

1. Planning
2. Public Information and warning
3. Operational coordination
4. Access control and identity verification
5. Cybersecurity
6. Intelligence and information sharing
7. Interdiction and disruption
8. Physical protective measures
9. Risk management for protection programs and activities
10. Screening, search, and detection
11. Supply chain integrity and security (DHS, 2011a, pp. 6–9)

One example of FDNY fulfilling its protection mission is another program initiated in response to intelligence provided to the FS regarding the potential for a nuclear or radiological attack. The FDNY is currently "working with the NYC Department of Health and Mental Hygiene (DOHMH) to collect and share radiological data during radiation emergencies for use in geographic information systems (GIS) analysis" (FDNY, 2011, p. 19).

Another example is found in the missions of some branches of the FDNY's CTDP. One of the missions of the CTDP is to participate in planning for varying terrorist threats as identified through their intelligence branch. This planning culminates in emergency response plans (ERPs). ERPs are than released and become part of FDNY's SOPs, providing the appropriate tactics and background information to be utilized in the response to a terrorist incident. Some of these plans cover: hazardous materials releases;

chemical attacks in subways; biological, radiological and nuclear responses; collapse rescue; under-river tunnel operations; operations at explosive or incendiary incidents; and responding to an active shooter incident (FDNY, 2011, p. 12). The ability of the FDNY to respond to these as well as other incidents is often put to the test by the CTDP exercise design team. Exercises conducted by the team range from simple intra-/inter-agency tabletop exercises to full-scale, multi-agency exercises. The principal purpose of conducting such exercises is to evaluate the ability of the FDNY and participating agencies to respond to specific types of terrorist attacks (FDNY, 2011, p. 13).

3. Mitigation

Mitigation is defined as decreasing the forfeiture of life and infrastructure by reducing the consequences of potential hazards (DHS, 2011a, pp. 9–11). The seven core capabilities involved in mitigation are:

1. Planning
2. Public information and warning
3. Operational coordination
4. Community resilience
5. Long-term vulnerability reduction
6. Risk and disaster resilience assessment
7. Threats and hazard identification (DHS, 2011a, pp. 9–11)

In order to carry out its mitigation effectively, the FDNY determined that it would have to understand the potential threats it could encounter, these could only be understood through a proper risk assessment (FDNY, 2011, p. 20), much like a local version of the SNRA. To do this, FDNY utilizes the Risk Assessment and Target Hazard (RATH) Unit. This unit accomplishes the goals set forth in the *National Infrastructure Protection Plan* (NIPP) (DHS, 2009c). The RATH Unit gathers information on NYC's critical infrastructure and key resources identifying target hazards, prioritizing preparedness efforts and developing tactical response plans for specific structures. One specific example of this is found in a combined effort between the RATH Unit, the Army Corps of Engineers, and the Department of Transportation. In response to terrorist threats toward the bridges of NYC this effort produced the bridge operations guides. These

guides can be utilized to evaluate the structural integrity of bridges damaged in a terrorist attack. One version of this is carried on all FDNY apparatuses tasked with emergency response and a more in depth version is kept locked in the Fire Department Operations Center (FDOC) (the FDNY's Emergency Operations Center [EOC]) (FDNY, 2007b, p. 21).

4. Response

Response is defined as timely actions performed to protect lives and infrastructure, and provide the necessities to those affected by the event (DHS, 2011a, pp. 11–15). The 14 response core capabilities are:

1. Planning
2. Public information and warning
3. Operational coordination
4. Critical transportation
5. Environmental response/health and safety
6. Fatality management services
7. Infrastructure systems
8. Mass care services
9. Mass search and rescue operations
10. On-scene security and protection
11. Operational communications
12. Public and private services and resources
13. Public health and medical services
14. Situational assessment (DHS, 2011a, pp. 11–15)

In the majority of the areas of response described in the *National Planning Scenarios* (DHS, 2005b), the FDNY would move to the forefront of operations in the event of a catastrophic incident. Intelligence in the time leading up to the incident, during the incident, and following the incident is crucial. In the time leading up to an attack, the intelligence provided informs our planning and then our SOP's. It will also be crucial for the research and development, and finally the acquisition of equipment. Finally, it will be used for the purpose of curriculum development, training, and finally exercise

development. A specific example of this is the response of the FDNY to the possibility of a chemical attack on the subway system. FDNY developed SOPs and the ERP, entitled *Suspected Chemical Attack in an Underground Transit System* (FDNY, 2004).

The nature of the threat established the need for additional personal protective equipment (PPE). This consisted of such items as: chemical protective clothes, and rebreather masks. Rebreather masks are breathing apparatus capable of supplying hours of breathing air as opposed to the minutes supplied by most firefighting self-contained breathing apparatus (SCBA). In addition, rebreather units were formed not only to maintain this specialized equipment but also to assemble it and deliver it to the site of an attack. FDNY SOC established a training and recertification program for all of the personnel involved. All of this has culminated in several large scale multi-agency exercises. Items such as these required extensive research, development, and testing. Numerous units throughout the FDNY have been designated as special units and become part of the plan for a tiered response to an attack.

5. Recovery

Recovery focuses on the "timely restoration, strengthening, and revitalization of infrastructure; housing; and a sustainable economy; as well as the health, social, cultural, historic, and environmental fabric of communities affected by a catastrophic incident" (DHS, 2011a, p. 15).

The eight recovery core capabilities are:

1. Planning
2. Public information and warning
3. Operational coordination
4. Economic recovery
5. Health and social services
6. Housing
7. Infrastructure systems
8. Natural and cultural resources (DHS, 2011a, pp. 15–18)

With regard to specialized capabilities that intelligence has identified as important, FDNY addressed two major issues, implementing the principals of a tiered response and decentralization. One of the key principals of the *National Response Framework*, on a national level a tiered response, suggests that catastrophic events are best handled locally with additional layers of government assistance (e.g., state or federal) added only as required (DHS, 2014, pp. 5–6). FDNY utilizes this principle to assign units that possess the appropriate level of training and equipment for the mission at hand. In the past, only the special operations units had the training and equipment for many of the disciplines required to respond to various terrorist attacks. Now, other units receive the appropriate levels of training to respond to specific aspects of this type of operation.

Decentralization is a principle that spreads out capabilities that are unique but that could prove essential. This can be crucial in the event of these capabilities being lost as a result of the attack or isolation of capabilities through the loss of infrastructure, such as bridges and tunnels—both of which have been reported as potential targets. In regard to the five mission areas defined in PPD-8, the FDNY has demonstrated that it has a significant role in fulfilling the NPG as well as the ability to utilize intelligence to fulfill this role (DHS, 2014, p. 1).

B. THE FDNY'S ROLE IN THE VARIOUS FORMS OF TERRORIST ATTACK

To determine the intelligence requirements of FDNY, its role in the five mission areas has been established. In this section, the fictionalized accounts of terrorist attacks that were developed as training scenarios in the NPS and NPS: AT are analyzed to determine what the role of FDNY is in response to the various forms of terrorist attacks. To aid in this goal, this thesis includes an analysis of real attacks, both attempted and successful, upon the nation since September 11, 2001, pertinent trending attack patterns around the world, and some modes of attack that were assessed in the SNRA but not developed into scenarios in the NPS and NPS: AT.

The NPS consists of 15 all-hazard scenarios for use in homeland security preparedness activities. The NPS: AT (also known as attack prequels) are an addition to the NPS. These scenarios are used by all levels of government in planning for potential terrorist attacks and natural disasters. In the NPS, the scenario begins from the time of the attack and is intended to aid in planning the response phase. In contrast, the scenarios in the NPS: AT begin with the conception of the attack and end with the culmination of the attack. The prequels offer the scenario leading up to each of the terrorist attacks listed in the NPS (DHS, 2006b, pp. ii–iii).

The objective in developing these scenarios was to establish scenarios that were able to assist with both the development and the testing of the various capabilities required to fulfill the homeland security mission. Twelve of the scenarios represent terrorist attacks, and three represent naturally occurring events. For each of the 12 terrorism-related national planning scenarios, FEMA partnered with I&A and other IC and LE experts for their development (DHS, 2006b).

The 15 national planning scenarios are:

- Scenario 1: Nuclear Detonation—improvised nuclear device
- Scenario 2: Biological Attack—aerosol anthrax
- Scenario 3: Biological Disease Outbreak—pandemic influenza
- Scenario 4: Biological Attack—plague
- Scenario 5: Chemical Attack—blister agent
- Scenario 6: Chemical Attack—toxic industrial chemicals
- Scenario 7: Chemical Attack—nerve agent
- Scenario 8: Chemical Attack—chlorine tank explosion
- Scenario 9: Natural Disaster—major earthquake
- Scenario 10: Natural Disaster—major hurricane
- Scenario 11: Radiological Attack—radiological dispersal device
- Scenario 12: Explosives Attack—bombing using improvised explosive device
- Scenario 13: Biological Attack—food contamination
- Scenario 14: Biological Attack—foreign animal disease
- Scenario 15: Cyber Attack

To support the analysis of the NPS, I used reports from the Heritage Foundation as an up to date representation of terrorist plots and attacks against the homeland since

9/1/2001. The main report utilized is *60 Terrorist Plots Since 9/11: Continued Lessons in Domestic Counterterrorism* (Zuckerman et al., 2013). This report reviews the first 60 terrorist attacks that have been attempted within the U.S. since September 11, 2001. Additionally, the Heritage Foundation has published several other reports updating the initial report, including *67 Islamist Terrorist Plots Since 9/11: Spike in Plots Inspired by Terrorist Groups, Unrest in Middle East* (Inserra & Phillips, 2015) and several reports of individual attacks, the most recent of which is regarding the 73rd terrorist plot against the U.S. homeland.

The intent of the NPS is to establish the minimum number of scenarios required to develop and test the various mission areas. In order to accomplish this, NPS did not cover or covered only superficially several scenarios that were addressed in the SNRA. A scenario with significant homeland security implications that was not addressed in either was an EMP attack. However, the SNRA did cover space weather, which for the purposes of the FS is very similar to an EMP. In addition, while cyber-attacks were covered in the NPS, the SNRA elaborates on this by adding the classification of cyber-attacks against physical infrastructure, which would have greater consequences for the FS.

Finally, I assessed some of the large-scale attacks that have occurred around the globe that are considered by FDNY to be of exceptional significance and to represent a new tactic. These included: the 2008 attack on Mumbai, the 2013 attack on the Westgate Shopping Mall in Nairobi, Kenya, and the 2015 attacks in Paris and San Bernardino. The FDNY classifies attacks of this type as Mumbai-style attacks. According to the FDNY, some of the characteristics of this type of attack include: multiple attackers that are mobile, multiple targets, and combined weapons, including active shooters and fire and/or explosives (CTDP, 2009). I conclude that in every type of attack examined, a significant response of the FDNY would be required.

V. INTELLIGENCE POTENTIALLY AVAILABLE TO FDNY

In the previous chapter as the first step toward determining the intelligence requirements of FDNY, the possible missions of FDNY in regard to national preparedness and its role in response to various forms of terrorist attacks was determined. In this chapter, the NPS: AT is assessed for the intelligence that could be available in the time leading up to a terrorist attack. To accomplish this, the attack timelines (or prequels) are compared to the stages of the terrorist attack planning cycle. In addition, intelligence that is not specified in the terrorist attack planning cycle, but that has been shown to be available in accounts of terrorist plots against the homeland, is examined.

Due to the large amount of information contained in the NPS: AT pertaining to the various forms of attack, I decided to examine all the scenarios but to focus primarily on explosive attacks and secondarily on chemical attacks when establishing the intelligence requirements. I chose explosive attacks because they are by far the most predominant form of attack. According to the National Consortium for the Study of Terrorism and Responses to Terrorism (START), in 2014, bombings accounted for 54 percent of the tactics used in terrorist attacks worldwide. This was more than all of the other tactics combined. In addition, in a report focusing on terrorist attacks in NYC occurring between 1970 and 2007, START found that in 70 percent of the attacks bombs were the primary weapon. Chemical attacks were chosen because they could be considered representative of a majority of the remainder of attack scenarios in regard to the emergency response tactics. Of the 11 terrorism scenarios remaining after examining explosive attacks, four scenarios are chemical. From the perspective of an emergency responder, these can have many similarities to biological attacks (i.e., similar dispersal problems), which account for another four of the scenarios. I thought that examining these attacks would provide a good framework to build on (National Consortium for the Study of Terrorism and Responses to Terrorism [START], 2010, p. 4; 2015).

To determine the intelligence that could potentially be available for the prevention mission, information that was available in the time leading up to an attack was assessed against a concept known as the terrorist attack planning cycle. Within the military, the

LEC, and FDNY, a large body of information has been put forth to educate emergency responders and others in the stages of preparation that led up to a terrorist attack. Some refer to these stages as the terrorist attack cycle or the terrorist planning cycle. The terminology utilized here, referring to the phases preceding a terrorist attack as the terrorist attack planning cycle, was put forth by DHS and adopted by FDNY.

Some examples of this information is found in documents such as *A Military Guide to Terrorism in the Twenty-First Century*, which has an entire appendix devoted to the terrorist planning cycle (U.S. Army Training and Doctrine Command, 2007). Another example is the surveillance awareness course (IS-914: *Surveillance Awareness: What You Can Do*) offered by the FEMA Emergency Management Institute. This course is intended to enable participants to detect potential adversarial surveillance incidents. Strategic Forecasting Inc. (Stratfor) in the Fundamentals of Terrorism section of its publication *Security Weekly* put out several articles on detecting the terrorist attack planning cycle. The most pertinent of these for the purpose of my research was "Detection Points in the Terrorist Attack Cycle" (Stewart, 2012). The Regional Organized Crime Information Center (ROCIC) published *Indicators of Terrorist Activity, Stopping the Next Attack in the Planning Stages* (2004). In addition to general information on the intelligence gathering and surveillance phases, this publication actually lists specific indicators of various means of attack, such as suicide bombings and kidnappings.

Some of these examples concentrated on the overall cycle and some, such as in the surveillance awareness course, on specific aspects of the cycle. Although all of these examples offer some variations on the theme, the terrorist attack planning cycle put out by DHS is typical and consists of:

- Broad target consideration
- Specific target selection
- Pre-attack surveillance
- Attack rehearsal
- Training
- Intelligence gathering and surveillance

The planning cycle does not necessarily consist of all of these phases, and the sequence and timing can vary greatly. However, some of the phases are often recognizable such as surveillance, training, and rehearsals. The potential for discovery and recognition can offer an opportunity to disrupt the cycle and hence prevent the attack from occurring (DHS and DOJ, 2010).

Initially, I compared the terrorist attack planning cycle to events in the various scenarios in the NPS: AT. The comparison was than focused on each individual phase of the terrorist attack cycle as compared to NPS: AT, *Scenario 12—Explosives Attack—Bombing Using Improvised Explosive Devices* (DHS, 2006b). This was done for the sake of brevity, but my initial examination of the other scenarios yielded similar results. The comparison of each phase of the cycle to scenario 12 follows:

- Broad target consideration—The initial target selection is of a target that meets group's primary strategic goals, which consist of: a high death toll and a target of symbolic value.
- Specific target selection—The specific target selected is a sports stadium. The primary target is later expanded to include several secondary targets, such as an underground subway station near the stadium, first responders, the stadiums parking lot, and a nearby hospital.
- Pre-attack surveillance—Some of initial pre-attack surveillance included the purchasing of: a digital video camera, a laptop, and a photo printer. The first step is filming around the stadium to gather information on potential secondary targets, this is followed up by attendance at a sporting event to observe the stadium in operation, and this leads them to follow the crowd leading the stadium to a nearby subway station, which becomes a secondary target.
- Attack rehearsal—A rehearsal involving all the participants is conducted the night of a basketball game. The suicide bombers attend the game and occupy the area where they will detonate. The other members either park their vehicle borne improvised explosive devices (VBIEDs) or place their improvised explosive devices (IEDs) and proceed to locations from where they will detonate the devices.
- Training—The three terrorists that are tasked with the suicide bombing portion of the operation are tested. They are instructed to carry various small illegal items, such as drugs and weapons, into areas such as semi-secure public facilities. In addition, other members conduct a test run of small scale versions of the various explosive devices.

- Intelligence gathering and surveillance—Other surveillance and intelligence gathering include: gathering open source intelligence from the stadium website, further surveillance of the parking facilities to determine optimal explosives placement, and photographing an official stadium parking pass for replication. (DHS, 2006b, pp. 12-2 – 12-7)

While the information available in the scenarios of the NPS: AT fit in well with the terrorist attack planning cycle, there was an important body of information potentially available that was not specifically mentioned. The examination of the data pertaining to the numerous terrorist plots against the homeland, including information on how they were prevented, revealed a stage of preparation for the attacks that is not explicitly covered in the terrorist attack planning cycle. This stage involves the acquisition of weapons and other materials crucial to carrying out an attack, materials such as vehicles and identification. This is very often the stage where attacks are disrupted. To facilitate this disruption, recognition of the materials and techniques utilized to construct various WMDs is a part of the training of many emergency response personnel. This acquisition stage is an integral part of the scenarios in the NPS: AT. Many of the 67 terrorist plots against the U.S., analyzed in a report by the Heritage Foundation (Inserra & Phillips, 2015) were broken up during the weapons acquisition phase. One example is the arrest of a man who later pled guilty to a 2009 plot to bomb the NYC subway system. He was arrested after purchasing a large amount of chemicals used in the making of triacetone triperoxide (TATP) bombs. Moreover, there are numerous other cases of individuals arrested after purchasing such items as chemicals, explosives and firearms (Heritage Foundation, 2013, p. 9). This phase was also evident in the other national planning scenarios, including the bombing scenario. The terrorists in this scenario had to procure numerous items such as C4, chemicals for improvised explosives, bomb components (e.g., blasting caps), false documentation, vehicles (including an ambulance), and safe houses (DHS, 2006b, pp. 12-4–12-5).

The examination of: various categories of terrorist attacks, actual terrorist plots, and the terrorist attack planning cycle showed that there is a very solid body of knowledge pertaining to how terrorists carry out attacks and hence the information for

which the IC is searching. This is the information that is required for the prevention mission.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. ANALYSIS

In Chapter VI, the five preparedness missions were examined, and the conclusion is that FDNY has the potential for involvement in all five mission areas. In addition, I examined FDNY's role in relation to the various forms of terrorist attacks. This examination indicates that in addition to having a role in all of the preparedness missions, the FDNY would have a role in all of the forms of terrorist attacks. I also examined specific examples of FDNY's utilization of intelligence to respond to its roll in each mission area were also examined. In analyzing FDNY's role in each of the mission areas and the intelligence required to fulfill that role, I broke down the intelligence requirements into those required for the prevention mission and those required for the response mission. In the prevention mission, FDNY's primary roll would be one of a potential intelligence gatherer for the IC and LEC and as such would require information pertaining to what attack indicators they should be alert for. In the other mission areas, I determined that the intelligence that would be required by FDNY for its role in the response mission would also apply to the protection, mitigation, and recovery missions.

In Chapter VII, the NPS: AT was assessed regarding its relationship to the terrorist attack planning cycle. The applicability of this assessment is enhanced by the inclusion of an analysis of actual planned terrorist attacks against the nation. I determined that much of the framework for understanding the intelligence that would be available and of importance to FDNY in regard to the prevention mission already exists. In examining the five mission areas, the intelligence needs of FDNY can be represented by stating the requirements for the two mission areas of prevention and response.

A. THE PREVENTION MISSION

Analysis shows that the ability of the IC to provide intelligence for the prevention mission is well established. This is largely due to the existing prevention bias in both the IC and the LEC. This prevention bias is understandable as the primary concern of these communities is the prevention mission and this is the mission area they work in on a daily basis.

In addition, there are several other reasons that the IC is well equipped to provide intelligence for the FS to utilize in the prevention mission. One reason is that the majority of intelligence that is required for the prevention mission is the same no matter who is trying to accomplish it, whether it is the FS or more traditional consumers of intelligence, which in FDNY's area of operations would generally be LE. A substantial amount of this intelligence is covered by the extensive work that has been done on the terrorist attack planning cycle and its variants. This information is widely utilized throughout the emergency response community and also employed to some extent by the private sector. Furthermore, there is a large volume of intelligence provided to emergency responders through training conducted throughout the emergency response community regarding WMDs. This training does not just pertain to the response to such attacks but also to the recognition of the components and fabrication processes of such weapons. In addition to numerous in house programs and onsite training, the FDNY utilizes WMD schools throughout the country, including the Center for Domestic Preparedness in Anniston, Alabama; the Energetic Materials Research and Testing Center in Socorro, New Mexico; the Center for Radiological and Nuclear Training at the Nevada National Security Site; and Dugway Proving Ground in Utah.

The other main reason that the IC is well equipped to provide intelligence for the FS to utilize in the prevention mission is that in carrying out the prevention mission, the FS is really providing intelligence to the IC. The prevention mission of the FS is widely recognized by the IC to consist of its ability to act as intelligence gatherers. This is based on the ability of the FS to enter numerous structures on a daily basis and even to carry monitoring equipment on these entries. What this means is that the intelligence the IC provides to the FS, in the case of a prevention mission, relates directly to the intelligence that the IC requires for the prevention mission.

In general, most of the intelligence required by LE for the prevention of a terrorist attack would be appropriate for the FS. An important exception would be the intelligence that the FS does not need. An example is sensitive information such as the sources and methods of intelligence acquisition, which, while important to the LEC, would generally

be inconsequential to the FS. The criteria that is important for the FS to evaluate intelligence is its credibility and reliability.

B. THE RESPONSE MISSION

While the LEC and the IC focus on the prevention mission, the response mission is the area where the FS will have its most extensive role. While the ideal is to prevent terrorist attacks, history has repeatedly shown us that this will not always be possible. According to the *National Strategy for Counterterrorism*:

> At the same time, we recognize that no nation, no matter how powerful, can prevent every threat from coming to fruition. That is why we are focused on building a culture of resilience able to prevent, respond to, or recover fully from any potential act of terror directed at the United States. (U.S. Executive Office of President, 2011, p. 5)

Further highlighting the IC's prioritization of the prevention mission is that of the core goals that are defined in the NPG; intelligence and information sharing are only components of the prevention and protection missions. This corroborates the necessity to provide the IC with the intelligence requirements of the FS for the response mission.

To establish the intelligence required by the FS in the response mission, I conducted an analysis of the information that is gathered and utilized by the FS at emergency operations on a daily basis. This gathering process is known as conducting a size-up. In the FS, COAL WAS WEALTH is an acronym that is often taught as a mnemonic device to aid FFs to conduct a size up at a fire or other emergency operation. While there are several other popular methods, they are all very similar. The mnemonic COAL WAS WEALTH was chosen for this research because it is the one utilized by FDNY. However, one change to the mnemonic was introduced by Deputy Assistant Chief John Norman Chief, a retired member of FDNY, who was placed in charge of FDNY Special Operations Command (SOC) in the aftermath of the 9/11 attacks. In his book the *Fire Officer's Handbook of Tactics*, he made a change that is particularly pertinent when conducting a size-up of terrorist attacks that is included here (Norman, 2012). As taught by FDNY, COAL WAS WEALTH stands for:

COAL WAS WEALTH

- Construction
- Occupancy
- Auxiliary appliances
- Life
- Weather
- Apparatus and equipment
- Street conditions
- Water supply
- Exposures
- Area
- Location
- Time
- Height (FDNY, 2013b, pp. 3–4)

In the *Fire Officer's Handbook of Tactics*, area is combined with height, allowing the final H to be designated as hazardous materials. With this modification, COAL WAS WEALTH stands for:

- Construction
- Occupancy
- Auxiliary appliances
- Life
- Weather
- Apparatus and equipment
- Street conditions
- Water supply
- Exposures
- Area and height
- Location
- Time
- Hazardous materials (Norman, 2012, pp.10–11)

While the primary design of this size-up format and others like it is to assess a building fire, they are regularly utilized to assess fires in other structures such as ships and planes, and during other emergencies such as collapses. The intelligence provided through performing this assessment can be utilized in many emergencies including terrorist attacks. This may require minor substitutions to points of the size-up but these substitutions are simple once the principles are understood. As an example the categories of: construction (the method and material by and of which a building is built) and occupancy (what a building is utilized for) could both be explained by intelligence stating that the terrorist attack is in a subway.

When conducting an assessment utilizing this 13-point size-up, it is important to note that many points when examined can provide information on other points. Some examples would be: time can be an indicator of the life hazard (e.g., an apartment build at 3 AM can be expected to contain numerous sleeping occupants); occupancy can be an indicator of the presence of hazardous materials (e.g., an occupancy involved in plastics manufacturing can produce plastic dust which is explosive); and construction can be an indicator of the auxiliary appliances that are present (e.g., many buildings of type 1 construction have standpipe systems).

The following list is an explanation of each point of the 13-point (COAL WAS WEALTH) size-up, along with examples of their standard applications during fires and their potential applications during a terrorist attack.

1. Construction

Generally the FS utilizes the National Fire Protection Association's (NFPA's) method of classifying construction types, dividing building construction into five categories: type 1 (fire resistive), type 2 (noncombustible), type 3 (ordinary), type 4 (heavy timber), and type 5 (wood framed). Every type of building construction has different firefighting and emergency operations SOPs associated with it. This is due to such factors as how fire affects a structure, how fire and smoke spread, the collapse dangers of a building along with likely collapse patterns, and even information such as the building's vulnerability to a terrorist attack with a chemical weapon (or other

hazardous materials release) as well as a building's heating ventilating and air conditioning (HVAC) system used to disperse a WMD.

a. Type 1 Construction—Fire Resistive

Fire resistive buildings, the most common of which are known as "high-rises," are more than 75 feet tall and are constructed of concrete and fire protected steel. These structures generally limit the spread of fire and are resistant to collapse during usual fire conditions. Important features found in this type of construction can include a HVAC system, the components of which penetrate the structures fire resistive barriers, and other auxiliary appliances, such as standpipe systems that provide water for firefighting. The HVAC system can not only spread the products of combustion and other hazardous materials, it can also be used to contain and control the spread.

b. Type 2 Construction—Noncombustible

The structural elements in noncombustible construction, while they are noncombustible, they do not have the fire-resistive rating of type 1 construction. Type 2 buildings are most often made of steel and can include structures such as warehouses and schools. Since these structures are constructed with noncombustible materials the fireload is determined by the contents. Since these structures are not constructed with fire-resistive materials, they are prone to collapse under fire conditions.

c. Type 3 Construction—Ordinary

Ordinary construction, also known as "brick and joist" construction, is commonly made with non-combustible masonry walls and a wood roof and floors. This type of structure can have hidden areas where fire can spread, such as in separate but adjoining structures that have a common cockloft (attic).

d. Type 4 Construction—Heavy Timber

Heavy timber construction has masonry exterior walls that are load bearing. Interior structural members are of wood and to meet the type 4 criteria must be of

sufficient dimensions. Some common uses of this type of structure are found in commercial applications such as manufacturing or a warehouse.

e. Type 5 Construction—Wood Framed

Wood frame construction is very common and is generally utilized in the construction of private dwellings as well as other structures. This type 5 construction is found in many modern homes.

This system of classifying structures into five types is just a guideline as not every structure will fit perfectly into a given category. However, using the knowledge of construction put forth here enable an assessment of a structures strengths and weaknesses.

An emergency or attack upon something other than a building could also be covered by the construction point of the 13-point size-up. Some example would be attacks on: planes, trains, bridges or a subway system. This can also be applied to the next point, occupancy.

2. Occupancy

There are many categories of occupancy, such as is the structure residential or commercial; however, basically occupancy means, “what is the structure used for?” This can be an indicator of many things such as the life hazard. An apartment building would probably have a greater life hazard than a storage facility, and an assisted living facility would probably have a greater life hazard than an apartment building. The type of occupancy can also indicate a structure collapse potential. A structure that is subjected to the load of heavy equipment is generally a greater collapse hazard. It can also be an indicator of the structures potential as a terrorist target. Is the structure of historical significance? Is it a government building? Is the structure a chemical facility producing a chemical such as chlorine gas? All of these factors could increase a structures potential as a terrorist target.

3. Auxiliary Appliances

The main items that the FS is concerned with when referring to auxiliary appliances are standpipe and sprinkler systems; as well as other specialized fire suppression systems, such as halon, foam, or dry chemical. Standpipe systems are what the FS utilizes to provide it with water for firefighting operations. Sprinklers and other fire suppression systems can also aid in firefighting efforts. In addition, auxiliary appliances can also refer to various detection systems, such as smoke, chemical, carbon dioxide, or heat detectors. Many of these systems could become damaged secondary to an attack. For instance, the pipes supplying water to a standpipe system in a high rise building could be damaged by an explosion. This would make getting water on a fire on the 80th floor difficult. These systems themselves are also potential targets, which if successfully targeted, could take away the ability of the FS to both detect and respond to hazardous conditions.

4. Life

Life hazard is always the primary concern in any emergency. Some factors to take into consideration when assessing the life hazard are: how many people are in danger, what is their location (will removal be difficult such as in a subway system), and what is their physical condition? The occupant's condition could be an existing one, such as when responding to a hospital, or it could be secondary to the situation, such as incapacitation due to a chemical release. Life hazard does not just have to be those that are present at the target of the attack. The life hazard can also be the emergency responders, such as in the case of a secondary attack. Finally, the degree of the life hazard itself can also affect a structure's desirability as a terrorist target.

5. Weather

There are numerous weather conditions to consider. Temperature extremes of both hot and cold can be debilitating to operating personnel. In addition, snow and ice can hinder both response and operations. Temperature can play a major role in the effectiveness of a chemical attack (e.g., mustards have a low volatility at low temperatures but develop a major vapor hazard at high temperatures). Moreover,

temperature is also a major consideration in any hazardous material release as is the wind. Wind can also have a major effect on the spread of fire in both an urban and a wilderness environment. Forest fires have become a means of terrorist attack recommended by *Inspire* magazine. These can be affected by both dry weather and wind.

6. Apparatus, Equipment, and Personnel

The apparatus, equipment, and personnel needs are dictated by the incident. In times of elevated terrorist threats, manpower can be increased and/or reallocated, and specialized equipment and apparatus can be prepared and manned. Which personnel and equipment are activated could possibly be dictated by available intelligence. In 2004, the author was assigned for several months as an officer in Rescue 6, a rescue company that was set up on a temporary basis by the FDNY to deal with an elevated terrorist threat in a high risk area.

7. Street Conditions

This section refers to more than just street conditions, it refers to anything affecting the avenue of access to the area of operations, including any terrain or water features. An example would be a scenario requiring a response via fireboat. This can also be a result of weather conditions, such as heavy snowfalls. The means of access is a potential target for a terrorist attack—an example of which would be using vehicles to block out responders.

While in firefighting operations "street conditions" generally refers to the streets adjacent to the area of operations, with regard to terrorism, this should be expanded to include access and egress to and from the entire affected area. Additionally, it should include considerations for the access of various specialized units and equipment that could be required. As an example, in the time since 9/11, there have been several potential terrorist threats to the bridges of NYC. In response to these threats, the FDNY sought to develop a standalone capability for each of the five boroughs. This involves a certain level of duplication of certain classifications of units as well as equipment. This policy is intended to allow an area that is isolated by a terrorist act, such as the

destruction of a bridge or a tunnel, to have the resources to respond to the various types of potential attacks.

8. Water Supply

Water supply includes the availability of fire hydrants, bodies of water to pump out of, or any other initial water source. It can also include the apparatus necessary to pump and otherwise transport the water. For FDNY, this can include fire engines, fire boats to pump water, satellite units consisting of high capacity pumpers, and hose wagons to lay various large diameter and specialized hose line through which to pump water. In addition, water supply can include buildings systems, such as standpipes, sprinklers, and pumps. Establishing or maintaining an adequate water supply in the aftermath of an attack has long been a topic of concern for FDNY. This concern dates back to a time when members of FDNY were assigned to the London Fire Brigade during World War II to observe the tactics that London FFs had established to respond to the bombings of London. Interrupting the water supply at any link in the supply chain has the potential to prove disastrous in regard to firefighting and other emergency operations. This interruption could be secondary to an attack that involves as explosion or collapse that damages supply lines, or it could be the main focus of the attack, such as removing supply lines in a high rise buildings standpipe system to deny water to fight a fire on the 86th floor. Water is also a critical component of other emergency operations, such as gross decontamination operations in response to a chemical attack. Due to its great importance, the FDNY has many contingency plans to supply water in various situations such as using a hose wagon from a satellite unit to lay large diameter hose line to be used as a replacement for damaged water mains. This hose can be supplied from a fireboat, with access to a limitless supply of water, which pumps at a capacity of 50,000 GPM (standard FDNY engines pump at 1,000 GPM with some specialized engines pumping at 2,000 GPM).

9. Exposures

When referred to in relation to fire operations, exposures are generally referencing adjoining buildings or areas adjoining the fire area within the fire building. Among other

things, exposures are the areas that are susceptible to the spread of fire and toxic gases, resulting in a life hazard. Exposures can also be susceptible to collapse if the fire building collapses. In relation to emergency operations in general, exposures can be thought of as any area that can be affected by or affect the area of operations. As in collapse operations, this refers to the six sides of the collapse area: left, right, front, back, above, and below. In the event of a chemical attack, this could include the area expected to be engulfed by the plume, or in a chemical attack in a high-rise, an immediate exposure problem would be areas serviced by the same HVAC system. In regard to a pandemic, exposure considerations can be national and international. Finally, exposures are not just problematic, they can be useful for such purposes as providing access to the area of operations to emergency responders and egress for victim removal.

10. Area and Height

Most commonly in the urban FS, area and height refers to the area of the building or occupancy. However, in reference to response to terrorist attacks, these could refer to a much larger area, such as an intentionally set forest fire or a large scale chemical release. It can also refer to an even larger area such as a biological attack spreading throughout the country. In the aforementioned examples of buildings or occupancies, the area and height can be indicators of the numbers of victims and the difficulty of evacuation. These factors can also dictate tactics due to equipment limitations, such as the length of aerial ladders used by the FS for access and egress, or by established SOPs, such as the common practice in the FS of utilizing standpipe systems to provide access to water for firefighting in structures, such as high-rise buildings, bridges, and stadiums.

11. Location and Extent of Fire (or Incident)

In fire operations, depending on the type of structure, the location of the fire indicates such important factors as where the fire could spread to and the potential for collapse. In addition, much like during 9/11, areas above the fire area can become isolated, and if these areas are out of reach of fire department ladders the opportunities for victim removal are limited. At incidents in remote areas like the upper floors of a high-rise, removal can be problematic, even if the area does not become isolated, due to

the excessive distances involved. Attacks upon the means of egress, such as the elevators, can exacerbate these difficulties. This isolation can also take place during other types of attack, such as a chemical release. Another example would be an incident occurring below grade. In these incidents, venting toxic gases whether they are from fire or from a chemical attack can be very difficult. In addition, some potential weapons such as chlorine gas were designed with below grade attacks in mind. Chlorine gas is 2.5 times heavier than air and was used in trench warfare in World War I for its ability to travel along the ground and fill up the trenches. The FDNY has done much preparation for chemical attacks on the subway system with weapons like this in mind.

12. Time

Time of day along with the type of occupancy will generally dictate the life hazard. For example, during a fire at 3 AM, a multiple dwelling can be assumed to contain many sleeping occupants, as opposed to a fire at the same time in a factory. A factory at that time may well be closed for business and contain no life hazard. Time also takes into consideration the day of the week that an incident occurred on as well as anything else notable in regard to the date. On a Sunday, a grade school may be closed as opposed to on a weekday. Holidays must be taken into consideration both for estimating the life hazard present and for the symbolism they represent for terrorists planning an attack. When responding to an incident, the amount of time that has passed since the incident occurred must be taken into consideration. This is important in determining, such items as the stability of a structure exposed to long periods of fire or the viability of victims buried in a collapse or exposed to chemical weapons.

13. Hazardous Materials

The presence of hazardous materials is always a consideration when responding to an emergency situation. Fires, flooding, auto accidents and collapses are just a few examples of emergencies that can result in the release of hazardous materials. In the case of a terrorist attack the release of hazardous materials can be the main goal of the attack as in a chemical attack, a component of the attack as in a dirty bomb, or secondary to the primary attack as in a chemical release caused by an explosion. In addition this is the

category in which the type of attack can be covered be it chemical, fire, explosive or active shooter.

Many components or the 13-point size-up will tie together and overlap. As an example the time section can indicate different life hazards. One example is a mall at three in the afternoon has a different life than the same mall at three in the morning. Another example would be on a Monday afternoon a school may have a greater life hazard than a church; however, this could switch at the same time on a Sunday. Additionally, on another Monday in that same school and church the church could still be the greater hazard if that Monday happened to fall on December 25. Yet another example is how the type of occupancy can indicate the presence of certain hazardous materials.

Intelligence that is provided utilizing this 13-point size up would not only be useful in responding to a terrorist attack, it could also be used by the FS in the protection, mitigation, and recovery missions. Some examples of scenarios in which intelligence has been utilized by FDNY were touched upon in the discussion of the mission of FDNY. Receiving intelligence on the hazards point of COAL WAS WEALTH caused FDNY to set up a radiological detection program the main purpose of which is to have FDNY act as sensors of opportunity by equipping department boats, vehicles, and members with radiological sensors to scan for radiation during the normal course of operations. The hazard point is also addressed with intelligence that is disseminated to FDNY members though WMD recognition programs both in house and at schools around the country. This allows them to act as sensors of opportunity for all of the categories of WMDs. Examples of the construction and occupancy portions of the size up include intelligence received on potential attacks on the subway system and the bridges. In response to potential chemical attacks on the subways, emergency response plans were drawn up, specialized protective equipment was evaluated and purchased, members were trained, exercises were conducted, and maintenance and recertification programs were instituted. In response to intelligence regarding bridges as targets FDNY teamed with outside groups such as the Army Corps of Engineers, and the Department of Transportation to develop bridge operations guides. Theses guides are distributed to field units to be utilized to evaluate the structural integrity of a bridge that is damaged in a terrorist attack.

A more in depth version is locked in the FDOC to be transported to the site of an attack as needed.

A more well-known example of a terrorist plot that FDNY received actionable intelligence on was the 2007 John F. Kennedy (JFK) International Airport plot. This was an attack that was planned mainly against the pipelines and fuel facilities that supply JFK International Airport with aviation fuel and gasoline. These pipelines are collectively known as the buckeye pipeline. The conspirators in this plot believed that the attack would cause "greater destruction than in the September 11 attacks" (Faiola, & Mufson, 2007, p. 1). In this example, FDNY CTDP and FDNY fire marshals had received briefings on the potential attack. Since this intelligence was classified and involved an ongoing investigation it was disseminated on an extremely limited basis. However this dissemination did allow for an emphasis to be placed on the training and exercise program involving the buckeye pipeline and airport operations. Training on the pipeline would generally be conducted annually in a progressively tiered training program. In addition to responding to this intelligence, FDNY staff was able to contribute to the intelligence by conducting briefings for the IC that included FBI, DHS, and NYPD. These briefings contained information on the "operational considerations regarding the critical points of the Buckeye Pipeline infrastructure and the potential damage of a ruptured pipeline" (FDNY, 2007c).

VII. CONCLUSION

In laying out the objectives for this thesis, the main goal was to find the specific intelligence that would be required by FDNY to prevent, prepare for, and respond to terrorist attacks. This was to be accompanied by identifying examples of how the requested intelligence would be utilized and further determining what intelligence is not applicable toward these missions and therefore should not be provided.

To accomplish the objective, the intent of this research was to conduct a policy analysis utilizing a policy options analysis methodology. The goal of the analysis was to identify the positive and negative aspects of each policy in terms of potential adaptability, both practically and financially, and operational impact. Utilizing the fusion center model in the analysis was ruled out because that model was not a viable option for FDNY and many other fire departments. One policy option analyzed (Option A, traditional intelligence methods) was the widely utilized policy of the FS obtaining intelligence from the local LEC. In this method, local LE passes on the intelligence it has received and deems appropriate to the local fire department. The second policy option (Option B, network fusion) analyzed is that currently in use by FDNY. The final for analysis was for the FS to obtain the intelligence necessary to carry out its mission by utilizing a standardized set of information indices that the DHS IC would be required to supply to the FS.

In order to conduct the policy analysis the first phase was to be the development of the standardized set of intelligence requirements necessary to establish the third policy. In attempting to establish these indices, several items became apparent that were to modify the objective of this thesis but not the intent. In response to this modification, a standardized set of information indices were not developed. In addition to not establishing the standardized intelligence requirements necessary for the third policy option (Option C, establishing fire service intelligence requirements), other realities became apparent that brought to question the significance of analyzing the various policies against each other.

The first item that became apparent was the relevance of the vast disparity between fire departments. On one end of the spectrum, there are small departments consisting of a dozen members who are part-time volunteers located in a rural area with no history of either a terrorist attack or the threat of one. On the other end of the spectrum are large departments, such as FDNY, which has more than 13,000 members and is located in a city with a long history of terrorist attacks. This history includes: having been the target of 284 terrorist attacks from 1970 to 2007 (START, 2010, p. 1), having been one of the targets of the largest terrorist attack in the history of the nation, and a continuing history of being a primary terrorist target. In the case of the small department in this example, the department does not have the infrastructure to handle a large volume of incoming intelligence nor is this a priority. The FDNY has more personnel assigned to the CTDP than many small fire departments have in their entirety. However, any department faces the potential of dealing with the aftermath of a terrorist attack. The rural department could respond to attacks ranging from the consequences of an active shooter incident such as the 2015 San Bernardino attacks or an intentionally set forest fire. In an incident such as San Bernardino, the awareness of intelligence, such as that regarding distribution and/or emplacement secondary devices, could be crucial.

In addition to the size of the department and the potential for terrorist attack, there can be many other considerations, such as financial and political, that dictate the method by which the FS obtains its intelligence. The FDNY itself, despite its size and history of responding to terrorist attacks, does not have a fusion center owing to political considerations. The appropriate means for acquiring intelligence for one department is not be the same for another.

An overall comparison of the policy options listed is in the matrix in Table 1.

Table 1. Policy Options Matrix

OPTIONS	COMPARATIVE COST	LEGALITY ISSUES	POLITICAL ACCEPTABILITY	COMPARATIVE LEVEL OF EFFORT	EFFECTIVENESS
OPTION A Traditional Intelligence Methods	**Minimal**	**No**	**Yes**	**Minimal**	**Minimal to Moderate**
OPTION B Network Fusion	**Moderate**	**No**	**Yes**	**Moderate**	**Good**
OPTION C Establishing Fire Service Intelligence Requirements	**Moderate**	**No**	**Yes**	**Moderate**	**Very Good**

There is a clear need for timely, actionable intelligence to enable FDNY to make appropriate tactical and strategic decisions pertaining to terrorist attacks. In order to assist the IC in providing the appropriate information and to aid those compiling the information, the hypothesis of this thesis was that a standardized set of the specific intelligence that is required should be developed, including what information is necessary and what information is not. In addition, it would offer a basic description of why it would be required and how it would be handled and disseminated. Including the explanation of why it was necessary and what should be done with it would assure the IC that the intelligence requested was necessary and that it would be safeguarded. In addition, by providing an explanation of the intelligence that is not required, the flow of information should be expedited, as much of the most sensitive information, while important to the military and LE, has no practical application for the FS.

The literature review includes the writings of several groups that were either attempting to establish a list of the specific intelligence requirements of the FS or expressed a need for this or something similar such as the Emergency Service Sector Information & Intelligence Requirements Workshop (DHS, 2009a, p. 7) and the FSIE (DHS, 2009b, p. ii).

In researching to establish this goal, it became apparent that the methodology of potential terrorist attacks and thus the possible intelligence that could become available was not only vast but highly diverse and continually evolving. This negated the possibility of naming all of the specific intelligence that would be required by the FS in a list format. Thus, I considered an alternative a principle that is often employed when training members of FDNY SOC. In recognizing the impossibility of conceiving every possible emergency that a member could be called upon to respond to, it is important to stress principles. While training may deal with a specific scenario, the principles of alleviating that situation are stressed as is their varied applications. This method could be repeated throughout the fire service and in all fire departments.

VIII. RECOMMENDATIONS

In analyzing what intelligence would be required by the FS to make effective tactical and strategic decisions, the vast amount of variables on both sides of the equation became apparent. The first side of the equation is the vast difference in fire departments in regard to manpower, resources, and their prioritization of terrorism. The other side of the equation is the large variety of terrorist attacks, weapons, targets, etc. Taking into account the excessive amount of variables as well the ever changing dynamic environment reveals that compiling a list of specific intelligence requirements is not practical.

Assembling these specific requirements was a goal of the FSIE and is similar to requirements listed in the document *Fire Service Integration for Fusion Centers* (DOJ and DHS, 2010). This goal became the starting point for this thesis; however, during the analysis portion, this turned out to be an unrealistic option. Situations and the potential intelligence that could become available are not only highly varied but also continually evolving.

The NPG points out, “The terrorist threat is dynamic and complex” (DHS, 2011a, p. 4) and that this necessitates that the goal evolve. This requires the goal to be a living document, which must be periodically revised to insure its compatibility with current policies and the dynamic terrorist threat (DHS, 2011a, p. 19). The dynamic and complex nature of the terrorist threat that is written of in the NPG negates the possibility of formulating a particular list of intelligence requirements (DHS, 2011a).

In lieu of a specific list of intelligence requirements, a better option would be to make available to the IC an understanding of the operations of the FS in regard to decision making. By providing a basic understanding of the principles behind providing the FS with intelligence, a system could be established that would remain viable even as the terrorist’s tactics continue to morph. By providing an explanation of the information that the FS utilizes to prepare for and respond to emergencies on a daily basis, an

understanding, as opposed to a stagnant list, of the intelligence needs of the FS could be established.

In addition to providing a framework for the IC to utilize to provide intelligence to the FS pertaining to the vast and ever changing variety of potential terrorist attacks, this method of providing intelligence would also provide for the vast disparity in the resources available to and the situations encountered by different fire departments. In conducting the policy analysis, the immense difference between fire departments became apparent. However, the common denominators were the potential missions of the FS and the decision-making process utilized to carry out these missions and hence the intelligence required. While departments may have vast differences, they all have similar intelligence requirements. While they may be presented with different situations and have different resources to respond with, when presented with the same situation, they require the same intelligence. This also applies to intelligence that they do not require. Too much information can prove just as problematic as insufficient intelligence as excessive intelligence can overwhelm the system.

To accomplish this, a guide for those in the intelligence and LE communities tasked with providing the FS with intelligence could be established. This guide could be written upon a format similar to that provided by a guide employed by the FS to understand the IC the third edition of the *Intelligence Guide for First Responders* by the JCAT (2015); the original was published by the ITACG the predecessors to the JCAT. These guides explain the IC and intelligence to emergency responders and provide an explanation at a level that is understandable and pertinent to members of the FS.

The guide written for fire intelligence could provide an explanation of how to obtain the intelligence requirements of the FS. In addition, it could provide a description of the type of information the FS uses on a daily basis, an explanation of the application of the information, and examples applications pertaining to the FS's response to terrorist attacks.

The system of network fusion (Option B), which is an information sharing system that encourages collaboration across multiple disciplines and currently utilized by the

FDNY to provide for its intelligence needs, could be greatly enhanced by a document that provides an understanding of its intelligence needs (Pfeifer, 2012, pp. 1–2). The information that such a document provides would assist in breaking down current barriers and biases among the FDNY's intelligence collaborators and provide for a more efficient flow of pertinent intelligence. An example of such a document, a guide for fire service intelligence, is offered in the appendix.

The importance of intelligence to the FS cannot be stressed enough. No FF would consider going into a fire or any other type of emergency without first conducting a size up. These size ups are dynamic and ongoing throughout operations. The importance of utilizing a size up to gather the information required for effective decision making is taught to new FFs as well as to fire chiefs in fire academies across the nation. This does not just apply to decisions made at the scene of an emergency. No fire chief would write any SOPs without first gathering information on the problem to be addressed; no logistician would purchase equipment without first gathering information on the problem to be addressed; and no training officer would write a new curriculum without first gathering information on the problem to be addressed. In order to prevent, prepare for, and effectively respond to terrorist attacks the FS requires timely, actionable intelligence to enable the appropriate tactical and strategic decisions to be put forth.

Developing a guide of this sort should also prove particularly advantageous toward FDNY and the network fusion concept. This is due to the large number and diversity of the intelligence sources utilized. A guide such as this would provide a common knowledge base and reference point for all involved.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX. DRAFT ANALYST GUIDE TO PROVIDING FIRE SERVICE INTELLIGENCE

TABLE OF CONTENTS

INTRODUCTION

There have been several guides written to assist the fire service and other emergency response personnel in understanding intelligence community and law enforcement intelligence reporting. This guide is modeled on a guide originally published by the Interagency Threat Assessment and Coordination Group (ITACG), *Intelligence Guide for First Responders* (2009). The most recent edition of this guide was published by the Joint Counterterrorism Assessment Team, which is the successor to the Interagency Threat Assessment and Coordination Group (Joint Counterterrorism Assessment Team [JCAT], 2015). While the intent of those guides is to provide members of the fire service and other emergency responders with the ability to understand intelligence received from the law enforcement and intelligence communities, the intent of this *Analyst Guide to Providing Fire Service Intelligence* is to provide members of the intelligence and law enforcement communities with the ability to understand and provide for the intelligence requirements of the fire service.

PURPOSE OF THIS GUIDE

This guide is intended to provide members of the Intelligence Community (IC) who are tasked with providing the fire service (FS) with intelligence with an insight into the intelligence requirements of the FS. Generally, the IC is accustomed to providing intelligence to the military and law enforcement (LE) communities. This intelligence is generally aimed at prevention and protection; however, this is insufficient for the needs of the FS. The *National Strategy for Counterterrorism* states that we must build a culture of resilience because despite our best efforts, we will not be able to prevent all terrorist attacks (U.S. Executive Office of President, 2011, p. 5).To provide insight into the type of information and intelligence required by the FS, initially I analyzed the five preparedness mission areas (prevention, protection, mitigation, response, and recovery) defined in *Presidential Policy Directive (PPD) 8: National Preparedness* (U.S. Department of Homeland Security [DHS], 2014, p. 1). This analysis was accompanied by an analysis of terrorist attacks to determine the role of the FS in national preparedness and hence the intelligence required by the FS to fulfill that role.

THE NATIONAL PREPAREDNESS MISSION OF THE FIRE SERVICE

NOTE: Throughout this guide, FDNY has been used to provide examples of the FS utilizing intelligence in its decision-making process.

Presidential Policy Directive (PPD) 8: National Preparedness was released in March 2011 with the goal of strengthening the security and resilience of the United States through systematic preparation for the threats that pose the greatest risk to the security of the nation. This directive mandated the development of a series of documents to guide the nation's tactics toward ensuring national preparedness. PPD-8 defines five preparedness missions: prevention, protection, mitigation, response, and recovery (DHS, 2014, p. 1). One of the documents called for was the *National Preparedness Goal* (NPG) (DHS, 2005a). In order to develop the NPG, the *Strategic National Risk Assessment* (SNRA) was conducted by federal agencies, DHS components, and the intelligence community, among others (DHS, 2011b). This risk assessment looked at risks that would have a major impact on the nation's homeland security. The list of risks consisted of 23 national level events divided into three categories. These categories are: adversarial/ terrorist, natural, and technological. For purposes of assessing the homeland security mission of the FS one could argue that all of the risks in the technological category and the majority of those in the natural category could be the result of terrorism. Two examples would be: wildfires, which have become a terrorist weapon, and space weather, which has similar effects to those of an electromagnetic pulse (EMP) attack. All of the events examined have the potential to warrant some level of response by the FS (DHS, 2014, p. 1).

The missions of: prevention, protection, mitigation, response, and recovery are clearly established in these documents. Each of these missions was examined in order to determine what the potential role of the FS would be in fulfilling the mission requirements. For analysis purposes, FDNY was used as a model. As part of the analysis a comparison between the FDNY Center for Terrorism and Disaster Preparedness's (CTDP) *Counterterrorism and Risk Management Strategy* (2011) and the preparedness missions was conducted. This strategy lists specific examples of the FDNY's potential role in fulfilling each of the preparedness missions. In the analysis of each of the mission

areas, examples of FDNY's use of intelligence to fulfill that mission area have been provided.

Prevention

Prevention is defined as preventing, avoiding, or stopping a threatened or an actual act of terrorism (DHS, 2011a, p. 4). The prevention mission has a unique characteristic when compared to the other missions. While all of the other missions are based on an all-hazards approach, the prevention mission is specific to terrorism. This includes those capabilities necessary to avoid, prevent, or stop a threatened or actual act of terrorism (DHS, 2011a, pp. 4–6).

An example of prevention efforts, which were initiated in response to intelligence provided to the FS regarding the potential for a nuclear or radiological attack, is the FDNY's radiological detection program. As has been observed in the prevention mission, the FS can serve as not only consumers of intelligence but also as providers of intelligence. Firefighters (FFs) can serve as sensors of opportunity during the normal course of daily operations. The effectiveness of this program is in part due to the extraordinary access afforded to the FS to numerous structures on a daily basis. According to the FDNY, during fiscal year 2014, the FDNY responded in part to 503,668 fire incidents and 1,323,198 emergency medicine services (EMS) incidents in addition to conducting 190,346 fire prevention inspections and 7,206 fire investigations (Fire Department City of New York [FDNY], 2015).

A feature of the radiological detection program is that it takes advantage of FDNY member capabilities as roving sensors of opportunity. This program is intended not only as a means of detection but also as a deterrent due to the random nature of the monitoring. As part of this program field units are required to record the normal background levels of radiation in their areas of operation. To accomplish this program sensors are deployed in three ways:

1. Personal radiological sensors are worn by the officers of field units whenever they leave quarters. This policy causes the random monitoring of any structure entered throughout the course of the tour. This monitoring can take place while conducting routine errands, performing building inspections, or responding to fires and emergencies. (FDNY, 2007a, p. 2)

2. In addition to being worn by members, radiological sensors are also deployed on the apparatus of all FDNY fire companies. These sensors are constantly monitoring the atmosphere as fire companies travel throughout the city. (FDNY, 2007a, pp. 1, 7; 2006, p. 1)

3. As well as monitoring operations on land, FDNY fireboats provide radiological monitoring while conducting routine patrols as well as during choke-point operations conducted in cooperation with law enforcement. (FDNY, 2010, p. 13)

In addition to this prevention by detection program, the FDNY also has several training programs, both in house and federal utilized to train members to recognize various weapons of mass destruction (WMD), their components and WMD labs. The information in these programs is based on the most current intelligence available.

Protection

Protection is defined as protecting our citizens, residents, visitors, and assets against the greatest threats and hazards in a manner that allows our interests, aspirations, and way of life to thrive. This includes those capabilities necessary to secure the homeland against acts of terrorism and manmade or natural disasters (DHS, 2011a, pp. 6–9).

One example of FDNY fulfilling its protection mission is another program initiated in response to intelligence provided to the FS regarding the potential for a nuclear or radiological attack. The FDNY is currently "working with the NYC Department of Health and Mental Hygiene (DOHMH) to collect and share radiological data during radiation emergencies for use in geographic information systems (GIS) analysis" (FDNY, 2011, p. 19).

Another example is found in the missions of some branches of the FDNY's CTDP. One of the missions of the CTDP is to participate in planning for varying terrorist threats as identified through their intelligence branch. This planning culminates in emergency response plans (ERPs). ERPs are than released and become part of FDNY's standard operating procedures (SOPs), providing the appropriate tactics and background information to be utilized in the response to a terrorist incident. Some of these plans cover: hazardous materials releases; chemical attacks in subways; biological, radiological

and nuclear responses; collapse rescue; under-river tunnel operations; operations at explosive or incendiary incidents; and responding to an active shooter incident (FDNY, 2011, p. 12). The ability of the FDNY to respond to these as well as other incidents is often put to the test by the CTDP exercise design team. Exercises conducted by the team range from simple intra-/inter-agency tabletop exercises to full-scale, multi-agency exercises. The principal purpose of conducting such exercises is to evaluate the ability of the FDNY and participating agencies to respond to specific types of terrorist attacks (FDNY, 2011, p. 13).

Mitigation

Mitigation is defined as mitigating the loss of life and property by lessening the impact of future disasters (DHS, 2011a, pp. 9–11). In order to carry out its mitigation effectively, the FDNY determined that it would have to understand the potential threats it could encounter, these could only be understood through a proper risk assessment (FDNY, 2011, p. 20), much like a local version of the SNRA. To do this, FDNY utilizes the Risk Assessment and Target Hazard (RATH) Unit. This unit accomplishes the goals set forth in the *National Infrastructure Protection Plan* (NIPP) (DHS, 2009). The RATH Unit gathers information on NYC's critical infrastructure and key resources identifying target hazards, prioritizing preparedness efforts and developing tactical response plans for specific structures. One specific example of this is found in a combined effort between the RATH Unit, the Army Corps of Engineers, and the Department of Transportation. In response to terrorist threats toward the bridges of NYC this effort produced the bridge operations guides. These guides can be utilized to evaluate the structural integrity of bridges damaged in a terrorist attack. One version of this is carried on all FDNY apparatuses tasked with emergency response and a more in depth version is kept locked in the Fire Department Operations Center (FDOC) (the FDNY's Emergency Operations Center [EOC]) (FDNY, 2007b, p. 21).

Response

Response is defined as responding quickly to save lives, protect property and the environment, and meet basic human needs in the aftermath of a catastrophic incident.

This mission area focuses on ensuring that the nation is able to respond effectively to all types of incidents ranging from those that can be handled at a local level to those catastrophic events requiring a federal response (DHS, 2011a, pp. 11–15).

In the majority of the areas of response described in the *National Planning Scenarios* (DHS, 2005b), the FDNY would move to the forefront of operations in the event of a catastrophic incident. Intelligence in the time leading up to the incident, during the incident, and following the incident is crucial. In the time leading up to an attack, the intelligence provided informs our planning and then our SOPs. It will also be crucial for the research and development, and finally the acquisition of equipment. Finally, it will be used for the purpose of curriculum development, training, and finally exercise development. A specific example of this is the response of the FDNY to the possibility of a chemical attack on the subway system. FDNY developed SOPs and the ERP, entitled *Suspected Chemical Attack in an Underground Transit System* (FDNY, 2004).

The nature of the threat established the need for additional personal protective equipment (PPE). This consisted of such items as: chemical protective clothes, and rebreather masks. Rebreather masks are breathing apparatus capable of supplying hours of breathing air as opposed to the minutes supplied by most firefighting self-contained breathing apparatus (SCBA). In addition, rebreather units were formed not only to maintain this specialized equipment but also to assemble it and deliver it to the site of an attack. FDNY SOC established a training and recertification program for all of the personnel involved. All of this has culminated in several large scale multi-agency exercises. Items such as these required extensive research, development, and testing. Numerous units throughout the FDNY have been designated as special units and become part of the plan for a tiered response to an attack.

Recovery

Recovery focuses on the timely restoration, strengthening, and revitalization of infrastructure, housing, and a sustainable economy, as well as the health, social, cultural, historic, and environmental fabric of communities affected by a catastrophic incident (DHS, 2011a, pp. 15–18).

With regard to specialized capabilities that intelligence has identified as important, FDNY addressed two major issues, implementing the principals of a tiered response and decentralization. One of the key principals of the *National Response Framework*, on a national level a tiered response, suggests that catastrophic events are best handled locally with additional layers of government assistance (e.g., state or federal) added only as required (DHS, 2014, pp. 5–6). FDNY utilizes this principle to assign units that possess the appropriate level of training and equipment for the mission at hand. In the past, only the special operations units had the training and equipment for many of the disciplines required to respond to various terrorist attacks. Now, other units receive the appropriate levels of training to respond to specific aspects of this type of operation.

Decentralization is a principle that spreads out capabilities that are unique but that could prove essential. This can be crucial in the event of these capabilities being lost as a result of the attack or isolation of capabilities through the loss of infrastructure, such as bridges and tunnels—both of which have been reported as potential targets. In regard to the five mission areas defined in PPD-8, the FDNY has demonstrated that it has a significant role in fulfilling the NPG as well as the ability to utilize intelligence to fulfill this role (DHS, 2014, p. 1).

THE ROLE OF THE FIRE SERVICE TOWARDS VARIOUS TERRORIST ATTACKS

In addition to what mission areas the FS would have a role in, the type of terrorist attack that the FS would have a role was analyzed. As in the mission areas, this analysis used FDNY as a model. In addition, to assist in determining the FS's role the national planning scenarios (NPS) were utilized. The NPS consists of 15 all-hazard scenarios for use in homeland security preparedness activities. The *National Planning Scenarios: Attack Timelines* (NPS: AT) (also known as attack prequels) are an addition to the national planning scenarios. These scenarios are used by all levels of government in planning for potential terrorist attacks and natural disasters. In the NPS, the scenario begins from the time of the attack and was intended to aid in planning the response phase. In contrast, the scenarios in the NPS: AT begin with the conception of the attack and end

with the culmination of the attack. The prequels offer the scenario leading up to each of the terrorist attacks listed in the NPS (DHS, 2006, pp. ii–iii).

The objective in developing these scenarios was to establish the minimum number of scenarios required to develop and test the range of required prevention, protection, response, and recovery resources. Twelve of the scenarios represent terrorist attacks, and three represent naturally occurring events. For each of the 12 terrorism-related national planning scenarios, Federal Emergency Management Agency (FEMA) partnered with I&A and other IC and LE experts for their development.

The 15 national planning scenarios are:

- Scenario 1: Nuclear Detonation—improvised nuclear device
- Scenario 2: Biological Attack—aerosol anthrax
- Scenario 3: Biological Disease Outbreak—pandemic influenza
- Scenario 4: Biological Attack—plague
- Scenario 5: Chemical Attack—blister agent
- Scenario 6: Chemical Attack—toxic industrial chemicals
- Scenario 7: Chemical Attack—nerve agent
- Scenario 8: Chemical Attack—chlorine tank explosion
- Scenario 9: Natural Disaster—major earthquake
- Scenario 10: Natural Disaster—major hurricane
- Scenario 11: Radiological Attack—radiological dispersal device
- Scenario 12: Explosives Attack—bombing using improvised explosive device
- Scenario 13: Biological Attack—food contamination
- Scenario 14: Biological Attack—foreign animal disease
- Scenario 15: Cyber Attack

As stated, the intent of the NPS is to establish the minimum number of scenarios required to develop and test the various mission areas. In order to accomplish this, several scenarios that were addressed in the SNRA were either not covered or were covered superficially. One scenario with significant homeland security implications that was not addressed in either is an EMP attack. However, the SNRA did cover space weather which

for the purposes of the FS is very similar to an EMP. In addition, while cyber-attacks were covered in the NPS, the SNRA elaborates on this by adding the classification of cyber-attacks against physical infrastructure, which would have greater consequences for the FS. In addition to these scenarios, an analysis of real attacks, both attempted and successful, upon the nation since September 11, 2001, pertinent trending attack patterns around the world, and some modes of attack that were assessed in the SNRA that were not developed into scenarios in the NPS and NPS: AT was also conducted.

Finally, I assessed some of the large scale attacks that have occurred around the globe that are considered by FDNY to be of exceptional significance and to represent a new tactic. These included: the 2008 attack on Mumbai, the 2013 attack on the Westgate Shopping Mall in Nairobi, Kenya, and the 2015 attacks in Paris and San Bernardino. The FDNY classifies attacks of this type as Mumbai-style attacks. According to the FDNY, some of the characteristics of this type of attack include: multiple attackers that are mobile, multiple targets, and combined weapons, including active shooters and fire and/or explosives (Center for Terrorism and Disaster Preparedness, 2009). In every type of attack that was examined, a significant response of the FDNY would be required.

THE CHALLENGE IN PROVIDING THE FIRE SERVICE WITH INTELLIGENCE

As has been previously stated the IC generally is accustomed to providing intelligence to the military and law enforcement communities. This intelligence is generally aimed at prevention and protection; however, this falls short for the needs of the FS. Assistant Chief Joseph Pfeifer, the FDNY's Chief of Counterterrorism and Emergency Preparedness, elaborates on some of the problems the FS experiences in obtaining intelligence in his article, "Network Fusion: Information and Intelligence Sharing for a Networked World," published in *Homeland Security Affairs*. Chief Pfeifer writes of the dangers of information originating from a place of limited perspective; with the information only being pushed when the originating agency deems it necessary (Pfeifer, 2012, p. 5). He also writes of various types of organizational bias that can hinder the dissemination of appropriate intelligence, including an in-group bias toward LE and another form of bias, mitigation neglect. Mitigation neglect is a bias toward intelligence

required to prevent a terrorist attack and neglecting the intelligence that is necessary to mitigate such an attack (Pfeifer, 2012, pp. 7–8). This guide is intended to overcome these phenomena by establishing within the IC an understanding of the FS and hence intelligence requirements.

UNDERSTANDING THE INTELLIGENCE REQUIREMENTS OF THE FIRE SERVICE

The intelligence cycle consists of developing raw information into finished intelligence for consumers of intelligence to use in their decision-making process (ITACG, 2009, p. 10). The first step of this cycle is "establishing the intelligence requirements of the consumer of intelligence" (JCAT, 2015, p. 30). The IC must first understand what is required in regard to intelligence before it can provide it. To establish the intelligence requirements of the FS, it was first necessary to determine the mission requirements in regard to national preparedness of the FS and the type of terrorist attacks in which the FS would have a role.

After the five preparedness missions were examined, it was concluded that the FS has the potential for involvement in all five mission areas. In addition, the FS's role in relation to the various forms of terrorist attacks was also examined. This examination indicates that in addition to having a role in all of the preparedness missions the FS would have a role in all of the forms of terrorist attacks. Specific examples of FDNY's utilization of intelligence to respond to its roll in each mission area were also examined. In analyzing FDNY's role in each of the mission areas and the intelligence required to fulfill that role, the intelligence requirements were broken down into two mission areas: those required for the prevention mission and those required for the response mission. In the prevention mission, FDNY's primary roll would be one of a potential intelligence gatherer for the IC and law enforcement community (LEC) and as such would require information pertaining to what attack indicators it should be alert for. In the other mission areas, it was determined that the intelligence that would be required by FDNY for its role in the response mission would also apply to the protection, mitigation, and recovery missions.

THE INTELLIGENCE REQUIREMENTS OF THE FIRE SERVICE

In examining the five mission areas, the intelligence needs of FDNY can be represented by stating the requirements for the two mission areas of prevention and response.

Intelligence for the Prevention Mission

The ability of the IC to provide intelligence to the FS for the prevention mission and on imminent attacks is well established. This is largely due to the existing prevention bias in both the IC and the LEC. This is rightfully the primary concern of these communities as the prevention mission is the mission area they work in on a daily basis and preventing an attack is the optimal outcome.

In addition, there are several other reasons that the IC is well equipped to provide intelligence for the FS to utilize in the prevention mission. One reason is that the majority of intelligence that is required for the prevention mission is the same no matter who is trying to accomplish it, whether it is the FS or more traditional consumers of intelligence; which in FDNY's area of operations would generally be LE. A substantial amount of this intelligence is covered by the extensive work that has been done on the terrorist attack planning cycle and its variants. This information is widely utilized throughout the emergency response community and also employed to some extent by the private sector. Furthermore, there is a large volume of intelligence provided to emergency responders through training that is being conducted throughout the emergency response community in regard to WMDs. This training is not just pertaining to the response to such attacks but to the recognition of the components and fabrication processes of such weapons. In addition to numerous in house programs and onsite training, the FDNY utilizes WMD schools throughout the country including: the Center for Domestic Preparedness in Anniston, Alabama; the Energetic Materials Research and Testing Center in Socorro, New Mexico; the Center for Radiological and Nuclear Training at the Nevada National Security Site; and Dugway Proving Ground in Utah.

The other main reason that the IC is well equipped to provide intelligence for the FS to utilize in the prevention mission is that in carrying out the prevention mission the

FS is really providing intelligence to the IC. The prevention mission of the FS is widely recognized by the IC to consist of its ability to act as intelligence gatherers. This is based on the ability of the FS to enter numerous structures on a daily basis and even to carry monitoring equipment on these entries. What this means is that the intelligence the IC provides to the FS for the prevention mission relates directly to the intelligence that the IC requires for the prevention mission.

In general most of the intelligence required by LE for the prevention of a terrorist attack would be appropriate for the FS. An important exception would be the intelligence that the FS does not need. This exception would consist of sensitive information, such as the sources and methods of intelligence acquisition, which while important to the LEC would generally be inconsequential to the FS. The criteria that is important for the FS to evaluate intelligence for its credibility and reliability.

Intelligence for the Response Mission

While the LEC and the IC focus on the prevention mission, the response mission is the area where the FS will have its most extensive role. While the ideal is to prevent terrorist attacks, history has repeatedly shown us that this will not always be possible. According to the *National Strategy for Counterterrorism*:

> At the same time, we recognize that no nation, no matter how powerful, can prevent every threat from coming to fruition. That is why we are focused on building a culture of resilience able to prevent, respond to, or recover fully from any potential act of terror directed at the United States. (U.S. Executive Office of President, 2011, p. 5)

Further highlighting the IC's prioritization of the prevention mission is that of the core goals that are defined in the NPG; intelligence and information sharing are only components of the prevention and protection missions. This corroborates the necessity to provide the IC with the intelligence requirements of the FS for the response mission.

To establish the intelligence required by the FS in the response mission, I conducted an analysis of the information that is gathered and utilized by the FS at emergency operations on a daily basis. This gathering process is known as conducting a size-up. In the FS, COAL WAS WEALTH is an acronym that is often taught as a

mnemonic device to aid FFs to conduct a size up at a fire or other emergency operation. While there are several other popular methods, they are all very similar. The mnemonic COAL WAS WEALTH was chosen for this research because it is the one utilized by FDNY. However, one change to the mnemonic was introduced by Deputy Assistant Chief John Norman Chief, a retired member of FDNY, who was placed in charge of FDNY Special Operations Command (SOC) in the aftermath of the 9/11 attacks. In his book the *Fire Officer's Handbook of Tactics*, he made a change that is particularly pertinent when conducting a size-up of terrorist attacks that is included here (Norman, 2012). As taught by FDNY, COAL WAS WEALTH stands for:

- Construction
- Occupancy
- Auxiliary appliances
- Life
- Weather
- Apparatus and equipment
- Street conditions
- Water supply
- Exposures
- Area and height
- Location
- Time
- Hazardous materials

While the primary design of this size-up format and others like it is to assess a building fire, they are regularly utilized to assess fires in other structures such as ships and planes, and during other emergencies such as collapses. The intelligence provided through performing this assessment can be utilized in many emergencies including terrorist attacks. This may require minor substitutions to points of the size-up but these substitutions are simple once the principles are understood. As an example the categories of: construction (the method and material by and of which a building is built) and

occupancy (what a building is utilized for) could both be explained by intelligence stating that the terrorist attack is in a subway.

When conducting an assessment utilizing this 13-point size-up it is important to note that many points when examined can provide information on other points. Some examples would be: time can be an indicator of the life hazard (e.g., an apartment build at 3 AM can be expected to contain numerous sleeping occupants); occupancy can be an indicator of the presence of hazardous materials (e.g., an occupancy involved in plastics manufacturing can produce plastic dust which is explosive); and construction can be an indicator of the auxiliary appliances that are present (e.g., many buildings of type 1 construction have standpipe systems).

The following list is an explanation of each point of the 13-point (COAL WAS WEALTH) size-up, along with examples of their standard applications during fires and their potential applications during a terrorist attack.

Construction

Generally, the FS utilizes the National Fire Protection Association's (NFPA) method of classifying construction types, dividing building construction into five categories. These are: type 1: fire resistive, type 2: noncombustible, type 3: ordinary, type 4: heavy timber and type 5: wood framed. Every type of building construction has different firefighting and emergency operations SOPs associated with it. This is due to such factors as: how fire affects a structure, how fire and smoke spread, the collapse dangers of a building along with likely collapse patterns, and even items such as the buildings vulnerability to a terrorist attack with a chemical weapon (or other hazardous materials release), such as a buildings heating ventilating and air conditioning (HVAC) system utilized to disperse a WMD.

Type 1 Construction—Fire Resistive

Fire resistive buildings, the most common of which are known as "high-rises," are more than 75 feet tall and are constructed of concrete and fire protected steel. These structures generally limit the spread of fire and are resistant to collapse during usual fire conditions. Important features found in this type of construction can include a HVAC

system, the components of which penetrate the structures fire resistive barriers, and other auxiliary appliances, such as standpipe systems that provide water for firefighting. The HVAC system can not only spread the products of combustion and other hazardous materials, it can also be used to contain and control the spread.

Type 2 Construction—Noncombustible

The structural elements in noncombustible construction, while they are noncombustible, they do not have the fire-resistive rating of type 1 construction. Type 2 buildings are most often made of steel and can include structures such as warehouses and schools. Since these structures are constructed with noncombustible materials the fireload is determined by the contents. Since these structures are not constructed with fire-resistive materials, they are prone to collapse under fire conditions.

Type 3 Construction—Ordinary

Ordinary construction, also known as “brick and joist” construction, is commonly made with non-combustible masonry walls and a wood roof and floors. This type of structure can have hidden areas where fire can spread, such as in separate but adjoining structures that have a common cockloft (attic).

Type 4 Construction—Heavy Timber

Heavy timber construction has masonry exterior walls that are load bearing. Interior structural members are of wood and to meet the type 4 criteria must be of sufficient dimensions. Some common uses of this type of structure are found in commercial applications such as manufacturing or a warehouse.

Type 5 Construction—Wood Framed

Wood frame construction is very common and is generally utilized in the construction of private dwellings as well as other structures. This type 5 construction is found in many modern homes.

This system of classifying structures into five types is just a guideline as not every structure will fit perfectly into a given category. However, using the knowledge of

construction put forth here enable an assessment of a structures strengths and weaknesses.

An emergency or attack upon something other than a building could also be covered by the construction point of the 13-point size-up. Some example would be attacks on: planes, trains, bridges or a subway system. This can also be applied to the next point, occupancy.

Occupancy

There are many categories of occupancy, such as is the structure residential or commercial; however, basically occupancy means, “what is the structure used for?” This can be an indicator of many things such as the life hazard. An apartment building would probably have a greater life hazard than a storage facility, and an assisted living facility would probably have a greater life hazard than an apartment building. The type of occupancy can also indicate a structure collapse potential. A structure that is subjected to the load of heavy equipment is generally a greater collapse hazard. It can also be an indicator of the structures potential as a terrorist target. Is the structure of historical significance? Is it a government building? Is the structure a chemical facility producing a chemical such as chlorine gas? All of these factors could increase a structures potential as a terrorist target.

Auxiliary Appliances

The main items that the FS is concerned with when referring to auxiliary appliances are standpipe and sprinkler systems; as well as other specialized fire suppression systems, such as halon, foam, or dry chemical. Standpipe systems are what the FS utilizes to provide it with water for firefighting operations. Sprinklers and other fire suppression systems can also aid in firefighting efforts. In addition, auxiliary appliances can also refer to various detection systems, such as smoke, chemical, carbon dioxide, or heat detectors. Many of these systems could become damaged secondary to an attack. For instance, the pipes supplying water to a standpipe system in a high rise building could be damaged by an explosion. This would make getting water on a fire on the 80th floor difficult. These systems themselves are also potential targets, which if

successfully targeted, could take away the ability of the FS to both detect and respond to hazardous conditions.

Life

Life hazard is always the primary concern in any emergency. Some factors to take into consideration when assessing the life hazard are: how many people are in danger, what is their location (will removal be difficult such as in a subway system), and what is their physical condition? The occupant's condition could be an existing one, such as when responding to a hospital, or it could be secondary to the situation, such as incapacitation due to a chemical release. Life hazard does not just have to be those that are present at the target of the attack. The life hazard can also be the emergency responders, such as in the case of a secondary attack. Finally, the degree of the life hazard itself can also affect a structure's desirability as a terrorist target.

Weather

There are numerous weather conditions to consider. Temperature extremes of both hot and cold can be debilitating to operating personnel. In addition, snow and ice can hinder both response and operations. Temperature can play a major role in the effectiveness of a chemical attack (e.g., mustards have a low volatility at low temperatures but develop a major vapor hazard at high temperatures). Moreover, temperature is also a major consideration in any hazardous material release as is the wind. Wind can also have a major affect on the spread of fire in both an urban and a wilderness environment. Forest fires have become a means of terrorist attack recommended by *Inspire* magazine. These can be affected by both dry weather and wind.

Apparatus, Equipment, and Personnel

The apparatus, equipment, and personnel needs are dictated by the incident. In times of elevated terrorist threats, manpower can be increased and/or reallocated, and specialized equipment and apparatus can be prepared and manned. Which personnel and equipment are activated could possibly be dictated by available intelligence. In 2004, the author was assigned for several months as an officer in Rescue 6, a rescue company that

was set up on a temporary basis by the FDNY to deal with an elevated terrorist threat in a high risk area.

Street Conditions

This section refers to more than just street conditions, it refers to anything affecting the avenue of access to the area of operations, including any terrain or water features. An example would be a scenario requiring a response via fireboat. This can also be a result of weather conditions, such as heavy snowfalls. The means of access is a potential target for a terrorist attack—an example of which would be using vehicles to block out responders.

While in firefighting operations "street conditions" generally refers to the streets adjacent to the area of operations, with regard to terrorism, this should be expanded to include access and egress to and from the entire affected area. Additionally, it should include considerations for the access of various specialized units and equipment that could be required. As an example, in the time since 9/11, there have been several potential terrorist threats to the bridges of NYC. In response to these threats, the FDNY sought to develop a standalone capability for each of the five boroughs. This involves a certain level of duplication of certain classifications of units as well as equipment. This policy is intended to allow an area that is isolated by a terrorist act, such as the destruction of a bridge or a tunnel, to have the resources to respond to the various types of potential attacks.

Water Supply

Water supply includes the availability of fire hydrants, bodies of water to pump out of, or any other initial water source. It can also include the apparatus necessary to pump and otherwise transport the water. For FDNY, this can include fire engines, fire boats to pump water, satellite units consisting of high capacity pumpers, and hose wagons to lay various large diameter and specialized hose line through which to pump water. In addition, water supply can include buildings systems, such as standpipes, sprinklers, and pumps. Establishing or maintaining an adequate water supply in the aftermath of an attack has long been a topic of concern for FDNY. This concern dates back to a time

when members of FDNY were assigned to the London Fire Brigade during World War II to observe the tactics that London firefighters had established to respond to the bombings of London. Interrupting the water supply at any link in the supply chain has the potential to prove disastrous in regard to firefighting and other emergency operations. This interruption could be secondary to an attack that involves as explosion or collapse that damages supply lines, or it could be the main focus of the attack, such as removing supply lines in a high rise buildings standpipe system to deny water to fight a fire on the 86th floor. Water is also a critical component of other emergency operations, such as gross decontamination operations in response to a chemical attack. Due to its great importance, the FDNY has many contingency plans to supply water in various situations such as using a hose wagon from a satellite unit to lay large diameter hose line to be used as a replacement for damaged water mains. This hose can be supplied from a fireboat, with access to a limitless supply of water, which pumps at a capacity of 50,000 gallons per minute (GPM) (standard FDNY engines pump at 1,000 GPM with some specialized engines pumping at 2,000 GPM).

Exposures

When referred to in relation to fire operations, exposures are generally referencing adjoining buildings or areas adjoining the fire area within the fire building. Among other things, exposures are the areas that are susceptible to the spread of fire and toxic gases, resulting in a life hazard. Exposures can also be susceptible to collapse if the fire building collapses. In relation to emergency operations in general, exposures can be thought of as any area that can be affected by or affect the area of operations. As in collapse operations, this refers to the six sides of the collapse area: left, right, front, back, above, and below. In the event of a chemical attack, this could include the area expected to be engulfed by the plume, or in a chemical attack in a high-rise, an immediate exposure problem would be areas serviced by the same HVAC system. In regard to a pandemic, exposure considerations can be national and international. Finally, exposures are not just problematic, they can be useful for such purposes as providing access to the area of operations to emergency responders and egress for victim removal.

Area and Height

Most commonly in the urban FS, area and height refers to the area of the building or occupancy. However, in reference to response to terrorist attacks, these could refer to a much larger area, such as an intentionally set forest fire or a large scale chemical release. It can also refer to an even larger area such as a biological attack spreading throughout the country. In the aforementioned examples of buildings or occupancies, the area and height can be indicators of the numbers of victims and the difficulty of evacuation. These factors can also dictate tactics due to equipment limitations, such as the length of aerial ladders used by the FS for access and egress, or by established SOPs, such as the common practice in the FS of utilizing standpipe systems to provide access to water for firefighting in structures, such as high-rise buildings, bridges, and stadiums.

Location and Extent of Fire (or Incident)

In fire operations, depending on the type of structure, the location of the fire indicates such important factors as where the fire could spread to and the potential for collapse. In addition, much like during 9/11, areas above the fire area can become isolated, and if these areas are out of reach of fire department ladders the opportunities for victim removal are limited. At incidents in remote areas like the upper floors of a high-rise, removal can be problematic, even if the area does not become isolated, due to the excessive distances involved. Attacks upon the means of egress, such as the elevators, can exacerbate these difficulties. This isolation can also take place during other types of attack, such as a chemical release. Another example would be an incident occurring below grade. In these incidents, venting toxic gases whether they are from fire or from a chemical attack can be very difficult. In addition, some potential weapons such as chlorine gas were designed with below grade attacks in mind. Chlorine gas is 2.5 times heavier than air and was used in trench warfare in World War I for its ability to travel along the ground and fill up the trenches. The FDNY has done much preparation for chemical attacks on the subway system with weapons like this in mind.

Time

Time of day along with the type of occupancy will generally dictate the life hazard. For example, during a fire at 3 AM, a multiple dwelling can be assumed to contain many sleeping occupants, as opposed to a fire at the same time in a factory. A factory at that time may well be closed for business and contain no life hazard. Time also takes into consideration the day of the week that an incident occurred on as well as anything else notable in regard to the date. On a Sunday, a grade school may be closed as opposed to on a weekday. Holidays must be taken into consideration both for estimating the life hazard present and for the symbolism they represent for terrorists planning an attack. When responding to an incident, the amount of time that has passed since the incident occurred must be taken into consideration. This is important in determining, such items as the stability of a structure exposed to long periods of fire or the viability of victims buried in a collapse or exposed to chemical weapons.

Hazardous Materials

The presence of hazardous materials is always a consideration when responding to an emergency situation. Fires, flooding, auto accidents, and collapses are just a few examples of emergencies that can result in the release of hazardous materials. In the case of a terrorist attack the release of hazardous materials can be the main goal of the attack as in a chemical attack, a component of the attack as in a dirty bomb, or secondary to the primary attack as in a chemical release caused by an explosion. In addition this is the category in which the type of attack can be covered be it chemical, fire, explosive or active shooter.

Many components or the 13-point size-up will tie together and overlap. As an example the time section can indicate different life hazards. One example is a mall at three in the afternoon has a different life than the same mall at three in the morning. Another example would be on a Monday afternoon a school may have a greater life hazard than a church; however, this could switch at the same time on a Sunday. Additionally, on another Monday in that same school and church the church could still be

the greater hazard if that Monday happened to fall on December 25. Yet another example is how the type of occupancy can indicate the presence of certain hazardous materials.

Intelligence that is provided utilizing this 13-point size up would not only be useful in responding to a terrorist attack, it could also be used by the FS in the protection, mitigation, and recovery missions.

CONCLUSION

There is a clear need for timely, actionable intelligence to enable the FS to make appropriate tactical and strategic decisions pertaining to terrorist attacks. In determining what intelligence is required by the FS two items became apparent:

One, there is a vast disparity between fire departments. On one end of the spectrum, there are small departments consisting of a dozen members who are part-time volunteers located in a rural area with no history of either a terrorist attack or the threat of one. On the other end of the spectrum are large departments, such as FDNY, which has more than 13,000 members and is located in a city with a long history of terrorist attacks. This history includes: having been the target of 284 terrorist attacks from 1970 to 2007 (National Consortium for the Study of Terrorism and Responses to Terrorism, 2010, p. 1), having been one of the targets of the largest terrorist attack in the history of the nation, and a continuing history of being a primary terrorist target. In the case of the small department in this example, the department does not have the infrastructure to handle a large volume of incoming intelligence nor is this a priority. The FDNY has more personnel assigned to the CTDP than many small fire departments have in their entirety. However, any department faces the potential of dealing with the aftermath of a terrorist attack. The rural department could respond to attacks ranging from the consequences of an active shooter incident such as the 2015 San Bernardino attacks or an intentionally set forest fire. In an incident such as San Bernardino, the awareness of intelligence, such as that regarding distribution and/or emplacement secondary devices, could be crucial.

Two, the methodology of potential terrorist attacks and thus the possible intelligence that could become available is not just vast but highly diverse and

continually evolving. This negates the possibility of naming all of the specific intelligence that would be required by the FS in a list format.

In the *National Preparedness Goal*, it points out how the "The terrorist threat is dynamic and complex" (DHS, 2011a, p. 4) and that this necessitates that the goal continue to evolve. This requires the goal to be a living document, which will be regularly reviewed to evaluate consistency with existing and new policies, and evolving conditions (DHS, 2011a, p. 19). The dynamic and complex nature of the terrorist threat that is written of in the goal negates the possibility of formulating a specific list of intelligence requirements. In lieu of this, a better option is to establish within the IC an understanding of the operations of the FS in regard to decision making. By having an understanding of the principles behind providing the FS with intelligence, a system is established that will remain viable even as the terrorist's tactics continue to morph. By providing an explanation of the information that the FS utilizes to prepare for and respond to emergencies on a daily basis an understanding, as opposed to a stagnant list, of the intelligence needs of the FS is established.

In addition to providing a framework for the IC to utilize to provide intelligence to the FS pertaining to the vast and ever changing variety of potential terrorist attacks, this method of providing intelligence also takes into account the vast disparity in the resources available to and the situations encountered by different fire departments. While there may be vast differences between fire departments, there are common denominators. These common denominators are the potential missions of the FS in a given scenario, the decision-making process utilized to carry out these missions and hence the intelligence required to carry out these missions. While departments may have vast differences, they all have similar intelligence requirements. While they may be presented with different situations and have different resources to respond with, when presented with the same situation they require the same intelligence. This also applies to intelligence that they do not require. Too much information can prove just as problematic as insufficient intelligence as excessive intelligence can overwhelm the system.

GUIDE LIST OF ACRONYMS

CTDP	Center for Terrorism and Disaster Preparedness
DHS	U.S. Department of Homeland Security
DOHMH	NYC Department of Health and Mental Hygiene
EMP	electromagnetic pulse
EMS	emergency medical service
EOC	emergency operations center
ERP	emergency response plan
FDNY	Fire Department City of New York
FDOC	Fire Department Operations Center
FEMA	Federal Emergency Management Agency
FS	fire service
GIS	geographic information systems
GPM	gallons per minute
HVAC	heating ventilating and air conditioning
IC	Intelligence Community
ITACG	Interagency Threat Assessment and Coordination Group
JCAT	Joint Counterterrorism Assessment Team
LE	law enforcement
LEC	law enforcement community
NFPA	National Fire Protection Association
NIPP	*National Infrastructure Protection Plan*
NPG	*National Preparedness Goal*
NPS	*National Planning Scenarios*
NPS: AT	*National Planning Scenarios: Attack Timelines*
NYC	New York City
PPD	presidential policy directive
RATH	Risk Assessment and Target Hazard Unit
SNRA	*Strategic National Risk Assessment*
SOC	FDNY Special Operations Command
SOP	standard operating procedure
WMD	weapon of mass destruction

GUIDE LIST OF REFERENCES

Center for Terrorism and Disaster Preparedness. (2009, February 19). The Mumbai terrorist attack. In *Fireguard.* Fort Totten, New York: Fire Department City of New York.

Center for Terrorism and Disaster Preparedness. (2011). *Counterterrorism and Risk Management Strategy*. Fort Totten, New York: Fire Department City of New York.

Fire Department City of New York. (2004, August 30). Addendum 2, suspected chemical attack in an underground transit system. In *Fire tactics and procedures, emergency response plan*. Brooklyn, New York: author.

Fire Department City of New York. (2006, May 16). Addendum 4a, operational guidelines for Radalert™ 50 radiological monitor. In *Fire tactics and procedures, emergency response plan*. Brooklyn, New York: author.

Fire Department City of New York. (2007a). Addendum 4d, ultraradiac personal radiation monitor. In *Fire tactics and procedures, emergency response plan*. Brooklyn, New York: author.

Fire Department City of New York. (2007b). *Terrorism and disaster preparedness strategy*. Brooklyn, New York: author.

Fire Department City of New York. (2010). *Fire Department City of New York marine operations strategy*. Brooklyn, New York: author.

Fire Department City of New York. (2011). *FDNY counterterrorism and risk management strategy*. Brooklyn, New York: author.

Fire Department City of New York. (2015). *FDNY vital statistics calendar year 2014.* Brooklyn, New York: author. Retrieved April 24, 2015, from http://www.nyc.gov/html/fdny/pdf/vital_stats_2014_cy.pdf

Interagency Threat Assessment and Coordination Group. (2009). *Intelligence guide for first responders*. Retrieved October 9, 2012, from http://www.nctc.gov/docs/ITACG_Guide_for_First_Responders_2011.pdf

Joint Counterterrorism Assessment Team. (2015) *Intelligence guide for first responders*. Joint Counterterrorism Assessment Team. Retrieved November 10, 2015, from https://www.ise.gov/sites/default/files/Intelligence%20Guide%20for%20First%20Responders_web.pdf

National Consortium for the Study of Terrorism and Responses to Terrorism. (2010). *Background report: Terrorist attacks in New York City*. College Park, MD: author.

Norman, J. (2012). *Fire officers handbook of tactics* (4th ed). Tulsa, OK: PennWell Corporation.

Pfeifer, J. (2012, October). Network fusion: information and intelligence sharing for a networked world. *Homeland Security Affairs, 8*, 1–20.

U.S. Department of Homeland Security. (2005a). *Interim national preparedness goal*. Washington, DC: author.

U.S. Department of Homeland Security. (2005b). *National planning scenarios*. Washington, DC: Homeland Security Council.

U.S. Department of Homeland Security. (2006). *National planning scenarios: Attack timelines*. Washington, DC: author.

U.S. Department of Homeland Security. (2009). *National infrastructure protection plan*. Emmitsburg, MD: author.

U.S. Department of Homeland Security. (2011a). *National preparedness goal* (1st ed.). Emmitsburg, MD: author.

U.S. Department of Homeland Security. (2011b). *Strategic national risk assessment in support of PPD 8: a comprehensive risk-based approach toward a secure and resilient nation*. Washington, DC: author.

U.S. Department of Homeland Security. (2014). *Overview of the national planning frameworks*. Washington, DC: author.

U.S. Executive Office of President. (2011). *National strategy for counterterrorism*. Washington, DC: author. Retrieved April 24, 2015, from https://www.hsdl.org/?view&did=776858

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Bureau of Justice Assistance. (2005). *Intelligence-led policing: the new intelligence architecture, new realities, law enforcement in the post-9/11 era*. Washington, DC: U.S. Department of Justice.

Center for Terrorism and Disaster Preparedness. (2009, February 19). The Mumbai terrorist attack. In *Fireguard.* Fort Totten, New York: Fire Department City of New York.

Cruthers, F. (2008, 1st quarter). 2007 fire service intelligence enterprise conference. *With New York Firefighters*, 22–23.

Ellis, M. (2014). *Identifying and leveraging trust as a key element in the development, implementation and sustainment of the Salt Lake City Fire Department's intelligence program*. Master's thesis, Naval Postgraduate School, Monterey, CA.

Faiola, A & Mufson, S. (2007, June 3). N.Y. airport target of plot, officials say. *The Washington Post*. Retrieved May 5, 2011, from http://www.washingtonpost.com/wp-dyn/content/article/2007/06/02/AR2007060200606.html

Fire Department City of New York. (2004, August 30). Addendum 2, suspected chemical attack in an underground transit system. In *Fire tactics and procedures, emergency response plan*. Brooklyn, New York: author.

Fire Department City of New York. (2006a, February 2). Addendum 4, radiological operations. In *Fire tactics and procedures, emergency response plan*. Brooklyn, New York: author.

Fire Department City of New York. (2006b, May 16). Addendum 4a, operational guidelines for Radalert™ 50 radiological monitor. In *Fire tactics and procedures, emergency response plan*. Brooklyn, New York: author.

Fire Department City of New York. (2007a). Addendum 4d, ultraradiac personal radiation monitor. In *Fire tactics and procedures, emergency response plan*. Brooklyn, New York: author.

Fire Department City of New York. (2007b). *Terrorism and disaster preparedness strategy*. Brooklyn, New York: author.

Fire Department City of New York. (2007c). *Department order no. 48*. Brooklyn, New York: author.

Fire Department City of New York. (2009). *All units circular 342, sensitive but unclassified information policy*. Brooklyn, New York: author.

Fire Department City of New York. (2010). *Fire Department City of New York marine operations strategy*. Brooklyn, New York: author.

Fire Department City of New York. (2011). *FDNY counterterrorism and risk management strategy*. Brooklyn, New York: author.

Fire Department City of New York. (2013a, 4th quarter). Counterterrorism and disaster preparedness. *With New York Firefighters*, 20–21.

Fire Department City of New York. (2013b). Ladder company operations tenements. In *Firefighting procedures* Vol. 3, book 3. Brooklyn, New York: author.

Fire Department City of New York. (2015). *FDNY vital statistics calendar year 2014.* Brooklyn, New York: author. Retrieved April 24, 2015, from http://www.nyc.gov/html/fdny/pdf/vital_stats_2014_cy.pdf

Gartenstein-Ross, D. & Dabruzzi, K. (2008). *Firefighters' developing role in counterterrorism*. Manhattan: Center for Policing Terrorism, Manhattan Institute.

Heirston, B. (2009). *Terrorism and firefighters: Where are the information-sharing boundaries?* Master's thesis, Naval Postgraduate School, Monterey, CA.

Inserra, D. & Phillips, J. (2015). *67 Islamist terrorist plots since 9/11: spike in plots inspired by terrorist groups, unrest in Middle East.* Special Report No. 4392. Washington, DC: The Heritage Foundation.

Interagency Threat Assessment and Coordination Group. (2009). *Intelligence guide for first responders*. Retrieved October 9, 2012, from http://www.nctc.gov/docs/ITACG_Guide_for_First_Responders_2011.pdf

Joint Counterterrorism Assessment Team. (2015) *Intelligence guide for first responders*. Joint Counterterrorism Assessment Team. Retrieved November 10, 2015, from https://www.ise.gov/sites/default/files/Intelligence%20Guide%20for%20First%20Responders_web.pdf

Lowenthal, M. (2006). *Intelligence: From secrets to policy* (3rd ed.). Washington, DC: CQ Press.

Lowenthal, M. (2009). *Intelligence: From secrets to policy* (4th ed.). Washington, DC: CQ Press.

Martinez, B. and McLoughlin, J. (2008, February). The fire service and counterterrorism: unified command. *Fire Engineering.* 73–78.

Masse, Todd. (2006). *Homeland security intelligence: perceptions, statutory definitions, and approaches*. Washington, DC: Congressional Research Service.

National Commission on Terrorist Attacks upon the United States. (2004). *Final report of the National Commission on Terrorist Attacks upon the United States*. New York: W. W. Norton.

National Consortium for the Study of Terrorism and Responses to Terrorism. (2010). *Background report: Terrorist attacks in New York City*. College Park, MD: author.

National Consortium for the Study of Terrorism and Responses to Terrorism. (2015). *Annex of statistical information, country reports on terrorism 2014*. College Park, MD: author.

National Counterterrorism Center. (2011). *2010 NCTC report on terrorism*. Washington, DC. author.

New York State Intelligence Center. (2010). *The vigilance project an analysis of 32 terrorism cases against the homeland*. New York: author.

Norman, J. (2012). *Fire officers handbook of tactics* (4th ed.). Tulsa, OK: PennWell Corporation.

Pitts, D. (2008, January). Getting the 411. *Fire Chief*, 62–66.

Pfeifer, J. (2011, 3rd quarter). Revisiting the center for terrorism and disaster preparedness. *With New York Firefighters*, 10–13.

Pfeifer, J. (2012, October). Network fusion: information and intelligence sharing for a networked world. *Homeland Security Affairs, 8*, 1–20.

Regional Organized Crime Information Center. (2004). *Indicators of terrorist activity, stopping the next attack in the planning stages*. Retrieved from http://media.cygnus.com/files/base/OFCR/document/2012/01/terroristindicators_10619278.pdf.

Stewart, S. (2012, March 1). Detection points in the terrorist attack cycle. *STRATFOR, Security Weekly*. Retrieved October 20, 2013, from https://www.stratfor.com/weekly/detection-points-terrorist-attack-cycle

U.S. Army Training and Doctrine Command. (2007). *A military guide to terrorism in the twenty-first century*. Fort Leavenworth, KS: author.

U.S. Department of Homeland Security. (2005a). *Interim national preparedness goal*. Washington, DC: author.

U.S. Department of Homeland Security. (2005b). *National planning scenarios*. Washington, DC: Homeland Security Council.

U.S. Department of Homeland Security. (2006a). *Intelligence Enterprise Strategic Plan*. Washington, DC: author.

U.S. Department of Homeland Security. (2006b). *National planning scenarios: Attack timelines*. Washington, DC: author.

U.S. Department of Homeland Security. (2007). *National preparedness guidelines*. Washington, DC: author.

U.S. Department of Homeland Security. (2009a). *Emergency Service Sector Information and Intelligence Requirements Workshop after action report*. Emmitsburg, MD: National Emergency Training Center.

U.S. Department of Homeland Security. (2009b). *Fire service intelligence enterprise concept plan*. Emmitsburg, MD: author.

U.S. Department of Homeland Security. (2009c). *National infrastructure protection plan*. Emmitsburg, MD: author.

U.S. Department of Homeland Security. (2011a). *National preparedness goal* (1st ed.). Emmitsburg, MD: author.

U.S. Department of Homeland Security. (2011b). *Strategic national risk assessment in support of PPD 8: a comprehensive risk-based approach toward a secure and resilient nation*. Washington, DC: author.

U.S. Department of Homeland Security. (2014). *Overview of the national planning frameworks*. Washington, DC: author.

U.S. Department of Homeland Security, & U.S. Department of Justice. (2010). *Roll call release, opportunities to disrupt terrorist attack planning cycle*. Washington, DC: author.

U.S. Department of Justice. (2008). *Baseline capabilities for state and major urban area fusion centers*. Washington, DC: United States. Department of Justice, Global Justice Information Sharing Initiative.

U.S. Department of Justice, & U.S. Department of Homeland Security. (2005). *Fusion center guidelines*. Washington, DC. Retrieved October 20, 2014, from https://www.hsdl.org/?view&did=471518

U.S. Department of Justice, & U.S. Department of Homeland Security. (2010). *Fire service integration for fusion centers*. Washington, DC: U.S. Department of Justice.

U.S. Executive Office of President. (2011). National strategy for counterterrorism. Retrieved April 24, 2015, from https://www.hsdl.org/?view&did=776858

U.S. Federal Emergency Management Agency. (2009). *FEMA fact sheet: universal adversary program*. Retrieved April 24, 2015, from https://www.hsdl.org/?view&did=17901

U.S. Homeland Security Council. (2007). *National strategy for homeland security goal to prevent and disrupt terrorist attacks*. Retrieved November 20, 2014, from http://www.dhs.gov/national-strategy-homeland-security-october-2007

White House. (2003). Homeland security national presidential Directive 8: National preparedness. *Weekly Compilation of Presidential Documents, 39*(51), 1822–1826. Retrieved April 24, 2015, from https://www.hsdl.org/?view&did=441951.

White House. (2007). *National strategy for information sharing.* Retrieved November 10, 2014, from https://www.hsdl.org/?view&did=480495

Zuckerman, J, Bucci, S., & Carafano, J. (2013). *60 terrorist plots since 9/11: Continued lessons in domestic counterterrorism*. Special Report No. 137. Washington, DC: The Heritage Foundation.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California