



**NAVAL
POSTGRADUATE
SCHOOL**

MONTEREY, CALIFORNIA

THESIS

**TERRORISM PREVENTION AND FIREFIGHTERS:
WHERE ARE THE INFORMATION-SHARING
BOUNDARIES?**

by

Bryan Heirston

March 2009

Thesis Advisor:
Second Reader:

John Rollins
Christopher Bellavita

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.				
1. AGENCY USE ONLY		2. REPORT DATE March 2009	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE Terrorism Prevention and Firefighters: Where are the Information-Sharing Boundaries?			5. FUNDING NUMBERS	
6. AUTHOR(S) Bryan Heirston				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			12b. DISTRIBUTION CODE A	
13. ABSTRACT (maximum 200 words) The nation's one million firefighters are embedded in virtually every urban or rural area of the United States. Firefighters enter homes, businesses, vehicles, and other assets during emergency and non-emergency duties thousands of times each day in their efforts to prevent or respond to life and property loss. The unparalleled access that firefighters have to public and private locations puts them in a unique position to positively or negatively impact our nation's homeland defense and security information-sharing efforts. This thesis analyzes a number of information-sharing activities relating to terrorism and all-hazard strategies, policies, and programs in an attempt to identify whether U.S. fire personnel should participate in terrorism-related information sharing and—if they should participate—where the legal, political, and operational boundaries lie. The research identified a number of new strategic applications and tactical practices. The strategies and tactics are the result of comparing and contrasting legal compliance, political acceptability, target capabilities list linkage, operational impact, and cost factors of the current U.S. fire service information-sharing environment, the New York City Fire Department's Terrorism and Disaster Preparedness Strategy, the U.S. Fire Service's Intelligence Enterprise, and the United Kingdom's Civil Contingencies Act.				
14. SUBJECT TERMS Firefighters, Terrorism, Prevention, Response, Information Sharing, U.S. Fire Service, Homeland Security, New York City Fire Department Terrorism and Disaster Preparedness Strategy, U.S. Fire Service Intelligence Enterprise, Civil Contingencies Act, Legal, Operations, Cost, Political.			15. NUMBER OF PAGES 140	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

**TERRORISM PREVENTION AND FIREFIGHTERS: WHERE ARE THE
INFORMATION-SHARING BOUNDARIES?**

Bryan Heirston
Deputy Fire Chief, Oklahoma City Fire Department
B.S., Southern Nazarene University, 2001

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 2009**

Author: Bryan Heirston

Approved by: John Rollins, J.D.
Thesis Advisor

Christopher Bellavita, PhD
Second Reader

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

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The nation's one million firefighters are embedded in virtually every urban or rural area of the United States. Firefighters enter homes, businesses, vehicles, and other assets during emergency and non-emergency duties thousands of times each day in their efforts to prevent or respond to life and property loss. The unparalleled access that firefighters have to public and private locations puts them in a unique position to positively or negatively impact our nation's homeland defense and security information-sharing efforts. This thesis analyzes a number of information-sharing activities relating to terrorism and all-hazard strategies, policies, and programs in an attempt to identify whether U.S. fire personnel should participate in terrorism-related information sharing and—if they should participate—where the legal, political, and operational boundaries lie. The research identified a number of new strategic applications and tactical practices. The strategies and tactics are the result of comparing and contrasting legal compliance, political acceptability, target capabilities list linkage, operational impact, and cost factors of the current U.S. fire service information-sharing environment, the New York City Fire Department's Terrorism and Disaster Preparedness Strategy, the U.S. Fire Service's Intelligence Enterprise, and the United Kingdom's Civil Contingencies Act.

THIS PAGE INTENTIONALLY LEFT BLANK

We will build a national environment that enables the sharing of essential homeland security information. We must build a “system of systems” that can provide the right information to the right people at all times. Information will be shared “horizontally” across each level of government and “vertically” among federal, state, and local governments, private industry, and citizens.

-The President’s National Strategy for Homeland Security¹

¹ White House, *National Strategy For Homeland Security*, 56.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	TERMS AND DEFINITIONS	2
B.	WHY FIREFIGHTERS?	4
C.	RESEARCH QUESTION	5
	1. Overview of Legal, Moral and Ethical Considerations	6
	2. Future Research Efforts and Near Term Customers	7
D.	RESEARCH METHOD	7
E.	INFORMATION-SHARING FACTORS.....	8
	1. Legal Compliance.....	8
	2. Political Acceptability.....	10
	3. Target Capabilities Linkage.....	10
	4. Operational Impact.....	11
	5. Costs	11
F.	CONCLUSION	12
II.	LITERATURE REVIEW	15
III.	THE CURRENT FIRE SERVICE INFORMATION-SHARING ENVIRONMENT.....	23
A.	INFORMATION-SHARING EXAMPLES AND SCENARIOS.....	24
B.	TERRORISM INDICATORS	26
C.	OPERATIONAL AND CITIZEN TRUST ISSUES	27
D.	FIRE SERVICE INTELLIGENCE ENTERPRISE.....	30
E.	CURRENT FIRE SERVICE INFORMATION-SHARING FACTORS	32
	1. Legal Compliance.....	33
	2. Political Acceptability.....	33
	3. Target Capabilities Linkage.....	34
	4. Operational Impact.....	35
	5. Costs	35
F.	CURRENT FIRE SERVICE AND FSIE INFORMATION-SHARING MATRIX.....	36
G.	CONCLUSION	37
IV.	NEW YORK CITY FIRE DEPARTMENT TERRORISM AND DISASTER PREPAREDNESS STRATEGY	39
A.	ELEMENTS OF THE FDNY STRATEGY	40
	1. Evaluation Points	41
	2. Breaking Points	41
B.	INFORMATION-SHARING TACTICS	42
C.	RISK ASSESSMENT	44
D.	BUREAU OF FIRE INVESTIGATION.....	45

E.	COLLABORATION.....	46
F.	INTELLIGENCE GATHERING.....	47
G.	INTELLIGENCE DISSEMINATION.....	48
H.	FDNY STRATEGY INFORMATION-SHARING MATRIX.....	49
I.	FDNY STRATEGY INFORMATION-SHARING FACTORS.....	49
	1. Legality and Political Acceptability	50
	2. Target Capabilities Linkage.....	50
	3. Operational Impact.....	51
	4. Costs	52
J.	RECOMMENDATIONS.....	52
K.	CONCLUSION	53
V.	UNITED KINGDOM CIVIL CONTINGENCIES ACT OF 2004 (CCA).....	55
A.	ANALYSIS OF THE CCA.....	56
B.	THE CCA AND INFORMATION SHARING	57
C.	THE CCA PROCESS.....	59
D.	SHARING SENSITIVE INFORMATION.....	62
E.	EXAMPLES OF INFORMATION-SHARING UNDER THE CCA.....	64
F.	CCA INFORMATION-SHARING MATRIX	66
G.	CCA INFORMATION-SHARING FACTORS	66
	1. Legal Compliance.....	66
	2. Political Acceptability.....	68
	3. Target Capabilities Linkage.....	69
	4. Operational Impact.....	69
	5. Costs	70
H.	RECOMMENDATIONS.....	70
I.	CONCLUSION	73
VI.	ANALYSIS AND RECOMMENDATIONS.....	75
A.	ANALYSIS CRITERIA	76
B.	CURRENT U.S. FIRE SERVICE, FDNY, FSIE AND CCA INFORMATION-SHARING MATRIX	76
	1. Legal Compliance.....	76
	2. Political Acceptability.....	78
	3. Target Capabilities List Linkage.....	79
	4. Operational Impact.....	80
	5. Costs	81
C.	RECOMMENDATIONS.....	82
	1. Current Fire Service Information-Sharing and FSIE Recommendations	82
	2. FDNY Strategy Recommendations	84
	3. CCA Recommendations	85
D.	CONCLUSION	86

VII. STRATEGIC PLANNING TO IMPROVE INFORMATION-SHARING BETWEEN THE FIRE SERVICE AND HOMELAND SECURITY COMMUNITY	87
A. WHY STRATEGIC PLANNING?.....	87
B. CREATING THE PREFERRED FUTURE.....	90
1. Elimination	91
2. Reduction	92
3. Increase	92
4. Creation	92
5. Fire Service/Homeland Security Information-Sharing Tool	93
6. Fire Service Information-Sharing Power vs. Interest Grid	94
7. Planning Process	96
8. Guiding Coalition.....	98
C. DETERMINE WHERE WE ARE	98
D. IDENTIFYING POTENTIAL DESTABILIZING FORCES.....	99
E. DETERMINE WHERE WE WANT TO BE	100
F. DETERMINE HOW TO GET THERE	101
G. FIRE SERVICE INFORMATION-SHARING IMPLEMENTATION AND EVALUATION PHASES	104
VIII. CONCLUSION	105
BIBLIOGRAPHY	109
INITIAL DISTRIBUTION LIST	117

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1.	Current Fire Service and FSIE Information-Sharing Matrix	36
Figure 2.	FDNY Network-Centric Command System	44
Figure 3.	FDNY Strategy Information Sharing Matrix	49
Figure 4.	Target Capabilities List Linkage.....	51
Figure 5.	Information Request under the CCA	60
Figure 6.	Response to Information Requests under the CCA	61
Figure 7.	England’s Sensitive Information-Sharing System	63
Figure 8.	Information-Sharing Matrix for the CCA.....	66
Figure 9.	Information-Sharing Matrix.....	76
Figure 10.	Legal Compliance	76
Figure 11.	Political Acceptability.....	78
Figure 12.	Target Capabilities List Linkage.....	79
Figure 13.	Operational Impact.....	80
Figure 14.	Costs.....	81
Figure 15.	Fire Service/Homeland Security Information-Sharing Tool.....	93
Figure 16.	Fire Service Information-Sharing Power vs. Interest Grid	94

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The nation's one million firefighters are embedded in virtually every urban and rural area of the United States. Firefighters enter homes, businesses, vehicles, and other assets during emergency and non-emergency duties thousands of times each day in their efforts to prevent or respond to life and property loss. The unparalleled access that firefighters have to public and private locations puts them in a unique position to positively or negatively impact our nation's homeland defense and security information-sharing efforts. This thesis analyzes the current U.S. fire service information-sharing environment, the New York City Fire Department's Terrorism and Disaster Preparedness Strategy, the U.S. Fire Service's Intelligence Enterprise and the United Kingdom's Civil Contingencies Act of 2004 in an attempt to determine whether U.S. fire personnel should participate in terrorism-related information sharing and—if they should participate—where the legal, political, and operational boundaries lie. The research identified a number of new strategic applications and tactical practices. The strategies and tactics are the result of comparing and contrasting legal compliance, political acceptability, target capabilities list linkage, operational impact, and cost factors. The research produced three macro level findings, four information-sharing matrices, two strategic applications, and nine smart practices.

The first universal or macro-level finding indicates that U.S. firefighters have legal, moral, and ethical responsibilities to gather and share potential terrorist-related information that could assist the homeland security community in preventing and disrupting terrorist attacks. Second, these responsibilities must be conducted within the context of a two hundred fifty-year U.S. fire service enterprise founded on saving lives and property while maintaining exemplary trustworthiness, reliability, and credibility with the public. The third inclusive finding is that legal and operational issues may be addressed by firefighters using standardized terrorist indicators while operating as sensors of opportunity during emergency and non-emergency operations, but that fire personnel must not be specifically asked or assigned to gather information on suspected terrorists or terrorist activities.

The first strategic recommendation of this thesis is to modify the National Strategy for Information Sharing (NSIS) to include the fire service as an information-sharing partner in some situations. The second strategic recommendation presents a strategic information-sharing plan to enhance the current homeland security community and fire service ad hoc information-sharing environment.

The nine suggested smart practices are located in the chapter on analysis and recommendations and range from four common terrorist indicators that every firefighter should know to national U.S. guidance templates for formally requesting classified or sensitive information.

Possibly more important than all the findings, recommendations, plans, and smart practices identified in this thesis is the recognition of who firefighters are and what they can do to prevent or disrupt terrorism through information sharing. Since before the time of Fire Chief Benjamin Franklin, the fire service has been built on the legal, moral, and ethical commitment to protect U.S. citizens through prevention and response. The continued sporadic, unstructured information sharing of potential terrorist-related information is unacceptable. We are at war, and war calls for risks if we want to prevail. One of the risks of using fire personnel to collect information in plain sight is the tarnishing of our reputation or possible legal action. I propose that the risk is considerably less than dealing with the consequences of the attacks on the Murrah Building or the World Trade Center, or more horrendous acts of terrorism. We must continue to build on the U.S. fire service's long and successful history of prevention.

More than seven years ago the terrorist attacks of 9/11 became the catalyst for the U.S. expansion of information gathering and sharing with non-traditional partners such as the fire service. Now is the time for action. The significant value of fire personnel's prevention of life and property loss from terrorism through the use of standardized terrorist indicators and formalized collaboration with the homeland security community should not be underestimated. The one million U.S. fire personnel serving in over thirty thousand fire departments may be a phenomenal resource for our homeland security partners, and our homeland security partners could be a valuable resource for firefighters.

If the strategic and operational recommendations identified in this thesis are implemented by the nation's fire personnel, the volume of suspicious-activity reporting should increase and with it the potential for the prevention or disruption of future terrorism in the United States. Citizens will be safer and, in my opinion, will appreciate their firefighters stepping up as they have historically done to prevent life and property loss in our country. The terrorist beat us on at least two days, April 19, 1995, and September 11, 2001. We should not let this happen again because we do not choose to overcome our information-sharing challenges.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This thesis leverages smart practices, as well as several new ideas that were born out of the loss of life from acts of terrorism or natural disasters at local, national, and international levels. It is my hope that the recommendations and strategic management of change identified in this project will be given serious consideration by policy groups, administrators, managers, and operations personnel through out the homeland security community in an effort to lessen or eliminate future loss of life and to encourage others to further study this issue.

I would like to recognize those who made this thesis a reality: first and foremost God, in whom we trust; second, my wife, Linda, and children, Alex and Sam, who sacrificed many nights and weekends so that I could work on this project; Oklahoma City Fire Chief and friend, Keith Bryant, for believing in me and granting me the time to attend the Naval Postgraduate School; my thesis advisor, John Rollins, for his wise counsel to construct a thesis that is more than an academic assignment; and Chris Bellavita, for encouraging me to think in non-traditional ways about the value of firefighters as collectors, consumers, and collaborators of potential terrorist-related information. Thank you.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The role of the fire service in preventing terrorism through information sharing with local, state, and federal homeland security partners is not clear.² The *9/11 Commission Report* described the failure of the intelligence community to “connect the dots” that may have prevented the terrorist attacks on September 11, 2001.³ The purpose of this thesis is to identify the level of firefighter involvement in the collection, dissemination, and consumption of potential terrorist information in order to “connect the dots” before the next major attack in the United States. The current information-sharing environment, one local U.S. strategy, a U.S. national concept, and the United Kingdom’s Civil Contingencies Act are analyzed and qualitatively compared to each other and the current fire service–homeland security information-sharing environment. The recommendations range from local tactical through national strategic actions for the U.S. fire service.

Over six years have passed since the release of the *National Strategy for Homeland Security*, yet little progress has been made toward solving the Gordian knot of information sharing between the U.S. fire service’s more than 1 million fire personnel and the homeland security community.⁴ Unfortunately, we cannot simply cleave the knot in two. We must rely on a variety of skills ranging from strategic and policy expertise to

² In the fall of 2007, I met with Oklahoma City Fire Chief Keith Bryant to discuss potential thesis topics that would benefit the Oklahoma City Fire Department and the Department of Homeland Security (DHS). In a broader context we also considered contemporary fire service and homeland security issues. Chief Bryant had recently returned from a Metropolitan Fire Chiefs Association conference in which homeland security issues had been considered. We discussed the current homeland security prevention, protection, response, and recovery missions as they relate to traditional fire service prevention and response missions. Chief Bryant indicated that he and other fire chiefs of metropolitan-size fire departments were inquiring about their departments’ role in an emerging all-hazards homeland security culture.

³ National Commission, *9/11 Commission Report*, 426.

⁴ U.S. Office of the Director of National Intelligence, *Information Sharing*, 10. “For the purposes of the ISE IP, the term “homeland security community” includes the Department of Homeland Security and those agencies with public health and welfare, emergency response, transportation, fire, and emergency management.” It should be noted that the only reference to “fire” or “homeland security community” in the 123-page document is a footnote on page 10.

the most fundamental tactical skill, in order to develop horizontal and vertically oriented policies, strategies, and tactics to identify and share potential terrorist-related information and intelligence.⁵

A. TERMS AND DEFINITIONS

There has been, and continues to be, considerable ambiguity among the homeland security community regarding what is homeland security.⁶ Christopher Bellavita, in his article “Changing Homeland Security: What is Homeland Security?” indicated, “There are at least seven different definitions of homeland security.”⁷ For the purposes of this thesis, the terms “homeland security community” or “homeland security partners” are defined based on the Office of the Director of National Intelligence, *Information Sharing Environment Information Sharing Plan*: “The term ‘homeland security community’

⁵ White House, *National Strategy For Homeland Security*, 56. The national vision for Homeland Security is that “we will build a national environment that enables the sharing of essential homeland security information. We must build a ‘system of systems’ that can provide the right information to the right people at all times. Information will be shared ‘horizontally’ across each level of government and ‘vertically’ among federal, state, and local governments, private industry, and citizens. With the proper use of people, processes, and technology, homeland security officials throughout the United States can have complete and common awareness of threats and vulnerabilities as well as knowledge of the personnel and resources available to address these threats. Officials will receive the information they need so they can anticipate threats and respond rapidly and effectively. The incorporation of data from all sources across the spectrum of homeland security will assist in border management, critical infrastructure protection, law enforcement, incident management, medical care, and intelligence. In every instance, sensitive and classified information will be scrupulously protected. We will leverage America’s leading-edge information technology to develop an information architecture that will effectively secure the homeland.”

⁶ Bellavita, “Changing Homeland Security,” Regarding the definition of homeland security, Dr. Bellavita indicates that “the argument has been made that a single definition would be desirable and beneficial for a number of reasons, mostly having to do with efficiency and effectiveness criteria. But there is no one authority that can command everyone to use language the same way. Other important and often used terms—like terrorism, justice, disaster, or emergency management—also do not have single definitions. Yet we make progress in understanding and using each of those ideas. The absence of agreement can be seen as grist for the continued evolution of homeland security as a practice and as an idea. Even if people did agree to define homeland security with a single voice, there would still be the matter of behavior. What people, organizations, and jurisdictions do is as instructive as what they say.”

⁷ Ibid.

includes the Department of Homeland Security and those agencies with public health and welfare, emergency response, transportation, fire, and emergency management responsibilities.”⁸

The term “information sharing,” within the framework of this thesis, is based on the Homeland Security Act of 2002, which defines homeland security information as “any information possessed by a federal, state, or local agency that (a) related to the threat of terrorist activity, (b) relates to the ability to prevent, interdict or disrupt terrorist activity, (c) would improve the identification or investigation of a suspected terrorist or terrorist organization; or (d) would improve the response to a terrorist act.”⁹ The terms “fire personnel, firefighter or fire service” include the functions of “firefighting, emergency medical services, technical rescue, hazardous materials operations, aviation operations, marine operations, fire prevention activities, fire inspections, fire investigations and fire communications.”¹⁰

The term “information sharing or intelligence” is defined as

All-hazard information that has been gathered and vetted through the intelligence cycle in order to generate products that can be used to guide Fire Service decisions at the strategic, operational, and tactical levels. Also information provided by the Fire Service to the intelligence community to support the production of finished intelligence products.¹¹

⁸ U.S. Office of the Director of National Intelligence, *Information Sharing*, 10. “For the purposes of the ISE IP, the term “homeland security community” includes the Department of Homeland Security and those agencies with public health and welfare, emergency response, transportation, fire, and emergency management.” It should be noted that the only reference to “fire” or “homeland security community” in the 123-page document is a footnote on page 10.

⁹ Masse, “Homeland Security Intelligence,” See P.L. 107-296, Sec. 892(f). The House Committee on Homeland Security clarified homeland security information within a terrorism framework. Under Rule IV, Subcommittees, it defines the jurisdiction of the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment as being, in part, “intelligence and information sharing for the purpose of preventing, preparing for, and responding to potential terrorist attacks on the United States; the responsibility of the Department of Homeland Security for comprehensive, nationwide, terrorism-related threat, vulnerability, and risk analyses; the integration, analysis, and dissemination of homeland security information, including the Department of Homeland Security’s participation in, and interaction with, other public and private entities for any of those purposes.” Masse goes on to provide the following reference: “Committee on Homeland Security, U.S. House of Representatives, Rules and Appendix for the Committee on Homeland Security, Committee Print 109-B, Oct. 2005.”

¹⁰ U.S. Homeland Security Act 2002.

¹¹ U.S. Department of Homeland Security, Office of Intelligence and Analysis, State and Local Program Office, “Fire Service Intelligence Enterprise – Executive Briefing,” 3.

For the purposes of this thesis, the term "all-hazards" refers to "domestic terrorist attacks, natural disasters, and other emergencies."¹²

B. WHY FIREFIGHTERS?

Fire service information sharing and collaboration may be at the beginning stage of future homeland security partnerships, if one considers that the United States has over one million firefighters serving in over thirty thousand fire departments that respond to over twenty-four million emergencies annually.¹³ Firefighters enter homes, businesses, vehicles, and other assets during emergency and non-emergency duties thousands of times each day in their efforts to prevent and respond to life and property loss. This access allows them to identify potential terrorist activities, oftentimes unexpectedly for both the firefighters and the potential terrorists. The unparalleled interface that firefighters have with public and private locations puts them in a unique position to positively or negatively impact our homeland security information-sharing efforts.

Information sharing between the fire service and the homeland security community is important for at least two reasons. The first reason relates to legal issues. The unprecedented access that firefighters gain onto or into private property places them in a unique position to gather potential terrorist-related information for the prevention or disruption of terrorist attacks before they occur, but firefighters must be cognizant of activities and actions that may result in civil rights violations of the people they have been given the honor to serve. The second reason relates to policy and operational information-sharing issues. Since 9/11 more citizens, government, private sector, and other non-traditional intelligence community actors are being encouraged to report suspicious behaviors or circumstances. Despite the obvious potential benefit of sharing information, a number of policy and operational challenges must be addressed. For example there are issues relating to firefighters as consumers of intelligence and

¹² U.S. Homeland Security Presidential Directive HSPD-8.

¹³ National Fire Protection Association, *The United States Fire Service*, 1; U.S. Fire Administration, *Fire Departments*, 1.

information in preparation for and in response to potential terrorist incidents at specific locations or special events. What policies and procedures are necessary for non-traditional information sources such as firefighters as producers and consumers of open source and, in some cases, classified information? Also, few firefighters have received formal training in what terrorist indicators to look for and how to communicate the information efficiently.

C. RESEARCH QUESTION

What homeland security strategies, policies, and programs may be used to assist fire departments and the homeland security community in the identification and sharing of information about potential terrorist activities?¹⁴ The findings of this thesis indicate that firefighters may have legal, moral, and ethical responsibilities to gather and share potential terrorist-related information that could assist the homeland security community in preventing and disrupting terrorist attacks. These responsibilities must be conducted within the context of a 250-year U.S. fire service enterprise of working together to save lives and property while maintaining exemplary credibility with the public. Legal applicability of reporting observations collecting and sharing information must be adhered to, not only to reduce legal exposure, but also to lessen or prevent tarnishing the fire service reputation of trustworthiness and reliability. Legal and operational issues may be addressed by firefighters using uniform terrorist indicators that do not detract from their primary mission or violate the customer's legal rights.

This thesis identifies a number of smart practices from local, national, and international fire service strategies and governmental actions. Using qualitative criteria, thought was given to local, national, and international smart practices, gaps, and potential blind spots applicable to the U.S. fire service information-sharing environment using the

¹⁴ U.S. Homeland Security Council, National Strategy for Homeland Security Goal to Prevent and Disrupt Terrorist Attacks, 15. "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." One barrier is the lack of consistent, basic, potential terrorism-related information collection, sharing, and feedback guidelines for the fire service. The lack of guidelines may create an environment where critical information to prevent or disrupt terrorist activities is not identified or effectively communicated to the intelligence community for inclusion into the intelligence cycle.

following criteria. Consideration was given to the legal, political, governance, effectiveness and costs aspects for the four information-sharing options.

The nation's more than one million firefighters are embedded in virtually every community in the United States, and they routinely operate in public and on private property, in emergency and non-emergency environments with little or no warning. Oftentimes firefighters live and work in the same neighborhoods, districts, or communities for twenty years or more. Their responsibility to enter a property at any time for the good and welfare of the people places them in a position to witness "the thousands and thousands of routine, everyday observations and activities" of which Secretary Chertoff spoke.¹⁵

1. Overview of Legal, Moral and Ethical Considerations

The legal, moral, and ethical limits associated with firefighters' gathering and sharing potential terrorism information has produced various opinions about what, if any, terrorist information collection firefighters should be involved with. For example, since the fall of 2007, there have been several media stories as well as discussions among the National Postgraduate School Master's of Homeland Security 0705/0706 Cohorts regarding fire department participation in terrorism prevention activities, particularly the fire service role in information collection, dissemination, and participation in fusion centers. The media reports and cohort discussions have resulted in a wide range of opinions about what fire departments are doing or should be doing to prevent terrorism. Keith Olberman's interview with Mike German on MSNBC's *Countdown*, is one example. Mike German, a former FBI agent who was the national security policy counsel to the ACLU, indicated that the traditional role of firefighters is for life safety and property conservation—not intelligence collection for the homeland security community.¹⁶

¹⁵ Chertoff, Remarks at the 2006 Bureau of Justice Assistance, March 14, 2006.

¹⁶ Olberman, Interview with Mike German. Mike German is a former FBI agent who is now national security policy counsel to the ACLU. See also National Terror Alert Response Center, "Firefighters to Help In Fight Against Terrorism."

Several court cases have indicated that warrants or consents are not required for entry by firefighters as long as there are emergency or exigent circumstances present, and any evidence acquired during fire origin-and-cause determination should be reported.¹⁷

Fire personnel access appears to place firefighters in a position to identify terrorist activities or information in plain sight. Further discussion of the legal, moral, and ethical issues relating to the authority of firefighter participation in information sharing during emergency and non-emergency activities is discussed in later chapters.

2. Future Research Efforts and Near Term Customers

For many years it has been a common practice in U.S. fire departments to informally share information relating to potential illegal activities with the law enforcement community. This collaboration has occurred during emergency and non-emergency operations. A fire service-wide policy for terrorism information collection and sharing may be a logical extension of historical law enforcement and fire department information-sharing relationships. This thesis may assist future efforts in the area of information collection and sharing among non-traditional homeland security partners.

Regarding benefactors of this thesis, the immediate and primary consumers are the U.S. fire service and the Department of Homeland Security (DHS), based on a mission of preventing and mitigating life and property loss through information sharing.

D. RESEARCH METHOD

The qualitative methodology utilized in this thesis project was intended to identify and illuminate benefits and detriments by eliminating options that are clearly weaker in terms of legality, political acceptability, target capabilities list linkage, operational impact, and costs. The results of this thesis reflect recommendations to assist U.S. fire departments and their information-sharing partners in the identification, dissemination, and consumption of potential terrorist-related information. Recommendations are based on the gaps between the current U.S. fire service–homeland security information-sharing environment and the smart practices from local, national, and international sources.

¹⁷ *Michigan v. Tyler*, 436 U.S. 499 (1978); *Michigan v. Clifford*, 464 U.S. 287 (1984).

The national effort to enhance homeland security through information sharing with the fire service may result in considerable benefits and involve relatively small financial and other costs. The most significant benefits of information sharing are reduction in the risk of terrorist attacks and enhanced preparedness of firefighters. Other benefits include reduction in the effects of unintentional manmade disasters such as hazardous materials releases, as well as improved natural disaster mitigation, response, and recovery operations.

E. INFORMATION-SHARING FACTORS

The factors used to compare and contrast the four information-sharing options (current fire service, FDNY Strategy, FSIE and CCA) are described below. Each of the four information-sharing options examined for this thesis is analyzed based on five factors and graphically represented by an information-sharing matrix. The five factors measured are legal compliance, political acceptability, target capabilities linkage, operational impact, and cost.

1. Legal Compliance

The four information-sharing options were considered for compliance with legal rulings as they relate to entry onto or into property by firefighters during emergency and non-emergency operations. The cases regarded as applicable for fire personnel collecting potential terrorist information were: *Michigan v. Tyler*, 436 U.S. 499 (1978); *Michigan v. Clifford*, 464 U.S. 287 (1984); and *Camara v. Municipal Court of the City and County of San Francisco*, 387 U.S. 523 (1967), as well as the Homeland Security Act 2002,

Subtitle I—Information Sharing.¹⁸ The definitions of Homeland Security Intelligence and Information may help clarify legal compliance. In an attempt to define homeland security intelligence, Todd Masse in his Congressional Research Service, Report for Congress “Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches” stated:

Homeland security intelligence could likely be defined as a more refined and finished version of homeland security information. The nexus to terrorism and terrorist-related events is direct and compelling. One complication of discerning what is homeland security information remains how the investigator or operator knows that the activity which they are investigating or monitoring is related to terrorism.... Given that there are substantial national and homeland security penalties for not sharing homeland security intelligence, at least at the policy level and to some extent at the operational level, arguably there is now a bias in favor of sharing raw intelligence across levels of government more quickly than in the past. The extent to which this information is shared systematically is an open question.¹⁹

Masse went on to say that:

The primary statutory definition that applies is that which appears in the Homeland Security Act of 2002, which defines homeland security information as any information possessed by a federal, state, or local agency that (a) related to the threat of terrorist activity, (b) relates to the ability to prevent, interdict or disrupt terrorist activity, (c) would improve the identification or investigation of a suspected terrorist or terrorist organization; or (d) would improve the response to a terrorist act.²⁰

¹⁸ “The basic purpose of the Fourth Amendment, which is enforceable against the States through the Fourteenth, through its prohibition of ‘unreasonable’ searches and seizures is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials,” *Camara*, 387 U.S. at 528. “(1) Under procedures prescribed by the President, all appropriate agencies, including the intelligence community, shall, through information sharing systems, share homeland security information with Federal agencies and appropriate State and local personnel to the extent such information may be shared, as determined in accordance with subsection (a), together with assessments of the credibility of such information. (2) Each information sharing system through which information is shared under paragraph (1) shall— (A) have the capability to transmit unclassified or classified information, though the procedures and recipients for each capability may differ; (B) have the capability to restrict delivery of information to specified subgroups by geographic location, type of organization, position of a recipient within an organization, or a recipient’s need to know such information; (C) be configured to allow the efficient and effective sharing of information; and (D) be accessible to appropriate State and local personnel.” U.S. Homeland Security Act 2002.

¹⁹ Masse, “Homeland Security Intelligence,” 12.

²⁰ *Ibid.*

Masse attempts to clear up the ambiguity with the following: “Although the DHS remains an organization designed to protect against ‘all Hazards,’ the focus of homeland security information, at least as defined in law, is counterterrorism.”²¹

Masse’s comments may reinforce the idea of enhancing fire service information sharing with the DHS through a systematic approach based on the philosophy that involves firefighters as sensors of opportunity, within the scope of their normal or primary duties.

Firefighters may have a legal right and responsibility to collect and share potential terrorist-related information if the information is in plain sight during the course of their duties. Firefighters may enter homes, businesses, vehicles, and other assets without warrants to prevent and respond to potential life and property loss. They should legally identify potential terrorist activities or information in plain sight while performing their assigned emergency and non-emergency duties. The court rulings do not allow for “arbitrary invasions” or “unreasonable searches and seizures” by fire personnel.

2. Political Acceptability

For this thesis, “political acceptability” refers to policy-level support. The decision makers generally considered were formal policy groups accountable for the strategy, concept of operations or act. Examples could be local, state, or national governing bodies accountable for the strategy or act. In some circumstances consideration was given to labor representatives, such as the International Association of Firefighters or the ACLU, that might have significant influence and interest in the political acceptability of the strategy, act, or current information-sharing environment.

3. Target Capabilities Linkage

In 2004, DHS released fifteen National Planning Scenarios.²² The National Planning Scenarios listed and explained the hazards and risks associated with high-

²¹ Masse, “Homeland Security Intelligence,” 13.

²² U.S. Department of Homeland Security, National Planning Scenarios.

impact events that would significantly affect local emergency-response capabilities. The capabilities identified in the planning scenarios resulted in thirty-six target capabilities within four mission areas (prevention, protection, response, and recovery). The criteria for this thesis relied on four of the nine “prevention target capabilities” listed in the *DHS National Preparedness Guidelines*.²³ The four target capabilities were selected due to their correlation to information sharing.²⁴ The four target capabilities were:

- Intelligence/information-sharing and dissemination;
- CBRNE detection;
- Information gathering and recognition of indicators;
- Warnings, intelligence analysis, and production.

4. Operational Impact

How the current fire service information-sharing environment, Strategy or CCA would influence the operation of the homeland security information-sharing community was measured initially by collecting key indicators of success, such as those identified in the documents themselves and in some cases post-product analysis.

5. Costs

The United States spends approximately \$100 billion per year on homeland security.²⁵ Homeland security expenses include federal, state, and local law enforcement, and emergency medical, public works, and fire services, but excluded most funding for the armed forces.²⁶ Generally speaking, the national effort to enhance homeland security through information sharing with the fire service appears to involve some relatively small fiscal costs. Costs include the human resources the fire service and homeland security communities have committed specifically to information sharing. Most costs appeared to

²³ U.S. Department of Homeland Security, *National Preparedness Guidelines*, 4.

²⁴ *Ibid.*

²⁵ White House, *National Strategy for Homeland Security*, xxii.

²⁶ *Ibid.*

be “soft costs” absorbed by current fire and intelligence personnel responsible for the collection, analysis, and dissemination of information.

F. CONCLUSION

While intelligence gathering, collaboration, and dissemination is not new, the awareness of how fire service information sharing might enhance national, state, and local security has become an issue since late 2001. The current fire service information-sharing analysis conducted for Chapter III is based predominately on post-9/11 data and attempts to incorporate academic, speculative, and experiential sources. It should be noted that the information on fire service–homeland security participation and potential conceptual models is limited but appears to be growing, especially within the Department of Homeland Security, fusion centers, and larger metropolitan fire departments.

Chapter IV identifies the *Terrorism and Disaster Preparedness* FDNY Strategy (FDNY Strategy) information-sharing smart practices to improve safety and effectiveness in a post-9/11, multifaceted, all-hazards threat environment. According to the 9/11 Commission, the lack of information sharing on 9/11 may have resulted in unwarranted fatalities for civilians, firefighters, and other responders in New York City. “Information that was critical to informed decision making was not shared among agencies. FDNY Chiefs in leadership roles that morning have told us their decision making capability was hampered by lack of information from NYPD aviation.”²⁷

At the international level, a review of Canada, Australia, Israel, and the United Kingdom’s terrorism information-sharing environment related to the fire service and their homeland security partners resulted in the identification of one applicable information-sharing legislative action, the United Kingdom’s Civil Contingencies Act of 2004 (CCA). The CCA is the product of a legislative evolution that began with the United Kingdom’s Emergency Powers Act of 1920, continued with the 1948 Civil Protection Act, and the fuel crisis, the foot-and-mouth outbreak, and World Trade Center attacks that occurred in

²⁷ National Commission, *9/11 Commission Report*, 321.

2001. Chapter V of this thesis provides the results of a qualitative comparison of the CCA in relationship to the current U.S. fire service information-sharing environment.

In constructing the recommendations in Chapter VI, a local-to-international approach was used to compare and contrast information sharing between the fire service and other alliances. The fundamental qualitative premise was that there were—and are—lessons to be learned by the U.S. fire service from the current international, national, and local information-sharing partnerships. Chapter VI analyzes and consolidates the value of contemporary smart practices identified in Chapters III through V.

The final chapter of this thesis offers a road map for increased information sharing by combining traditional strategic planning approaches such as those found in *Strategic Planning for Public and Nonprofit Organizations* with emerging strategic planning systems such as *The Blue Ocean Strategy* and *The Starfish and the Spider*.²⁸

²⁸ Bryson, *Strategic Planning for Public and Nonprofit Organizations*; Kim and Mauborgne, *Blue Ocean Strategy*; Brafman and Ceckstrom, *The Starfish and the Spider*.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

The literature relating to the role of the fire service in prevention is almost exclusively recent and emerging. The terrorist attacks of 9/11 appear to be the catalyst for expansion of the idea of information-sharing policies with non-traditional partners such as fire departments. In most countries, including the United States, the value of the fire service in preventing life and property loss from terrorism through informal and formal collaboration with the homeland security community is yet to be determined at the national, state, and most local levels. Some of the information-sharing literature reviewed identifies value for the firefighters participating in information-sharing, while other literature was silent on the issue. In those documents supporting a fire service role in information sharing, firefighters were seen as significant force-multipliers in the effort to prevent and disrupt terrorist attacks.

In the United States there has been a growing number of policies, programs, and media stories regarding fire department participation in terrorism prevention activities, particularly the fire service role as collectors, disseminators, and consumers of potential terrorist-related information, as well as firefighter participation in fusion centers.²⁹ The media reports and policies have resulted in a wide range of opinions about what, if any, information-sharing activities fire departments are doing or should be doing to prevent terrorism. Awareness of how the U.S. fire service may or may not enhance terrorism prevention is not apparent.

This literature review was organized around the idea of the U.S. fire service's sharing information for the prevention of terrorism. Consideration was given to the type of organizations (local, state, national, and international) that might assist in defining what role the fire service has in the homeland security information-sharing community. The information on fire department homeland security participation and potential conceptual models is limited but appears to be growing, especially within DHS and larger metropolitan fire departments.

²⁹ Olberman. Interview with Mike German. See also National Terror Alert Response Center, "Firefighters to Help In Fight Against Terrorism," and Miller, Andrew Miller Center for Homeland Security and Defense "More Media Reaction to FIRE-INT (Intel gathered by Fire/Rescue)" thread.

In late 2002 President Bush commissioned the National Commission on Terrorist Attacks upon the United States (also known as the 9/11 Commission). The 9/11 Commission's Final Report included recommendations designed to guard against future attacks. One recommendation involved unity of effort. The following excerpt may have application to the role of the fire service in sharing information with the intelligence community:

National intelligence is still organized around the collection disciplines of the home agencies, not the joint mission. The importance of integrated, all source analysis cannot be overstated. Without it, it is not possible to "connect the dots." No one component holds all the relevant information.³⁰

On December 17, 2003, President George W. Bush released Homeland Security Presidential Directive 8 "*National Preparedness*" (HSPD-8).³¹ The intent of HSPD-8 was to:

Establish 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 by requiring a national domestic all-hazards preparedness goal, establishing mechanisms for improved delivery of Federal preparedness assistance to State and Local governments, and outlining actions to strengthen preparedness capabilities of Federal, State, and Local entities (emphasis added).³²

In the fire service, successful prevention has eliminated or mitigated many emergency responses. As the Oklahoma City Fire Marshal responsible for fire prevention services, it is my view that when a fire vehicle leaves the station responding to an emergency call, it is due to a gap in our prevention efforts. Successful fire and life loss-prevention missions require a unity of effort from a diversified cadre of citizens, federal, state, local, private, and public partners working together and sharing information to reduce life and property loss. The losses can be reduced through engineering controls and

³⁰ National Commission, *9/11 Commission Report*, 426.

³¹ U.S. Department of Homeland Security, Interim National Preparedness Goal, 3.

³² U.S. Homeland Security Presidential Directive HSPD-8, 1.

behavioral changes founded on an expectation of personal responsibility and sharing of information between all parties over an extended period of time. In the case of fire prevention in the United States, the time period has been hundreds of years. Unfortunately, in the current terrorism environment we do not have the luxury of decades or centuries to build the coalitions necessary to create the preferred future, so we must leverage all our assets to lessen or eliminate the terrorist threat now.

In October 2007, almost four years after HSPD-8, the *National Strategy for Information Sharing (NSIS)* was released. The *NSIS* helped to clarify the trend in the United States to collaborate with non-traditional human-intelligence partners.

The Intelligence Community will continue to be a primary source for this information; however, the Intelligence Community must modify its processes and procedures to encompass non-traditional customers at all levels of government with roles in prevention and response. In addition, important information regarding possible attack planning may come from organizations outside the Intelligence Community. Our challenge is to ensure that information from all sources is brought to bear on our efforts to protect our people and infrastructure from terrorist attacks.³³

The same month that the *NSIS* was released, the Homeland Security Council's *National Strategy for Homeland Security* was distributed.³⁴ The National Security Council's *Strategy* also supported the idea of collaboration with non-traditional partners as exemplified in the following statement:

State, Local, and Tribal governments, which best understand their communities and the unique requirements of their citizens, provide our first response to incidents through law enforcement, fire, public health, and emergency medical services. They will always play a prominent, frontline role in helping to **prevent** terrorist attacks as well as in preparing for and responding to a range of natural and man-made emergencies (emphasis added).³⁵

³³ National Security Council, *National Strategy for Information Sharing*, 10.

³⁴ U.S. Homeland Security Council, *National Strategy for Homeland Security*, 4.

³⁵ *Ibid.*

Firefighters and fire stations are located in virtually every community in the United States. Most fire departments are staffed by volunteers, and I suggest that those volunteers as well as most paid fire personnel understand their communities and the unique requirements of their citizens.

The homeland security community and “first responders” appear to have accepted the traditional role of fire departments in *response* to terrorist attacks.³⁶ What is not as clear is the fire service role, in the *prevention* of terrorist attacks in accordance with various presidential directives and national strategies.

Major fires throughout history have destroyed whole cities and caused massive loss of life and property. Solutions were devised that have gradually, over several hundred years, reduced the danger to a level that allows us to co-exist with the threat of fire by applying constant vigilance and investments in fire protection, but without living in constant fear and dread from fire. In their paper “The War on Terrorism and What We Can Learn from the War on Fire,” John Whitely and Gerold Yonas state “Prevention is the holy grail of our terrorism protection plan just as prevention is the key to our fire protection plan...we have created a multi-pronged approach to fire protection that involves both government and individuals in the prevention, mitigation, and response to fires.”³⁷ An example of terrorism protection that involved both government and people is the “See Something, Say Something” campaign. In March of 2003, the New York City Metropolitan Transit Authority (MTA) developed and implemented a program called “If You See Something, Say Something” to encourage transit passengers to report suspicious

³⁶ Department of Homeland Security, Interim National Preparedness Goal; U.S. Homeland Security Presidential Directive HSPD-8. “The term ‘first responder’ refers to those individuals who in the early stages of an incident are responsible for the protection and preservation of life, property, evidence, and the environment, including emergency response providers as defined in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101), as well as emergency management, public health, clinical continued, care, public works, and other skilled support personnel (such as equipment operators) that provide immediate support services during prevention, response, and recovery operations.”

³⁷ Whitely and Yonas, *The War on Terrorism*, 3-9.

activities and help in the prevention or disruption of terrorist activities. The program yielded 1,944 tips in 2006 and has been adopted by transit systems worldwide.³⁸

An example of a fire department that is active in terrorism prevention is the New York City Fire Department (FDNY). According to FDNY Fire Commissioner Nicholas Scoppetta, the FDNY is working cooperatively with the homeland security community. The FDNY Bureau of Fire Investigation is linked to the New York State Office of Public Security Counter Terrorism Network System and participates with the Joint Terrorist Task Force and the Metropolitan Committee on Counter Terrorism. The FDNY revised the way they process missing or stolen property so that the NYPD Intelligence Bureau and the FBI are now notified immediately. Other cooperative efforts include participation in the compilation of the City's Vulnerable Location Database and reporting of potentially suspicious toxic substances. Commissioner Scoppetta indicated, "There is more we can do and will do. Although our responders are not law enforcement personnel, they can, by the nature of their work, gather valuable information."³⁹

Information sharing among disciplines within the New York City Emergency Services Sector also appears to be growing, as exemplified by the following October 9,

³⁸ New York State Metropolitan Transit Authority, "If You See Something, Say Something." The program is based on a multi-media public education campaign that encourages users of the MTA's transportation network to call an NYPD hotline or tell an MTA employee if they see anything suspicious. According to Elliot G. Sander, MTA Executive Director and CEO, "The 'See Something, Say Something' campaign is a phenomenally successful component of the MTA's comprehensive security strategy.... We are proud that our customers play such an active role in keeping the system safe, and I am not surprised that the campaign has been copied around the world, from Chicago to Amsterdam. Keeping our customers safe remains the MTA's top priority." MTA Director of Security William A. Morange indicated, "It is impossible for the police departments to be everywhere and see everything. Our passengers extend our reach and—by sharing their information—make the system safer." The program reminds passengers to contact authorities if any of the following are noticed: "Be alert to unattended packages. Be wary of suspicious behavior. Take notice of people in bulky or inappropriate clothing. Report exposed wiring or other irregularities. Report anyone tampering with surveillance cameras or entering unauthorized areas. Learn the basics of safe train evacuation at www.mta.info."

³⁹ National Commission, *9/11 Commission Report*, 26-27.

2008 *Watchline* excerpt that was shared between the fire, police, and other departments.⁴⁰

Routine Call Uncovers Possible Terrorist “Nest” – Police officers were investigating a suspected identity thief, but instead uncovered terrorist-related materials that include copied identifications, al-Qaeda news clippings, literature on purchasing and processing chemicals, laboratory glassware catalogs and a survival book titled the *Hostile Planet: The Essential Guide to Surviving Natural Disasters, Pandemics and Terrorist Attacks*. Recommendation: Remember the FDNY remains on the frontlines in the War on Terror. Members should be aware of this new global threat environment and potential implications. Evidence of this is the recent arrest of a computer programmer in India who is accused of being a terrorist organizations media officer, reportedly traveling to the U.S. frequently for his employer without arousing any suspicions.

In an effort to increase information collection to share with the homeland security community, Commissioner Scoppetta pointed out, “We are in the process of creating a curriculum that incorporates terrorism recognition awareness for all Firefighters and EMS personnel.”⁴¹ Chapter IV of this thesis analyzes the FDNY Terrorism and Disaster Preparedness Strategy for applicability in identifying the role of the fire service in preventing terrorism through information sharing with local, state, and federal homeland security partners.⁴²

⁴⁰ Fire Department City of New York, “*Watchline*.” *Watchline* distribution is for official use only and intended for “law enforcement, EMS personnel, firefighting personnel, security personnel, antiterrorism personnel and intelligence personnel. Further dissemination should be limited to a minimum, consistent with the purpose of supporting effective law enforcement and security of installation personnel, equipment and facilities. The *Watchline* is not to be furnished to the media or any other agencies outside of law enforcement. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C 552) and/or the Freedom of Information Law (New York Public Officers Law, Sections 87 & 89).”

⁴¹ Scoppetta, Testimony before the National Commission on Terrorist Attacks upon the United States, 26-27.

⁴² Fire Department City of New York, “Terrorism.”

At the national level, DHS Secretary Michael Chertoff made public an arrangement to include firefighters in fusion centers.⁴³ Chertoff indicated that the National Operations Center includes a fire service representative who works with officials from organizations such as the FBI, other law enforcement agencies, and the intelligence community, and that Charlie Allen, the DHS assistant secretary for intelligence and analysis, “is working to add firefighter personnel to state and local fusion centers.” Chertoff added, “Fusing firefighters and responders into the normal law enforcement and Counterterror Intelligence Fusion Center is critical to get a whole picture of what’s going on.” Referring to intelligence as a means of providing early warning of terrorist attacks, Secretary of Homeland Security Michael Chertoff stated:

Intelligence, as you know, is not only about spies and satellites. Intelligence is about the thousands and thousands of routine, everyday observations and activities. Surveillance, interactions—each of which may be taken in isolation as not a particularly meaningful piece of information, but when fused together, gives us a sense of the patterns and the flow that really is at the core of what intelligence analysis is all about...”⁴⁴

Since most of the nation’s firefighters live and work in the neighborhoods or communities they serve, they may be in a position to provide some of “the thousands of routine everyday observations and activities” necessary to prevent or disrupt terrorism.

⁴³ Chertoff, Remarks at the International Association of Fire Chiefs.” Chertoff told the International Association of Fire Chiefs that at the DHS, “We’re trying to integrate fire operations into the very fabric of DHS. Our National Operation Center now has a fire desk. We now have a Fire Service representative sitting at the table with our interagency colleagues from the FBI, state and local law enforcement and the intelligence community whenever we deal with an operational challenge. We recognize that you have special insight. We want your input into the whole range of our operations, and your expertise whenever we’re dealing with a hazard.”

⁴⁴ Chertoff, Remarks at the 2006 Bureau of Justice Assistance, March 14, 2006.

THIS PAGE INTENTIONALLY LEFT BLANK

III. THE CURRENT FIRE SERVICE INFORMATION-SHARING ENVIRONMENT

Nationally, fire departments have impressive staffing and capabilities. According to the National Fire Protection Association, total employment in firefighting occupations was 1,141,900 in 2006, of which more than 823,950 were part-time or volunteers.⁴⁵ Of the 30,635 fire departments in the United States, 4,052 are career departments, while the majority of departments (26,583) are staffed by volunteers.⁴⁶ Firefighters are often the first personnel at the scene of emergency incidents, where they perform a myriad of critical life-saving and property-conservation functions. Fire departments and firefighters are located throughout the country, from densely populated urban environments, residential neighborhoods and airports, to chemical plants, grasslands, forests, and large unincorporated areas.⁴⁷ Research for this thesis revealed that as few as fifteen of the thirty thousand U.S. fire departments formally use terrorism indicators and communicate the information gathered in this manner to the homeland security community.

Firefighters working and living in the communities they serve may be able to identify activities that in and of themselves may not be out of place from an outsider's point of view, but to a firefighter who lives, works, and responds to emergencies in the area, they may be suspicious. The realization of numerous intelligence centers collaborating and distributing information to the emergency-services sector enhances information sharing with non-traditional consumers such as the fire service. I expect this trend to continue.

The fire service strategies and legislative actions identified in this and other chapters were based on domestic and international information-sharing documents. The examples identified in this chapter help to define the current U.S. fire service role as a producer and consumer of terrorist-related information. Currently the draft National Strategy for the Fire Service Intelligence Enterprise Concept of Operations (FSIE

⁴⁵ National Fire Protection Association, U.S. Fire Department Profile Through 2006.

⁴⁶ Ibid.

⁴⁷ U.S. Department of Labor, Bureau of Labor Statistics, "Fire Fighting Occupations."

CONOPS) and the *Fire Department City of New York Terrorism and Disaster Preparedness Strategy* (FDNY Strategy) appear to be the only fire-specific U.S. information-sharing approaches available.

A. INFORMATION-SHARING EXAMPLES AND SCENARIOS

It appears that open source and Unclassified//For Official Use Only (U//FOUO) information regarding the identification and sharing of potential information is limited but increasing in quantity and quality. A number of U//FOUO and sensitive examples were shared with the author of this thesis under the condition that they not be used in an open source thesis. In an effort to provide this thesis to the widest audience possible, only open source or open source approved U//FOUO examples were used in this thesis.

To identify the current level of information sharing between the fire service and the homeland security community, I began by researching terrorist-related information using the National Fire Information System (NFIRS). NFIRS appeared to be a good choice because it represents the world's largest, national, annual database of fire service response information. Over twenty-one thousand fire departments participate in the NFIRS. The participating departments report an average of fourteen million incidents and one million fires each year.⁴⁸ Any potential terrorist data entered would be complemented by over two hundred other fire- or emergency-related fields and could be mined for terrorism trends and patterns. Unfortunately, several NFIRS subject matter experts were unable to identify or extract any terrorist or terrorism-related information from the

⁴⁸ U.S. Fire Administration, About NFIRS. The NFIRS database comprises more than one half of all reported fires that occur annually. The current NFIRS 5.0 version includes incident and casualty forms, a coding structure for data processing purposes, manuals, computer software and procedures, documentation, and a National Fire Academy training course for utilization of NFIRS. NFIRS allows participating local fire departments to fill out incident, casualty, and optional reports for fires and other event types as they occur.

database.⁴⁹ Apparently, the NFIRS database does not have fields for terrorist, terrorism, or suspicious related activities, and it is not possible to conduct a free text search of the narratives.

After unsuccessful attempts to query hundreds of thousands of emergency incidents in the NFIRS database for suspicious terrorist related information, I received an Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) e-mail that discussed emerging issues regarding firefighters sharing information with the law enforcement community. I contacted the EMR-ISAC representative for the Emergency Services Sector and discussed the current role of the fire service in preventing terrorism through information sharing with local, state, and federal homeland security partners. The EMR-ISAC representative agreed to research the issue. Like the NFIRS results, the EMR-ISAC research did not result in examples of information sharing between the fire departments and homeland security.

The EMR-ISAC representative recommended that I contact a senior intelligence analyst with DHS in Washington, D.C. After several phone conversations and e-mails, the DHS intelligence analyst provided me with the one example of successful information sharing that was a result of the DHS-sponsored New Mexico technology course, Incident Response to Suicide Bombings (IRTSB).

A member of a local fire department had attended the IRTSB class in Playas, New Mexico. The local fire department responded to a location for a “Smoke Condition” inside a building. During their check of the building for smoke, which proved to be negative, the firefighters came across fourteen one-gallon plastic containers filled with an unknown substance. The on-scene commander requested the Haz Mat unit, and upon their arrival, they determined the substance in the containers to be urine. The Incident Commander did not think anything of it, nor did the police supervisor at the scene. However, the member of the Haz Mat unit that had attended the IRSTB class indicated that the urine could be a component of a bomb, and because of this, the fire department contacted the FBI. Further searches of the house turned up an additional twenty empty

⁴⁹ Personal communication with National Fire Information Reporting System Board Member John Williams and Oklahoma City Fire Department Information Technology Captain Jim Kruta, February through March 2008.

containers and maps and train schedules of the New York metropolitan area. The tenant of the apartment was taken into custody by the FBI. At the time of this writing, the FBI investigation continues.

Internationally, several open-source information-sharing examples were identified during the preparation of this thesis. In 1995 an assassination attempt on the Pope by Al Qaeda operatives in Manila, Philippines was thwarted when a fire in the terrorists' rented hotel room tipped authorities to the attack.⁵⁰ Also, on June 29, 2007 a London-based ambulance crew "saw smoke coming from the green Mercedes...The ambulance had been called to the nightclub—where up to 1,700 people were inside...they spotted smoke, now believed to be vapour, inside the car." The ambulance crew shared the information with local law enforcement. After securing the area, Scotland Yard detonated the car, which contained sixty liters of gasoline, gas cylinders and nails.⁵¹

B. TERRORISM INDICATORS

Key to enhancing the current information-sharing environment are firefighters conducting operations with the knowledge, skills, and abilities to identify potential terrorist activities and to share the information with the appropriate homeland security partners. Uninformed firefighters acting without the benefit of the necessary knowledge, skills, and abilities may incur legal and civil rights violations of the people the firefighters have sworn to protect. A review of federal, state, local, public, and private open-source terrorism-prevention programs relating to the identification, collection, and communication of terrorist indicators resulted in over one hundred fifty different terrorist

⁵⁰ Posner, *Why America Slept*, 86–89.

⁵¹ British Broadcasting (BBC) News, "Police Avert Car Bomb Carnage."

indicators to look for.⁵² The following four indicators were prevalent in the prevention programs studied and are recommended for use by the U.S. fire service:

- *Suspicious behavior*: especially unusual nervousness for the situation and inappropriate or lack of eye contact.
- *Unusual supplies* for occupancy type (structure or vehicle): especially storing large amounts of chemicals, cash, electronics.
- *Unusual documents* for the occupancy type: especially maps, books, blueprints, or literature of critical infrastructures.
- *Intelligence gathering*: especially surveillance, taking pictures, video, notes, asking questions, attempting to gain access.

The use of the four common terrorist indicators combined with firefighter entry onto or into private property during emergency and non-emergency operations may place firefighters in a unique position to legally gather potential terrorist-related information in plain sight.

C. OPERATIONAL AND CITIZEN TRUST ISSUES

There are several issues relating to the current level of information collection, collaboration, and dissemination relative to citizen trust and operational information sharing. For example, firefighters should limit the use of terrorism indicators to those areas and circumstances within the scope of their primary emergency or non-emergency duties. Also, firefighters may need to become consumers of intelligence and related information in preparation for and in response to potential terrorist incidents at specific locations or special events. For the majority of the fire service and intelligence community, the current information-sharing environment may be informal at best and may not address strategic, legal, training, and operational issues adequately.

⁵² Eleven federal, state, and local organizations were reviewed for the identification of terrorist indicators that might be applicable for use by the U.S. fire service. The organizations were the Office of the Director of National Intelligence, New York City State Metropolitan Transportation System, Real Estate Board of New York, New York City Fire Department, New York State Office of Public Security, Federal Bureau of Investigation, Department of Homeland Security, U.S. Citizens Emergency Response Corps, Memorial Institute for the Prevention of Terrorism, Center for Defense and Homeland Security, Emergency Management and Response Information Sharing and Analysis Center, and Fire Service Intelligence Enterprise.

Currently, most fire departments operate on the legal premise that firefighters enter homes, businesses, vehicles, and other assets without warrants during emergency and non-emergency duties in their efforts to prevent and respond to life and property loss. This access may place them in a position to legally identify criminal activities or information in plain sight and to report the information to the appropriate homeland security partners. For example, in Oklahoma City if firefighters respond to a fire in the kitchen area, and while searching for victims or ventilating the structure, the firefighters notice a potential methamphetamine lab in the bedroom, the police department will be contacted. If children are present, the Department of Human Services will be notified.

The identification and sharing of potential terrorist indicators during non-emergency fire department operations presents other considerations. Virtually every city and town in America that has a paid fire department conducts mandatory fire inspections in businesses and offers non-mandatory inspections in homes. Fire- and life-safety code inspection local ordinances and state laws vary, but generally speaking firefighters may enter a business or rental property for periodic, routine, or complaint-driven inspections. Complaints are often received from citizens, employees, local law enforcement, and other city departments. All fire inspections require the implied or overt consent of the occupant. If the occupant denies consent, a warrant will be required unless an emergency condition exists.⁵³ Fire- and life-safety code inspections typically require examination of virtual all structural areas of a property. Use of the four common terrorism indicators may assist firefighters in recognizing potential terrorist activities during emergency operations and non-emergency fire- and life-safety inspections.

Another significant consideration relating to potential terrorist information sharing involves the trust that Americans have in their local fire departments and firefighters. Many paid and volunteer fire departments benefit from very high levels of citizen satisfaction and confidence. In some areas a community's identity is, in part, directly linked to its local fire department. This trust, if broken, could result in a long-

⁵³ *Camara v. Municipal Court*, 387 U.S. 523 (1967).

term negative effect to fire departments' and fire services' core mission to save lives and property. The National Strategy for Information Sharing commented on the issue of trust in the following statement:

While State and local officials work to prevent future terrorist attacks, they still must arrest criminals, put out fires, respond to traffic accidents, and deal with a host of public health and safety issues. Success in these endeavors depends on a strong partnership with the public, built on a foundation of communication and trust between local officials and the members of their community. These same partnerships will be used to protect these communities from future attacks by terrorists.⁵⁴

If firefighters enter premises primarily to obtain terrorism information, there is a distinct possibility that any information shared with the homeland security community would constitute an illegal search and violate the occupant's civil rights.⁵⁵ Firefighters must have a legitimate reason within the scope of their assigned emergency and non-emergency duties to enter a premise. If firefighters have legitimate emergency or non-emergency motives for conducting operations on or in private or public property, any potential terrorism indicators in plain sight during a firefighter's activities should be shared through a standardized process with the homeland security community.⁵⁶

One potentially simple system is for firefighters to report suspicious, non-time-sensitive information to the local intelligence community. The four terrorist indicators identified in this thesis could be informally or formally reported by the Incident Commander or senior fire official, to the fire marshal, local law enforcement representative, Joint Terrorism Task Force, fusion center, or other pre-identified intelligence-collecting entity.

For many years it has been a common practice in many U.S. fire departments to share information relating to potential illegal activities with the law enforcement

⁵⁴ White House. National Strategy for Information Sharing, 17.

⁵⁵ "The basic purpose of the Fourth Amendment, which is enforceable against the States through the Fourteenth, through its prohibition of 'unreasonable' searches and seizures is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials," *Camara*, 387 U.S. at 528.

⁵⁶ Masse, "Homeland Security Intelligence," 12. "Given that there are substantial national and homeland security penalties for not sharing homeland security intelligence, at least at the policy level and to some extent at the operational level, arguably there is now a bias in favor of sharing raw intelligence across levels of government more quickly than in the past. The extent to which this information is shared systematically is an open question."

community. This collaboration has occurred at emergency and non-emergency operations. At non-emergency operations such as fire code inspections, firefighters might report large quantities of explosives, chemicals, or firearms at businesses that typically do not handle those products. For emergency scenes the reporting of meth labs or their precursors, or domestic violence as a mechanism of injury, might be the catalyst for notifying the local law enforcement agency.

If the homeland security community, including law enforcement, requests the fire department to inspect a specific location for fire code violations and anything unusual that might be in plain sight, is the fire department now illegally collecting intelligence or sharing information gained in the course of its duties? An example of an illegal collection plan occurred in Oklahoma City. In 2007 a law enforcement representative approached an Oklahoma City firefighter and inquired if he would conduct a fire inspection at a local mosque in order to identify potential terrorist-related information. Fortunately, the firefighter's supervisor realized the legal exposure associated with the plan and denied permission to the firefighter to participate. One aspect of determining whether information collected by a firefighter is legal or "fruit of a poisonous tree" may lie in whether the firefighter was a sensor of opportunity or whether he was assigned the specific task of collecting information on suspected terrorists.

D. FIRE SERVICE INTELLIGENCE ENTERPRISE

In September of 2007, DHS coordinated a conference with over eighty executives from the fire service, public safety, homeland security, and intelligence communities to discuss the development of a national strategy for fire service intelligence and information sharing. Over the next nine months, fire department representatives who had attended the conference continued to meet and developed a set of recommendations for the development of the Fire Service Intelligence Enterprise (FSIE). In December of 2008, the FSIE released a "Draft Concept Plan" (FSIE CONPLAN) in an attempt to provide

direction in clarifying the role of the fire service in preventing terrorism and enhancing preparedness through information sharing with local, state, and federal homeland security partners.

The FSIE CONPLAN envisioned a national network of fire service and homeland security organizations that share all hazard information and intelligence in a collaborative effort to enhance the national prevention, preparation, response, and recovery missions.⁵⁷ The current mission of the FSIE CONPLAN is to:

Establish an institutionalized Fire Service information and intelligence sharing framework that will enhance the preparedness level of fire departments across the country while supporting the prevention, protection, response, and recovery efforts of all homeland security partners.⁵⁸

To date, the FSIE initiative is the only national strategic approach to information sharing between the U.S. fire service and homeland security community. Homeland security affiliates for the FSIE were identified within the FSIE framework as federal, state, local, tribal, and private sector “agencies or organizations that are stakeholders of FSIE initiatives, either as collaborators or customers” for the DHS.⁵⁹ The FSIE CONPLAN appeared to be a strategic extension and formal expansion of the current informal fire service information-sharing environment between the fire service and homeland security communities. The primary FSIE venues for sharing information were federal, state, and local fusion centers. Working within the Global Justice Information Sharing Initiative, fire service fusion center liaisons or representatives would act as nodes, and the fusion centers would act as hubs for receiving and disseminating relevant information in a timely and actionable manner.⁶⁰

⁵⁷ U.S. Department of Homeland Security, Office of Intelligence and Analysis, State and Local Program Office, Draft Fire Service Intelligence Enterprise Concept Plan.

⁵⁸ U.S. Department of Homeland Security, Office of Intelligence and Analysis, State and Local Program Office, Fire Service Intelligence Enterprise—Executive Briefing, 2.

⁵⁹ U.S. Department of Homeland Security, Office of Intelligence and Analysis, State and Local Program Office, Fire Service Intelligence Enterprise—Executive Briefing, 4.

⁶⁰ *Ibid.*, 6.

The FSIE CONPLAN is an important, new, and distinct course in clarifying the role of the fire service in preventing terrorism through information sharing with local, state, and federal homeland security partners and was based on four pillars:

- Identification of the types of intelligence and dissemination mechanisms that the fire service needs to enhance all-threat/all-hazard preparedness and to support fire service response and recovery operations.
- Identification of the way in which the Fire Service can contribute to local and national homeland security all-threat/all-hazard prevention and protection efforts.
- Collaborative development of an information/intelligence-sharing network within the fire service, and between the fire service and the homeland security/intelligence community, while ensuring the protection of citizen privacy and civil rights/civil liberties.
- Identification of a pool of fire service subject-matter experts to serve as advisors for DHS initiatives that involve or affect fire service interests.⁶¹

The DHS Office of Intelligence and Analysis (I&A)-coordinated FSIE initiative represents a logical progression in maximizing the current homeland security information-sharing culture. Given the current and future threat environments in this long-term conflict sometimes called the global war on terrorism, it might be careless or even negligent not to build on the FSIE's work to incorporate over one million firefighters into the information-sharing community.⁶²

E. CURRENT FIRE SERVICE INFORMATION-SHARING FACTORS

The current ad hoc or informal U.S. fire service information-sharing environment was the initial information-sharing option evaluated for this thesis. Each of the four

⁶¹ U.S. Department of Homeland Security, Office of Intelligence and Analysis, State and Local Program Office, Fire Service Intelligence Enterprise—Executive Briefing, 4.

⁶² In Chapter VI of this thesis, the FSIE CONPLAN is compared with other strategies and the current fire service/DHS information-sharing environment. In Chapter VII much of the FSIE CONPLAN Purpose, Desired End State and Goals and Objectives are integrated into the Fire Service/Homeland Security Information-Sharing Tool and Power vs. Interest Grid to provide recommended strategic structure and direction to the current ad hoc information sharing arrangements.

information-sharing options (current fire service, FSIE, FDNY Strategy, and CCA) examined for this thesis is qualitatively evaluated and then graphically represented by an information-sharing matrix based on five factors. The five factors are legal compliance, political acceptability, target capabilities linkage, operational impact, and cost. In Chapter VI, each information-sharing option is incorporated into an inclusive matrix that compares and contrasts all four information-sharing options.

1. Legal Compliance

The legality of current information-sharing practices is questionable, since most firefighters do not know what terrorism indicators to look for, when to look for them, or how to report them. Given that most firefighters are not actively aware of or engaged in reporting potential terrorist indicators, the fire service has not created any significant legal exposure or civil-liberties violations. Based on Masse's findings, the fire service has a legal responsibility to report suspicious activity.⁶³ In December 2007 the ACLU raised questions regarding firefighters' collecting and sharing potential terrorist information. The ACLU position indicated excessive potential loss of personal privacy rights would be the result of firefighters' collecting and sharing information.⁶⁴ Based on the court cases and public law identified in Chapter II of this thesis, firefighters have a legal right and the responsibility to collect and share potential terrorist-related information if the information is in plain sight during the course of their assigned duties. The current limited level of terrorism prevention awareness and training of the fire personnel may indicate the role of the U.S. fire service in collecting and sharing information (or not) is within the law.

2. Political Acceptability

Applicability of the current fire service information-sharing environment to the U.S. public, policy groups, labor unions, governmental agencies, and other related organizations is in the early stages of development. At the national level, DHS Secretary

⁶³ Masse, "Homeland Security Intelligence," 12.

⁶⁴ Olberman, interview with Mike German. See also National Terror Alert Response Center, Firefighters to Help In Fight Against Terrorism; Miller, More Media Reaction to FIRE-INT (Intel gathered by Fire/Rescue) thread.

Michael Chertoff made public an arrangement to include firefighters in fusion centers. Chertoff told the International Association of Fire Chiefs that at the DHS,

We're trying to integrate fire operations into the very fabric of DHS. Our National Operation Center now has a fire desk. We now have a Fire Service representative sitting at the table with our interagency colleagues from the FBI, state and local law enforcement and the intelligence community whenever we deal with an operational challenge. We recognize that you have special insight. We want your input into the whole range of our operations, and your expertise whenever we're dealing with a hazard.⁶⁵

Chertoff went on to say that Charlie Allen, the DHS Assistant Secretary for Intelligence and Analysis, "is working to add firefighter personnel to state and local fusion centers" and that "fusing firefighters and responders into the normal law enforcement and Counterterror Intelligence Fusion Center is critical to get a whole picture of what's going on."

Fire service information sharing and collaboration may be at the initial federal political stages of a significant future homeland security partnership, if one considers the scope and influence of the U.S. fire service.⁶⁶

3. Target Capabilities Linkage

Of the four information-sharing target capabilities selected for this project, the current fire service role in the homeland security information-sharing environment formally utilizes only the CBRNE detection-capabilities component through the DHS FY-2003 State Homeland Security Grant Program (SHSGP). The SHSGP also provided the most significant cost-related support to the current fire service–Homeland Security information-sharing environment.

⁶⁵ Chertoff, Remarks at the International Association of Fire Chiefs, October 26, 2007.

⁶⁶ National Fire Protection Association, The United States Fire Service; U.S. Fire Administration, Fire Departments. The United States has over one million firefighters serving in over thirty thousand fire departments that respond to over twenty-four million emergencies each year.

4. Operational Impact

The operational impact of the current information-sharing environment was difficult to assess as the current information-sharing strategies and programs are new, limited, and emerging. The existing role of the fire service within the intelligence cycle doesn't appear to have parameters for success or failure or specifics for associated budgets. The anecdotal successes associated with information sharing among homeland security and the emergency services, combined with the recent emergence of strategies and technical assistance programs suggest that there is a heightened awareness and increased opportunity to identify potential terrorists or specific terrorist targets or events. For example, the following Daily Open Source Briefing is an example of how heightened awareness among first responders impacted the Republican National Convention.

On the second day of the RNC, a Twin Cities paramedic spotted an “ambulance” with unusual generic markings in the city of Saint Paul. The medic had attended RNC briefings on the need for heightened awareness. The medic reported the location of the vehicle he had seen to a supervisor, and Saint Paul police were dispatched to investigate. Police found the vehicle unlocked; inside they found a large cache of weapons, bags of urine and feces, and related items to cause criminal damage to property. Saint Paul Police turned the fake ambulance over to the Secret Service. This find was invaluable to authorities and went a long way toward keeping people safe.⁶⁷

One labor organization that may have an operational impact is the International Association of Firefighters (IAFF). The IAFF represents over two hundred eighty thousand members in the United States and Canada. The IAFF offers terrorism response training for its members but has been silent on the issue of firefighters' role in the terrorism-prevention mission.

5. Costs

The SHSGP provided financial assistance for the purchase of specialized equipment to enhance the capability of state and local agencies to prevent and respond to incidents of terrorism involving the use CBRNE weapons. The SHSGP also allowed for:

⁶⁷ East Bay Terrorism Early Warning Group and Washington Regional Threat and Analysis Center, Daily Open Source Brief, November 5, 2008.

the protection of critical infrastructure and prevention of terrorist incidents; for costs related to the design, development, conduct, and evaluation of CBRNE exercises; for costs related to the design, development, and conduct of a state CBRNE training program; and for costs associated with updating and implementing each state’s homeland security strategy.⁶⁸

Funds were awarded to and distributed through State Administrative Agencies designated by the governor of each state.⁶⁹ Total funding provided through the SHSGP was \$566 million.⁷⁰ Since 2003 SHSGP funding has brought together state and local officials from throughout the emergency services sector to share information on their response needs and to collaborate on eligible purchases.

The matrix below is a graphic that identifies and broadly qualifies the current extemporized fire service/homeland security information-sharing environment. With the recent emergence of the FSIE, it is probable that current fire service information-sharing interests will be incorporated into national standards, protocols, and mechanisms for homeland security information and intelligence exchange.⁷¹ Therefore, the FSIE was considered as a separate and distinct information sharing option.

F. CURRENT FIRE SERVICE AND FSIE INFORMATION-SHARING MATRIX

Information-Sharing Option	Legal Compliance	Political Acceptability	Target Capabilities List Linkage	Operational Impact	Costs
Current U.S. Fire Service	Low/Average	Average	Low	Unacceptable	Low
FSIE	High	Unknown	Good	Unknown	Average

Figure 1. Current Fire Service and FSIE Information-Sharing Matrix

⁶⁸ U.S. Department of Homeland Security, FY 2003 State Homeland Security Grant Program, 1.

⁶⁹ Ibid., 5.

⁷⁰ Ibid.

⁷¹ U.S. Department of Homeland Security, Office of Intelligence and Analysis, State and Local Program Office, Draft Fire Service Intelligence Enterprise Concept Plan, 1.

G. CONCLUSION

Like many components of homeland security, the legal, moral, and ethical standards associated with firefighters sharing information are evolving. As the idea of information sharing among non-traditional intelligence cohorts progresses, there are a number of strategic and operational challenges to be considered. Based on the increase in informal and anecdotal information-sharing awareness, the advent of the FSIE, and FSIE CONPLAN identified in this chapter, the role of the fire service in sharing and receiving information with local, state, and federal homeland security partners may be increasing. For example, a small number of firefighters are participating in national, state, or local fusion centers where they operate as intelligence analysts and liaisons to the intelligence community. With that said, overall, it appears that the majority of firefighters have not received instruction on who, when, or how to report suspicious activity. Furthermore, the legal and moral responsibilities associated with firefighters gathering and sharing information has produced a range of estimations about what, if any, terrorist-related information collection and consumption firefighters should be involved in.⁷² The DHS Intelligence and Analysis, State and Local Program Office appears to be taking a lead role in developing and coordinating information-sharing partnerships. In Chapter IV, I will review the New York City Fire Department's Terrorism and Disaster Preparedness Strategy and qualify it based on the five information-sharing factors identified for this thesis (legal compliance, political acceptability, target capabilities linkage, operational impact and costs).

⁷² National Terror Alert Response Center, Firefighters to Help in Fight Against Terrorism; Edwards and Kane, Firefighters Asked to Report People.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. NEW YORK CITY FIRE DEPARTMENT TERRORISM AND DISASTER PREPAREDNESS STRATEGY

The lack of information sharing on 9/11 may have resulted in unwarranted fatalities for civilians, firefighters and other responders. The National Commission on Terrorist Attacks upon the United States, also known as The 9/11 Commission, stated:

Just as in the North Tower, callers from below and above the impact zone were advised to remain where they were and wait for help. The operators were not given any information about the inability to conduct rooftop rescues and therefore could not advise callers that they had essentially been ruled out. This lack of information combined with the general advice to remain where they were, may have caused civilians above the impact not to attempt to descend, although stairwell A may have been passable.⁷³

Regarding information-sharing with Fire Department, City of New York (FDNY), FDNY fire chiefs testifying to the 9/11 Commission reported that the lack of information sharing, particularly between the fire command staff and the police helicopter, adversely impacted operations.⁷⁴

As a direct result of 9/11, the FDNY released their comprehensive Terrorism and Disaster Preparedness FDNY Strategy (FDNY Strategy) in 2007. Based on my review of the FDNY Strategy, the fire department has taken steps to operate safely and effectively using information sharing in the post-9/11, multifaceted, all-hazards threat environment. The following statement in the FDNY Strategy indicates that the fire department is in a position to address a number of the information-sharing challenges within the homeland security community.

An examination of the events leading to 9/11 highlighted many gaps in information-gathering capabilities and information-sharing protocols within the homeland security community. The FDNY recognized that the Department could help to fill some of these gaps by contributing to local intelligence-gathering efforts. When routinely shared with intelligence and law enforcement agencies, the information gathered by FDNY personnel

⁷³ National Commission, 295.

⁷⁴ Ibid., 321. “Information that was critical to informed decision making was not shared among agencies. FDNY Chiefs in leadership roles that morning have told us their decision making capability was hampered by lack of information from NYPD aviation.”

could make a significant contribution to existing intelligence and lead to the identification and disruption of terrorist activities. Terrorism-related information can be gathered by the FDNY in many ways. During the course of routine building inspections, arson investigations and response to fires and medical emergencies, FDNY personnel have unique access to homes and building that generally are concealed from outsiders.⁷⁵

According to FDNY Commissioner Scoppetta and Fire Chief Cassano, the FDNY leadership employed the insight and skills from a cross section of FDNY's fifteen thousand-person work force to develop the FDNY Strategy. The FDNY Strategy was designed to provide direction and unity toward enhanced preparedness.⁷⁶

A. ELEMENTS OF THE FDNY STRATEGY

The FDNY Strategy is organized around four chapters. Chapter 1 (Strategy and Purpose) addresses the foundation of preparedness based on the current and future threat environment for man-made and natural disasters. Chapter 2 (mission and focus) examines the life-safety oriented work and focus of the FDNY, based on pre-determined significant issues that must be addressed to achieve the pre-identified levels of preparedness. Chapter 3 (Operational Readiness) describes how the FDNY ensures that firefighters have “the tools, training and support they need to do their job.”⁷⁷ Chapter 3 also identifies a number of the National Preparedness Goal components to assist FDNY firefighters in achieving the evaluation points identified in Chapter 4 of the FDNY Strategy. The National Preparedness Goal components identified in the FDNY Strategy are “planning; organization and leadership; equipment and systems; training; exercises, evaluations and corrective actions; and personnel.”⁷⁸ Chapter 4 (Coordination and Evaluation) is the final chapter of the FDNY Strategy and utilizes an “FDNY Strategy Cycle” to provide a systematic approach in identifying hazards, evaluating risks, implementing control measures and evaluating the FDNY Strategy.

⁷⁵ Fire Department City of New York, “Terrorism,” 20.

⁷⁶ Ibid.

⁷⁷ Ibid., 8.

⁷⁸ Ibid.

1. Evaluation Points

The FDNY Strategy control measures involve Evaluation Points, which are specific performance goals and objectives for the FDNY. On the whole, the FDNY Strategy appears to be designed to describe how FDNY will achieve all-hazards organizational preparedness and response to man-made and large-scale natural emergencies. All chapters include information-sharing practices.

The FDNY Strategy postulates that man-made and natural disasters can occur throughout New York City, “from the top floors of a high-rise building to a train car in a tunnel, aboard a ship docked in a port or in a crowded street.”⁷⁹ Due to the diverse threats faced by the FDNY, the focus of preparedness in New York City was based on an all-hazards approach that incorporated “terrorist attacks, major disasters, and other emergencies.”⁸⁰

2. Breaking Points

To address the numerous man-made and natural risks the FDNY relied upon an all-hazard, capabilities-based planning approach to address a wide range of challenges and FDNY fiscal constraints. The FDNY Strategy also considered FDNY’s “breaking points” or the point at which FDNY’s considerable resources would be unable to meet the demands of a large scale or complex emergency response.⁸¹ The need for pre-incident information sharing with external partners to assist with filling anticipated response gaps is evident in the following statement:

⁷⁹ Fire Department City of New York, “Terrorism,” 9.

⁸⁰ U.S. Department of Homeland Security, Interim National Preparedness Goal, 3.

⁸¹ Fire Department City of New York, “Terrorism,” 11. “A breaking point is the point at which operational needs exceed organizational capability (what FDNY can do), capacity (how much FDNY can do), proficiency (how well FDNY can do it) and/or deployment (how rapidly FDNY can do it)... The Department must examine breaking points in terms of *capability* (an incident may require tasks FDNY is in the best position to execute, but does not yet have the full ability to perform); *capacity* (an incident may require more resources than available); *proficiency* (an incident may require skills greater than the level possessed); and *deployment* (an incident may require resources more rapidly than FDNY can position them).”

Members also must recognize that not all response gaps can be reasonably filled by the FDNY alone. The complexity and scale of a worst-case scenario incident will require assets and abilities beyond those that could be acquired and sustained over the long-term by any single organization.⁸²

Based on FDNY resources, the FDNY Strategy’s capabilities-based planning approach required prioritization of assets for all-hazard preparedness. Specifics of the capabilities-based planning process are discussed in further detail later in this chapter.

B. INFORMATION-SHARING TACTICS

As the new preparedness reality relates to information-sharing smart practices in preventing terrorism through information sharing, the fire service may wish to consider the FDNY’s information-sharing enterprise that consolidates voice, video, and data information from multiple internal and external sources at a centralized command center. The system may have application to the current DHS interoperability initiatives.⁸³

The FDNY’s preparedness tactics include the importance of effectively sharing information internally among the thousands of FDNY fire personnel as well as externally among the homeland security community. Regarding terrorist threats, the FDNY considered modern terrorist capabilities to include the use of unconventional (chemical, biological, radiological, and nuclear) weapons, as well as improvised explosive devices and vehicle-borne improvised explosive devices.⁸⁴

⁸² Fire Department City of New York, “Terrorism,” 11.

⁸³ U.S. Department of Homeland Security Office of Science and Technology, Interoperability Initiatives Fact Sheet. “Emergency responders—police officers, firefighters, and emergency medical service personnel—need to exchange voice and data communications across disciplines and jurisdictions to successfully respond to day-to-day incidents and large-scale emergencies. Many people assume that emergency response agencies across the Nation are already interoperable. In actuality, emergency responders often cannot talk to some parts of their own agencies—let alone communicate to agencies in neighboring cities, counties, or states. Interoperability is a complex, multidimensional challenge involving cultural, technological, and financial factors. The U.S. Department of Homeland Security is addressing capability gaps through the Science and Technology Directorate’s Office for Interoperability and Compatibility (OIC) and the Directorate for National Protection and Programs’ Office of Emergency Communications (OEC). Through these programs, DHS is leading initiatives and providing tools that help local, tribal, state, and Federal emergency response agencies to accelerate interoperable communications progress.”

⁸⁴ U.S. Department of Homeland Security, Interim National Preparedness Goal, 10.

The network-centric information-sharing system reportedly provides a comprehensive real-time picture of credible threats for strategic and tactical planning purposes. The network-centric information-sharing system is also designed to provide situational assessments to enhance tactical multiple incident command(s) activities for real-time threat intelligence and numerous situational images. Components of the information-sharing system include FDNY databases, imaging libraries, and field units, as well as integration with other local, state, and federal agencies, the private sector, and multiple media outlets. The FDNY Strategy indicated during the response phase of an incident, the network-centric command structure and related information-sharing among all homeland partners would improve situation awareness through information sharing during the escalating period of operational activities and provide a universal operating picture for the FDNY and other response partners. The hub of FDNY's complex network-centric information-sharing enterprise is the FDNY Operations Center that coordinates information sharing among Borough Communications Center, Field Communications System Mobile Command Centers, Geographic Information Systems, the Automatic Vehicle Locator System, live video feeds from public and private sectors, and networked connections to the DHS, FBI, NYPD, NYC Office of Emergency Management, and other city, state, and federal agencies.⁸⁵

Although the network-centric information-sharing system appears to be heavily technologically dependent and may require considerable buy in and collaboration from numerous diversified public and private partners, it has the potential to substantially increase life safety and property conservation at natural and intentional emergency events. Figure 2 is a graphic representation of the network-centric command system that is information-sharing dependent. Besides being useful at emergency incidents, the system could be used during specific large-scale assembly occupancies, special events, or other potential terrorist targets.

⁸⁵ Fire Department City of New York, "Terrorism," 14.

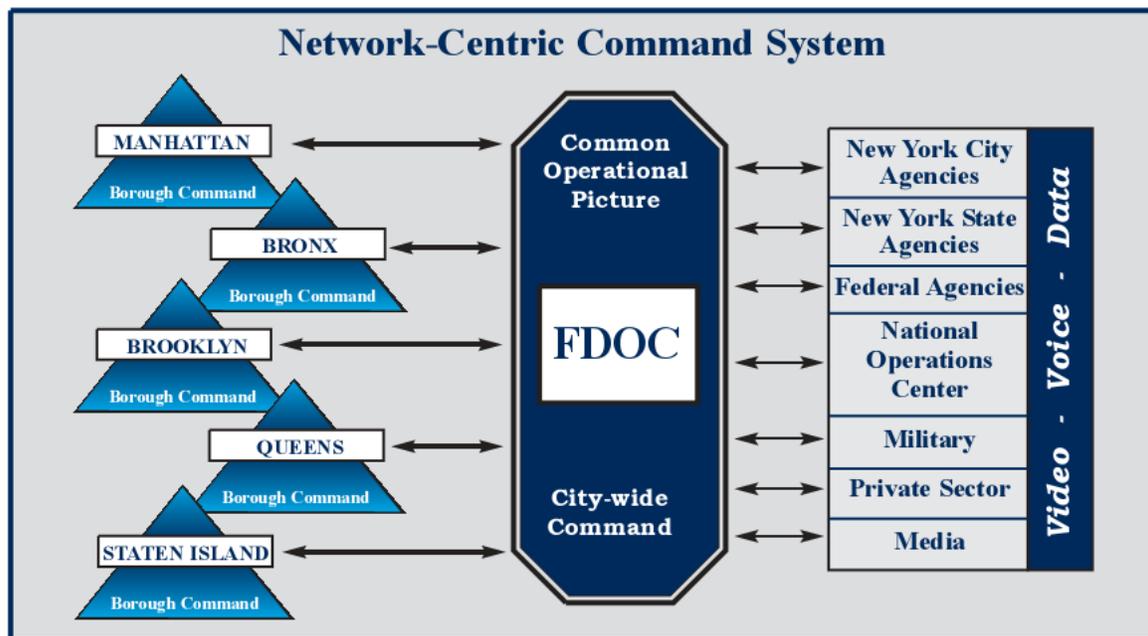


Figure 2. FDNY Network-Centric Command System

The FDNY Strategy quantified emergency and non-emergency activities with the following statement: “Each year, FDNY units make approximately two million fire, medical and other emergency responses and 300,000 building inspections.”⁸⁶ The millions of activities may be information-sharing opportunities to prevent or disrupt potential terrorism when the information shared is within the legal requirements described in this thesis.

C. RISK ASSESSMENT

The FDNY assesses critical infrastructure vulnerability using the Risk Assessment and Target Hazard program to collect, coordinate, and disseminate information. The program uses a database to provide comprehensive site information for incident planning and management by multiple homeland security partners. According to the FDNY Strategy, the Risk Assessment and Target Hazard unit is “working closely with the DHS Office of Infrastructure Protection to ensure the risk assessment models

⁸⁶ Fire Department City of New York, “Terrorism,” 18–21.

and databases FDNY produces follow national guidelines and can be integrated with national systems.”⁸⁷ While the law enforcement disciplines study buildings and other structures from a security standpoint, the FDNY (and the U.S. fire service) could provide another aspect of vulnerability by analyzing the same structures from an all-hazards risk assessment with a primary focus on life safety and property conservation. The fire service assessments may enhance law enforcement and intelligence agency pre-incident planning as well as response incident stabilization operations. The FDNY may wish to incorporate the terrorist indicators identified in this thesis in concert with their pre-incident information-sharing programs to enhance their all-hazard threat analysis procedures and programs.

D. BUREAU OF FIRE INVESTIGATION

Another information-sharing asset of the FDNY is the Bureau of Fire Investigation. The FDNY Bureau of Fire Investigation was identified as a primary FDNY point of contact for information sharing with several homeland security community partners.

The Bureau of Fire Investigation works closely with other law enforcement agencies and the intelligence community on threat analysis and complex incident investigations. Fire Marshals are members of numerous collaboration and intelligence networks, including the Joint Terrorism Task Force (JTTF), and the FBI. The information FDNY Fire Marshals exchange through the JTTF not only aids in incident investigations, but also helps FDNY and all New York City security and response agencies prepare and prevent future incidents.⁸⁸

The FDNY Bureau of Fire Investigation also assists local law enforcement agencies in identifying and protecting emergency operations personnel from secondary attacks. FDNY fire marshals work closely with the FBI’s Joint Terrorism Task Force on threat analysis and complex incident investigations.⁸⁹ These marshals have FDNY police

⁸⁷ Fire Department City of New York, “Terrorism,” 22.

⁸⁸ *Ibid.*, 19.

⁸⁹ *Ibid.*

powers and according to the FDNY Strategy played a significant role in the investigations following the attacks on the World Trade Center in 1993 and 2001.

The rationale used in integrating the FDNY fire marshals as terrorism information coordinators or fusion center liaison officers with the homeland security intelligence community may have application on a national scale. Fire marshals may be well-suited to act as the local fire service points of contact for information sharing between the fire service and homeland security partners relating to potential illegal activity such as terrorism, clandestine drug labs, violent gangs, and other activities that might affect citizen and firefighter safety or fire department operations.

E. COLLABORATION

Chapter 3 (Operational Readiness) of the FDNY Strategy focuses on six of the DHS National Preparedness Goal elements. The six elements are planning; organization and leadership; equipment and systems; training; exercises, evaluations and corrective actions; and personnel. The FDNY relied on intra-departmental collaborative emergency response plans for “all-hazard complex incident scenarios” and the creation of continuity of operations plans to ensure stability and adequate personnel succession.⁹⁰ The two plans collectively addressed emergency and non-emergency operations to effectively save lives and property before, during, and after long-term, high-resource, or complex incidents.

The private- and public-sector collaboration required for the development of the plans is similar to the information-sharing requirements used by England’s Local Resilience Forums (see Chapter V of this thesis for more information on UK Civil Contingencies Act, Local Resilience Forums and Risk Registers). Both the FDNY and England’s system leverage informal internal and external information-sharing partnerships in the planning process in order to establish relationships prior to emergency response and to enhance resource utilization, communication and collaboration during mitigation, preparedness and response activities. Both systems also prescribed overall

⁹⁰ Fire Department City of New York, “Terrorism,” 22.

terrorism and disaster-preparedness systems that require civic, private, and homeland security (including fire departments) to prioritize capability goals and to ensure specific local or regional needs are identified using a collaborative and regimented all-hazards approach.

F. INTELLIGENCE GATHERING

The FDNY Strategy was the only one of the four information-sharing options (current fire service, FSIE, FDNY Strategy and CCA) evaluated that considered signal intelligence (SIGINT) sharing. The other three options (current information-sharing , FSIE and CCA) only identified human intelligence (HUMINT) information sharing. The FDNY Strategy considered enhancing information collection and sharing through the use of a diverse suite of small unmanned aerial vehicles (UAVs) for reconnaissance and possibly intervention operations. According to the FDNY strategy UAVs may have application in measuring chemical, biological, or nuclear quantities and limited chemical/biological neutralization in New York City's urban environment.

Building on the idea of the use of real-time signal intelligence to assist the U.S. fire service and their homeland security partners in sharing information, the application of the Naval War College's Global Hawk-type system for use by the fire service and homeland security partners for real-time information sharing during or pre-planning of large scale natural, man-made disasters, including high-value terrorist targets, may be appropriate. Advantages of the Global Hawk system were identified in the following statement by David Hardesty in the September 2005 Naval War College Review.⁹¹

Intelligence, Surveillance, and Reconnaissance Unmanned aerial vehicles (UAVs) are likely to assume an increasing share of ISR responsibilities. "Specially designed UAVs have long loiter time, can be positioned flexibly near potential targets, and are small and relatively difficult to detect." Global Hawk offers a sixty-five-thousand-foot operating altitude, thirty-six-hour endurance, and an integrated suite of electro-optic/infrared (EO/IR) and synthetic aperture radar/moving target indicator (SAR/MTI) sensors.... A tiered, networked constellation of UAVs could be fielded that included high-altitude, wide-area-surveillance UAVs working with medium and low-altitude tactical UAVs employing EO/IR and range-

⁹¹ Hardesty, "Spaced Based Weapons," 16.

gated laser radars...UAVs, however, are not without limitations—primarily cost, large-bandwidth communications, and low combat survivability.

Based on the information from Hardesty, the application of a Global Hawk–type UAV system to all-hazards response by the U.S. fire service and DHS is significant. For example in late 2005 and early 2006, central Oklahoma experienced one of the most severe wildland fire seasons in its history. As one large wildland fire was progressing, the Unified Command used an available law enforcement helicopter to get an aerial view of the fire complex.⁹²

The aerial reconnaissance officer recognized that while numerous agencies and crews were working efficiently to extinguish a significant number of fire fronts, they were not working effectively. Many crews were suppressing fire in areas that could burn for days without loss of life or property while a few crews were working in an area that, if not extinguished within the next operational period, would eventually jeopardize hundreds of homes and thousands of residents. The Incident Action Plan was immediately modified to move firefighters from lower risk divisions to the division most susceptible to life and property loss.

I propose that the Global Hawk or a similar system would allow Unified Commands the ability to see the big picture necessary to make better strategic decisions, forecast potential outcomes, and enhance responder accountability through geospatial awareness at significant natural or man-made disasters for long periods of time. The Global Hawk system could also assist in pre-event staging and logistical alignment at large-scale, high-value terrorist targets.

G. INTELLIGENCE DISSEMINATION

Another operational information-sharing program identified in FDNY Strategy was the development and dissemination of a department-wide weekly bulletin called

⁹² Gibson, “Fire Ravages Oklahoma City.” “OKLAHOMA CITY, Okla. — Grassfires raged across the dry southern prairie Sunday, burning homes in Oklahoma City, destroying two small towns in Texas, and creating patchworks of flames as burning embers were blown by the gusting winds. Dozens of fires burned across the dry Oklahoma landscape as the wind gusts reached 50 mph.”

Watchline. The *Watchline* addresses all-hazard FDNY specific mitigation and response missions “to keep members abreast of new dangers and guard against complacency in the absence of new incidents.”⁹³ Of all unclassified information-sharing bulletins, dispatches, notices, and info-grams reviewed for this thesis, the FDNY *Watchline* appeared to be the best fire service–specific product and should be recreated by the DHS for distribution to the U.S. fire service through the Emergency Management and Response Information-sharing Analysis Center. *Watchline* is unique from a fire service perspective because the recommendations are tactically oriented, directed to the frontline firefighter, concise, and practical.

H. FDNY STRATEGY INFORMATION-SHARING MATRIX

Figure 3 identifies and grades the FDNY Strategy relating to the prevention and disruption of terrorism through information sharing.

Information-Sharing Option	Legal Compliance	Political Acceptability	Target Capabilities List Linkage	Operational Impact	Costs
Current U.S. Fire Service	Low/Average	Average	None	Unacceptable	Low
FSIE	High	Unknown	Good	Unknown	Average
FDNY Strategy	High	High	High	Average	Average

Figure 3. FDNY Strategy Information Sharing Matrix

I. FDNY STRATEGY INFORMATION-SHARING FACTORS

The FDNY Strategy scored well based on three of the five information-sharing factors identified for this thesis. One reason was the FDNY Strategy is the only U.S. fire service–related information-sharing strategy that has been vetted through a process that includes three of the five information-sharing factors. The three factors on which the FDNY Strategy scored well are legal compliance, political acceptability, and target capabilities list linkage.

⁹³ Fire Department City of New York, “Terrorism,” 27.

1. Legality and Political Acceptability

The FDNY Strategy was developed in concert with the DHS Office of Intelligence and Analysis using the requirements or guidelines of numerous accepted local, state and federal documents. In an attempt to comply with the current legal and political homeland security environment, the FDNY Strategy worked with local and national homeland security partners and considered local and national information-sharing related policies. Those policies most relevant to information sharing were: the U.S. Department of Homeland Security's National Preparedness Goal; New York City Office of Emergency Management's Citywide Incident Management System (CIMS); National Response Plan; the New York City Urban Area Homeland Security's Initial Assessment and FDNY Strategy; FDNY Management Indicator Reporting System; U.S. Department of Homeland Security's National Infrastructure Protection Plan; U.S. Office of Management and Budget's Guide to the Program Assessment Rating Tool (PART); and U.S. Code of Federal Regulations, Title 31, Section 115 (31 U.S.C. 1115).⁹⁴ It also appears that the FDNY has a desire to build on legal and political acceptability as exemplified in the following statement:

As the agency tasked with championing life safety within New York City, the FDNY is responsible for ensuring that mandates are effectively fulfilled. Additionally the Department also must continue to work with other City, State and Federal agencies, as well as the private sector, to enhance the quality, capability and cohesiveness of the City's and nation's overall ability to provide homeland security.⁹⁵

2. Target Capabilities Linkage

FDNY, like many—if not all—of the Urban Area Security Initiative cities and regions, used the planning scenarios to enhance their protection and response missions and to compete for DHS grant funding. The FDNY Strategy exceeded the criteria for this thesis by identifying the role of the FDNY in all thirty-six target capabilities identified in

⁹⁴ Fire Department City of New York, "Terrorism," D-1.

⁹⁵ *Ibid.*, 19.

the National Preparedness Guidelines. Figure 4 below identifies the four information-sharing thesis-specific target capabilities and the FDNY’s role.

National Target Capability	FDNY Role
Intelligence Information Sharing and Dissemination	<ul style="list-style-type: none"> • Joint Terrorism Task Force • Fusion Center • Inter-agency coordination (city, state, federal, and international) • Telecommunications and information technology
CBRNE Detection	<ul style="list-style-type: none"> • Routine field monitoring by Haz-Mat teams • Data collection and analysis • Syndromic surveillance
Intelligence Gathering and Recognition of Indicators and Warnings	<ul style="list-style-type: none"> • Bureau of Fire Investigation • Building inspections • Inter-departmental liaisons • Syndromic surveillance
Warnings, Intelligence Analysis, and Production	<ul style="list-style-type: none"> • <i>Watchline</i> • Coordination with DHS Office of Intelligence and Analysis • Bureau of Fire Investigation

Figure 4. Target Capabilities List Linkage

3. Operational Impact

The FDNY Strategy may be a model for increasing the operational impact of the U.S. fire service in the all-hazards information-sharing environment. For example, the FDNY Bureau of Investigation maintains numerous important connections with the homeland security community, such as serving on the JTTF, working with the DHS Office of Intelligence and Analysis, sharing pre-incident intelligence, filing observation reports and real-time incident updates with the NYC Fusion Center, keeping the FDNY leadership informed of current threats and how the FDNY can improve its contributions to New York City’s and the nation’s all-hazards preparedness. The FDNY fire marshals also share information at potential terrorist incidents by identifying and notifying first responders of secondary threats such as potential improvised explosive or incendiary devices.

Another example of FDNY's attempt to improve effectiveness is the development of a network-centric information-sharing-based command system that may someday significantly increase real-time information sharing among a myriad of local, state, and federal partners.

The FDNY also identifies and communicates national and local information to fire personal and the homeland security community through *Watchline*.

4. Costs

The cost of developing and implementing the FDNY Strategy appears to have been incorporated into the operating budget and supplemented with DHS grant funding for equipment. For example, the cost of producing and distributing *Watchline* as well as the cost of the network-centric Command System appeared to have been developed within the FDNY FY 06–07 operating budget.

J. RECOMMENDATIONS

If the FDNY and the U.S. fire service are to be successful in preventing or disrupting terrorism through information sharing in the current and future terrorist environment, they must continue to implement and refine robust approaches like the FDNY Strategy that include measurable information-sharing components within fire departments and in conjunction with other emergency service-sector and private partnerships. The recommendations below from the FDNY Strategy may have application to the current U.S. fire service information-sharing environment.

- Use of fire marshals as homeland security liaison officers with homeland security partners such as the JTTF, TWIG, FBI, fusion centers.
- Use of fire marshals at potential terrorist emergency scenes to ensure the safety of workers relating to secondary devices and scene control.
- Use of fire personnel to report common terrorist indicators in plain view, identified during normal emergency and non-emergency operations.

- Use of an integrated all-hazards Incident Command System–based information-sharing system for all multi-discipline, multi-agency emergency responses and preparation for high-profile or target-rich special events.
- If successful in New York City, consider expansion of the Risk Assessment and Target Hazard program for use by the U.S. fire service. The program could be coordinated and managed through the fifty-two fusion centers.
- With permission of the FDNY, re-creation of *Watchline* by the Emergency Management and Response Information Sharing Analysis Center for distribution to the U.S. fire service.
- Monitoring of the FDNY network-centric command system for applicability to the U.S. fire service.
- Use of the Naval War College’s Global Hawk system (or other UAV platforms) by the fire service and homeland security partners for real-time information sharing during or in pre-planning large-scale natural or man-made disasters, including high-value terrorist targets.

K. CONCLUSION

The lack of information sharing on 9/11 appears to have been the catalyst for conducting a gap analysis of FDNY policy and procedures. The result was the FDNY Strategy. The product of FDNY’s efforts included a number of recommendations that may have applicability to U.S. fire service/homeland security information sharing. For this thesis, consideration was given to the components of the FDNY Strategy relative to information sharing in the prevention, protection, response, and recovery missions that may be replicable at local, state, or national levels. The FDNY Strategy processes and systems also became the catalyst for the recommendations section of this chapter. Analysis of the FDNY Strategy for this thesis also included an assessment relative to the five information-sharing factors and included a comparison of the FDNY Strategy to the current fire service information-sharing environment as well as the FSIE. Further analysis of the FDNY Strategy is considered in Chapter VI of this thesis.

In the next chapter, England's CCA is evaluated for security strategies, policies, and activities that may be used to assist U.S. fire departments and the homeland security community in the identification and sharing of information regarding potential terrorist activities.

V. UNITED KINGDOM CIVIL CONTINGENCIES ACT OF 2004 (CCA)

The CCA Part 1 identifies and assigns local arrangements for information sharing and formally recognizes fire department brigades as an integral part of England's intelligence cycle. The CCA was the only international information-sharing document found that incorporated a role for the fire service.

The CCA may be the most comprehensive single national fire service-related information-sharing document analyzed for this thesis. In contrast, the National Information Sharing Strategy⁹⁶ released in October 2007 does not identify the U.S. fire service anywhere in its forty pages.⁹⁷ In England the fire service roles and responsibilities regarding information sharing are clearly identified in the CCA and in some cases the fire service is mandated to play the lead role.

The CCA is the product of a legislative evolution that began with the United Kingdom's Emergency Powers Act of 1920 and continued with the 1948 Civil Protection Act. Following the fuel crisis and severe flooding that occurred in late 2000, and the outbreak of foot-and-mouth disease in 2001, Deputy Prime Minister John Prescott initiated a review of the UK's emergency-planning and information-sharing arrangements that included input from public, private, and governmental agencies. The result indicated that new legislation was needed to deliver a different structure for civil protection in the UK.⁹⁸ The new structure needed to be capable of meeting the challenges associated with large-scale man-made or natural disasters. The bill received royal assent on November 18, 2004, and became known as the Civil Contingencies Act of 2004 (CCA).⁹⁹

⁹⁶ White House, National Strategy for Information Sharing, 17.

⁹⁷ Ibid. "While State and local officials work to prevent future terrorist attacks, they still must arrest criminals, put out fires, respond to traffic accidents, and deal with a host of public health and safety issues. Success in these endeavors depends on a strong partnership with the public, built on a foundation of communication and trust between local officials and the members of their community. These same partnerships will be used to protect these communities from future attacks by terrorists."

⁹⁸ United Kingdom, Cabinet Office, Civil Contingencies Secretariat, Civil Contingencies Act 2004, Short Guide, 1.

⁹⁹ United Kingdom, Cabinet Office, Civil Contingencies Secretariat, Civil Contingencies Act 2004, Part 1 Local Arrangements for Civil Protection.

The CCA was designed to provide a single legislative point for wide-ranging protection of civilians and military from significant all-hazard disasters. Part One focuses on local arrangements for civil protections, and identifies the legal framework regarding the roles and responsibilities for local Level 1 and 2 responders. Level 1 responders are referred to as “core responders” and include emergency services such as police, fire, ambulance, maritime and coastguard agencies, as well as local authorities, environmental, and health care agencies.¹⁰⁰ Category 2 responders or “co-operating responders” include utilities and transportation agencies.¹⁰¹

Part Two of the CCA focuses on the emergency powers at the national and regional governmental levels and includes special legislative actions and authority at the policy level that may be needed to address the effects of significant events such as the London 7/7 subway bombings, or the foot-and-mouth disease outbreak. Part Three addresses the general, fiscal, and administrative issues relating to implementing and maintaining the CCA.¹⁰²

A. ANALYSIS OF THE CCA

This thesis analyzes Part One of the CCA relating to the role of England’s fire service as a core responder in the prevention of terrorism through information sharing to fulfill its civil protection duties with other Level 1 and 2 responders and the public. This chapter utilizes the sections of the CCA relevant to England specifically and does not consider the other UK countries of Northern Ireland, Scotland or Wales.

Besides the CCA itself, several companion documents were used in the analysis of the CCA for this thesis. Below is a synopsis of the CCA categories and regulations that

¹⁰⁰ United Kingdom, Cabinet Office, Civil Contingencies Secretariat, Civil Contingencies Act 2004, Short Guide, Annex A. Category 1 responders (“core responders”) for emergencies services incorporate the following: “Police forces, British Transport Police, Fire authorities, Ambulance services Maritime and Coastguard Agency, All principal local authorities (i.e. metropolitan districts, shire counties, shire districts, shire unitaries), Port Health Authorities, Health bodies, Primary Care Trusts, Acute Trusts, Foundation Trusts , and the Health Protection Agency.”

¹⁰¹ Ibid.

¹⁰² United Kingdom, Cabinet Office, Civil Contingencies Secretariat, Civil Contingencies Act 2004, Part I.

are used by England's fire service and that may be applicable to the role of the U.S. fire service in the prevention or disruption of terrorism through information sharing with other emergency services and the homeland security community.¹⁰³

B. THE CCA AND INFORMATION SHARING

In category one of the Contingency Planning regulations, fire brigades and other local responders were identified as “the building block of resilience in the UK and are subject to the full set of civil protection duties.”¹⁰⁴ As core responders, England's firefighters are required to play a significant and sometimes lead role in information sharing.

In England, information sharing is a crucial element of preventing or disrupting terrorism “underpinning all forms of co-operation.”¹⁰⁵ According to HM Government, Emergency Preparedness, Guidance on Part One of the Civil Contingencies Act 2004:

Information sharing is necessary so that Level 1 and 2 responders are able to make the right judgments. If Level 1 and 2 responders have access to all the information they need, they can make the right decisions about how to plan and what to plan for. If they do not have access to all information,

¹⁰³ United Kingdom, Cabinet Office, Civil Contingencies Secretariat, Civil Contingencies Act 2004, Contingency Planning Regulations 2005, Statutory Instrument 2005 No. 2042. The Civil Contingencies Act 2004—Contingency Planning Regulations 2005 contain the regulations for the CCA and provided more information relating to the role of the U.S. fire service in preventing and disrupting terrorism through information sharing than the CCA did. Another useful document in the analysis of the CCA for this thesis was the UK Office of the Cabinet, Civil Contingencies Secretariat Civil Contingencies Act 2004 Short Guide, 57. CCA Part I regulations were organized around ten general categories and went into effect on November 14, 2005. Each of the ten categories of the regulations contained a varying number of specific regulations relating to that Part.

¹⁰⁴ United Kingdom, Cabinet Office, Civil Contingencies Secretariat, Civil Contingencies Act 2004, Short Guide. For the purposes of this thesis, English firefighters are required to “assess the risk of emergencies occurring and use this to inform contingency planning; Put in place emergency plans; Put in place Business Continuity Management arrangements; Put in place arrangements to make information available to the public about civil protection matters and maintain arrangements to warn, inform and advise the public in the event of an emergency; Share information with other local responders to enhance co-ordination; Co-operate with other local responders to enhance co-ordination and efficiency; and Provide advice and assistance to businesses and voluntary organisations about business continuity management.”

¹⁰⁵ United Kingdom, HM Government Emergency Preparedness, 24-25. “Information is shared between Category 1 and 2 responders as they work together to perform their duties under the Act. Information sharing is a crucial element of civil protection work, underpinning all forms of co-operation. It may involve simple liaison between bodies keeping each other up to date on their current arrangements and future plans. Such activities may be carried out through the proposed forums, and more informally.”

their planning will be weakened. They will be less well placed to make judgments around cost-benefit analysis – what to plan for and what not to plan for.¹⁰⁶

The 57 CCA Part One regulations and related compliance documents may have the potential to assist in clarifying the role of the U.S. fire service in preventing terrorism through information sharing between local state and federal homeland security partners. The CCA Part One may also apply to U.S. fire departments in the identification, dissemination, and receipt of potential classified and “for official use only” information.¹⁰⁷

The CCA requires informal or alternative routes of information sharing based on dialogue and cooperation. If that is not the case, “it is probably evidence of a wider systemic failing in the way the CCA is operating in the local area in question.”¹⁰⁸ Core and cooperating responders are required to consider alternative routes of information sharing before pursuing a formal information request to enhance cooperation in an effort to lessen the “over-bureaucratization of the information sharing process.”¹⁰⁹ Currently the primary U.S. fire service/homeland security information-sharing environment is ad hoc or informal. One difference between England’s system and the U.S. system is that the CCA requires involvement of all core responders in the Local Resilience Forums and Risk Registers. For example Regulation 55 requires the London Fire and Emergency Planning Authority (Fire Brigade) to take lead responsibility for maintaining community Risk Registers and to assist with exercises and training. Regulation 56 requires other core responders that have functions in London to cooperate with the London Fire and Emergency Planning Authority.

Mandatory Local Resilience Forum and Risk Register participation could create the setting for increased informal cooperation and information sharing. Due to DHS grant

¹⁰⁶ United Kingdom, HM Government Emergency Preparedness, 25.

¹⁰⁷ U.S. Homeland Security Council, National Strategy for Homeland Security Goal to Prevent and Disrupt Terrorist Attacks, 15.

¹⁰⁸ United Kingdom, HM Government Emergency Preparedness, 25.

¹⁰⁹ Ibid.

requirements involving regional collaboration, increased informal cooperation appears to have occurred in U.S. Urban Area Security Initiative (UASI) regions, but may be almost non-existent outside of the UASI areas.

C. THE CCA PROCESS

Another way that England increases informal information sharing involves completion of a three-step process prior to formally requesting information from another entity. For example, the fire brigade requesting the information must first “be satisfied that it does not already hold the information, either by virtue of a previous request or because of informal information exchange.”¹¹⁰ Second, the fire brigade must ensure that the information is not available through common open-source information networks. Third, the fire brigade must attempt to exhaust all informal networks and agreements already established. In the United States this process would require the requesting fire department to think in terms of its needs based on risk assessments or other local planning efforts (LRFs and RRs in England) or in other words, to be a knowledgeable consumer before requesting information to assist it in meeting specific terrorist-prevention goals or objectives that might not be readily available through established informal relationships. In England, if the local fire brigade is not able to obtain the information needed by conducting the steps above, CCA Regulations 47, 48, and 50 describe the formal request procedures.¹¹¹

¹¹⁰ United Kingdom, HM Government Emergency Preparedness, 26.

¹¹¹ *Ibid.*, Annex 3B, 182.

Figure 5 is the CCA guidance document template for formally requesting information.¹¹²

Information request under the Civil Contingencies Act 2004

Requesting organisation(s)	
Information-holding organisation(s)	
Information requested	
Reason why the information is required in connection with the Act or other civil protection duties (and how the information is likely to be used)	
Date of request	
Date by which information is required	
Form in which information is required	
Place to which information should be sent	
Contact details	

Figure 5. Information Request under the CCA

¹¹² United Kingdom, HM Government Emergency Preparedness, 181.

Once a formal request has been made, a formal response is required. Figure 6 is the CCA guidance document template for response to a formal request for information.¹¹³

Response to information request under the Civil Contingencies Act 2004

Requesting organisation(s)	
Information-holding organisation(s)	
Date of request	
Information requested	
Request accepted?	Yes/no
If no, please set out the exceptions on which you are relying	
If yes, please set out any sensitivities or further background information which might be necessary to ensure the information is properly understood and properly protected	
Date information supplied	
Contact details	

Figure 6. Response to Information Requests under the CCA

When instances of formalized information sharing might be necessary between the U.S. fire service and its homeland security partners, a template similar to the CCA

¹¹³ United Kingdom, HM Government Emergency Preparedness, Annex 3B, 182.

examples in Figures 5 and 6 might be useful. Formal requests between the U.S. fire service and the U.S. information-sharing network may be a good alternative to informal information sharing after every effort has been made to obtain the information through informal networks, processes, or associations.

D. SHARING SENSITIVE INFORMATION

Even though the presumption is that information should be shared informally, the CCA—like the U.S. intelligence community—recognizes that, due to the sensitivity of some information, not all formal or informal information can be shared among all emergency responders. England’s system of communicating sensitive or classified information may have application for use in the post-9/11 U.S. homeland security community.

When justified, the CCA allows for exceptions, exclusions, or denials of sensitive information sharing between information-sharing partners where the disclosure of information would prejudice sensitive information, the disclosure would threaten national security, or the intelligence service does not consent to disclosure.¹¹⁴ This arrangement does not appear to be much different from the current U.S. informal information-sharing experiences. If U.S. information is too sensitive, it can be redacted or modified to protect sources or ongoing investigations while providing the fire service consumer with the information needed to increase awareness or to prepare for specific potential terrorist attacks. The New York City Fire Department *Watchline* appears to be the premier example of this type of fire service homeland security information-sharing product.

In England formalized guidelines identifying the type of sensitive information and consent needed are available. Figure 7 identifies the CCA persons or organizations and the consent necessary for different types of security information.

¹¹⁴ United Kingdom, HM Government Emergency Preparedness, 27.

Type of sensitive information	Person or organisation whose consent is needed
Relates to national security and supplied indirectly or directly by one of the intelligence services	Minister of the Crown OR the intelligence service which supplied the information
Relates to national security but not supplied indirectly or directly by one of the intelligence services	Minister of the Crown OR (a) if the information is contained in a document which has been created by a public authority, that authority; (b) in other cases, the organisation which supplied the information
Relates to public safety and supplied indirectly or directly by one of the intelligence services	Minister of the Crown OR the intelligence service which supplied the information
Relates to public safety but not supplied indirectly or directly by one of the intelligence services	Minister of the Crown OR (a) if the information is contained in a document which has been created by a public authority, that authority; (b) in other cases, the organisation that supplied the information
Relates to the business or other affairs of a person or organisation where disclosure would harm the legitimate business interests of that person or organisation	The person or organisation to whom the information relates
Is personal data (within the meaning of the Data Protection Act 1998) where disclosure would contravene the data protection principles/ section 10 DPA	The individual to whom the information relates

Figure 7. England’s Sensitive Information-Sharing System

In England the fire service and intelligence community utilize a network of fire liaisons (battalion chief–level in the United States) in combination with executive-level officers who have advanced intelligence clearances (fire chief– and deputy chief–level in the United States) to share sensitive information. The outcome is that information or intelligence that may result in “intelligence-led” operations is shared with fire departments and firefighters. Acting as an interface between the fire service and intelligence services, England’s fire chiefs with clearances can filter information to ensure that their organization receives information that is relevant and in a format that is of direct use. Sensitive information coming in a restricted format can only be viewed by liaisons or executive-level chief officers who put plans in place or disseminate information without revealing the sensitive/classified information. Often the chiefs stage resources and put personnel on standby based on the intelligence, and if it turns out to be

a false alarm, the line officers and firefighters do not know precisely why—in effect protecting the source information and preventing undue public alarm while allowing the resources to be prepared.

E. EXAMPLES OF INFORMATION-SHARING UNDER THE CCA

The following are two examples of CCA information sharing among England's Level 1 responders.

One CCA-compliant "intelligence led" information-sharing operation involved ricin. The police had a number of terrorists under surveillance in a range of rented farm buildings in a rural area. Since the terrorists were known to be handling a number of precursor chemicals for the production of ricin intended to form part of a chemical weapon, the local fire department was put on standby before law enforcement specialist units carried out the raid. The communication structures and existence of trusted security-cleared officers meant that the fire department was able to prepare for a response in advance. The terrorists were arrested and are currently being housed in one of England's high security prisons. Fire department hazardous-materials services were not needed. The fire crews deployed did not need to know the specifics of the intelligence operations, but their officers had all the plans and chemical data available to them in case hazardous-materials intervention was necessary.

Another example of a potential terrorist-related incident involved a stolen van containing a radiation source for x-raying bridge structures. It was unclear whether the van had been stolen by terrorists who intended to use it as the basis for a dirty bomb, or whether it had been stolen by thieves who simply did not know what they had. Its description, registration number, and details were immediately transmitted to all emergency services, who were warned to be on the lookout for the van. Specific plans and guidance were put in place to deal with the radiological risks. It turned out to be a non-terrorist crime, and the issue never came to public notice.

The following are two examples of CCA informal information sharing where the local fire brigade took a lead role in an all-hazards environment.

Similar to most U.S. fire departments, the Hereford and Worcester Fire and Rescue Services carry out routine inspections of buildings for fire-code purposes and to make operational plans. The difference is that Hereford and Worcester firefighters regularly share pre-plan information with other agencies and communicate suspicious processes or activities. For example, in a large historic house, the fire plan might involve salvaging of irreplaceable contents (paintings worth millions of dollars) before or in conjunction with fire suppression. The Hereford and Worcester Fire and Rescue representative liaisons, working with police and the owners of the art, ensure that if the firefighters need to conduct salvage operations ahead of or in conjunction with fire-suppression operations, adequate arrangements would be put in place with the police and the owners to secure the contents from theft.

England's reported routine sharing of information between Level 1 and 2 responders has sometimes identified all-hazard issues that would otherwise have gone unnoticed. For example, when considering the impact of major coastal flooding, the fire service identified that the area could lose power. Informal information sharing with Level 2 responders revealed that the loss of power would cause the land drainage pumps to be inoperable, and this would cause flooding on an even greater scale than the initial inundation.

In England, whenever there is a major alert in relation to non-terrorist events, such as floods or avian flu, the lead government agency provides national briefings. The briefings have developed into a system of "common risk information pictures" or CRIP briefings issued to all Level 1 responders. The briefings are provided in a common format regardless of which government agency is handling the emergency.

F. CCA INFORMATION-SHARING MATRIX

The matrix below identifies and grades the CCA relative to the other three information-sharing options.

Information-Sharing Option	Legal Compliance	Political Acceptability	Target Capabilities List Linkage	Operational Impact	Costs
Current U.S. Fire Service	Low/Average	Average	Low	Unacceptable	Low
FDNY Strategy	High	High	High	Average	Average
FSIE	High	Unknown	Good	Unknown	Average
CCA	Unknown	Good	Average	Good	High

Figure 8. Information-Sharing Matrix for the CCA

G. CCA INFORMATION-SHARING FACTORS

Each of the four information-sharing options (current fire service, FSIE, FDNY Strategy, and CCA) examined for this thesis is qualitatively evaluated and then graphically represented by an information-sharing matrix based on five factors. The five factors are legal compliance, political acceptability, target capabilities linkage, operational impact, and cost.

1. Legal Compliance

The common law process used to adopt the CCA in the UK does not appear to be substantially different from the adoption of many post-9/11 homeland security–related U.S. guidelines, policies, strategies, presidential directives, and public laws relating to

counterterrorism information sharing.¹¹⁵ The difference is that the U.S. has chosen not to explicitly require information sharing between the fire service and the homeland security community, while England has. In both countries national crises occurred that necessitated change to lessen or eliminate future man-made and natural disasters. The United States and the United Kingdom both analyzed the issues, sought input from the major stakeholders, developed wide-ranging policies, strategies, and laws, and instituted measures in an effort to lessen or eliminate future catastrophic events.

The result for the U.S. fire service has been an informal information-sharing environment that is non-mandatory, casual and limited in structure and scope. In England the CCA requires fire brigades to participate (and to lead, in the case of London) in the Local Resilience Forums and to share information informally and formally. The majority of the fifty-seven regulations in Part One of the CCA significantly enhance the

¹¹⁵ Bush, Memorandum for the Heads of Executive Departments and Agencies: Guidelines and Requirements in Support of the Information Sharing Environment. “Ensuring the appropriate access to, and the sharing, integration, and use of, information by Federal, State, local, and tribal agencies with counterterrorism responsibilities, and, as appropriate, private sector entities, while protecting the information privacy and other legal rights of Americans, remains a high priority for the United States and a necessity for winning the war on terror. Consistent with section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108 458) (IRTPA), my Administration is working to create an Information Sharing Environment (ISE) to facilitate the sharing of terrorism information (as defined in Executive Order 13388 of October 25, 2005). Section 1016 of IRTPA supplements section 892 of the Homeland Security Act of 2002 (Public Law 107 296), Executive Order 13311 of July 29, 2003, and other Presidential guidance, which address various aspects of information access. On April 15, 2005, consistent with section 1016(f) of IRTPA, I designated the program manager (PM) responsible for information sharing across the Federal Government. On June 2, 2005, my memorandum entitled “Strengthening Information Sharing, Access, and Integration - Organizational, Management, and Policy Development Structures for Creating the Terrorism Information Sharing Environment” directed that the PM and his office be part of the Office of the Director of National Intelligence (DNI), and that the DNI exercise authority, direction, and control over the PM and ensure that the PM carries out his responsibilities under IRTPA. On October 25, 2005, I issued Executive Order 13388 to facilitate the work of the PM and the expeditious establishment of the ISE and restructure the Information Sharing Council (ISC), which provides advice concerning and assists in the establishment, implementation, and maintenance of the ISE. On June 2, 2005, I also established the Information Sharing Policy Coordination Committee (ISPCC), which is chaired jointly by the Homeland Security Council (HSC) and the National Security Council (NSC), and which has the responsibilities set forth in section D of Homeland Security Presidential Directive 1 and other relevant presidential guidance with respect to information sharing. The ISPCC is the main day-to-day forum for interagency coordination of information sharing policy, including the resolution of issues raised by the PM, and provides policy analysis and recommendations for consideration by the more senior committees of the HSC and NSC systems and ensures timely responses. Section 1016(d) of IRTPA calls for leveraging all ongoing efforts consistent with establishing the ISE, the issuance of guidelines for acquiring, accessing, sharing, and using information in support of the ISE and for protecting privacy and civil liberties in the development of the ISE, and the promotion of a culture of information sharing. Consistent with the Constitution and the laws of the United States, including section 103 of the National Security Act of 1947, as amended, and sections 1016 and 1018 of IRTPA...”

probability of informal and formal information sharing with England’s fire service. In the United States DHS funding—primarily in the form of grants to fusion centers and other information-sharing enterprises—has been the catalyst for fire service information sharing related to terrorism. Also in the United States most firefighters do not know what terrorism indicators to look for, when to look for them, or how to share the information.

2. Political Acceptability

At the U.S. national level, the political acceptability of the fire service information sharing (compared to the CCA model that requires cooperation among the homeland security and intelligence communities) is practically non-existent and therefore unknown. From a U.S. fire service perspective the CCA categorization of emergency services such as police, fire, emergency medical, and coastguard agencies into “Level 1 or Core Responders” could occur within the U.S. system with a modification to the National Strategy for Information Sharing.¹¹⁶ Requiring Core Responders to interact with Cooperating Responders through the Local Resilience Forums and requiring the Responder-based forums to develop and publish Risk Registers significantly enhances the probability of information sharing in the prevention or disruption of terrorism.¹¹⁷ Similar models may have application in the United States.

In the United States from 2002 through 2005, President Bush attempted to ensure “the appropriate access to, and the sharing, integration, and use of, information by Federal, State, local, and tribal agencies with counterterrorism responsibilities, and, as appropriate, private sector entities, while protecting the information privacy and other legal rights of Americans,” through the authorization of numerous strategies, processes,

¹¹⁶ White House, National Security Council, National Strategy for Information Sharing, 17.

¹¹⁷ United Kingdom, Cabinet Office, Civil Contingencies Secretariat, Civil Contingencies Act 2004, Short Guide, Annex A. Category 2 or cooperating responders include the following disciplines: electricity distributors and transmitters, gas distributors, water and sewerage undertakers, telephone service providers (fixed and mobile), network rail, train operating companies (passenger and freight), London Underground, transport for London, airport operators, harbour authorities, highways agency, strategic health authorities, and health and safety executive.

and systems to facilitate the sharing of terrorist related information.¹¹⁸ The CCA is probably a less complex and more efficient method of enhancing terrorism prevention and preparation through collaboration and information sharing within government agencies and of incorporating public and private-sector partners into the process. Many of the U.S. enterprises are beginning to mature, and the U.S. fire service appears to be an ancillary partner, especially at the state and local levels including fusion centers.

3. Target Capabilities Linkage

Of the four target capabilities selected for this project, England's current fire service role addressed three of the four target capabilities fully and the CBRNE capability partially. Intelligence/information sharing and dissemination U.S. DHS target capability issues applicable to CCA Part One regulations were found in regulations 18, 45-53.¹¹⁹ Relating to CBRNE detection, the CCA did not address detection issues specifically but did refer to radiological planning and public information in Regulation 12.¹²⁰ Regulations similar to the information gathering and recognition of indicators target capabilities were identified in regulations 11, 15, 33.¹²¹ Regulations that had applicability to the warnings, intelligence analysis, and production target capabilities were found in regulations 20 and 28 through 35.¹²²

4. Operational Impact

In England the 2006 National Capability Survey suggested that local responders have made good progress in effectively implementing the Civil Contingencies Act.¹²³ Regarding cooperation and information sharing the survey indicated, "The vast majority

¹¹⁸ Bush, Memorandum for the Heads of Executive Departments and Agencies: Guidelines and Requirements in Support of the Information Sharing Environment.

¹¹⁹ United Kingdom, Cabinet Office, Civil Contingencies Secretariat, Civil Contingencies Act 2004, Part 1 Local Arrangements for Civil Protection. Regulation 18: [Provision of information relating to assessment of risk to other responders](#); Regulation 32: [Identification of Category 1 responder with lead responsibility for warning, informing and advising](#); Regulations 45-53.

¹²⁰ Ibid., Regulation 12, [Existing emergency planning duties](#).

¹²¹ Ibid.

¹²² Ibid.

¹²³ United Kingdom Resilience, Emergency Preparedness, Progress on Implementation of the Civil Contingencies Act.

of Local Resilience Forums and supporting task groups are up and running and functioning effectively. Almost all local responders are happy that Local Resilience Forums are providing the right level of engagement to enable members to perform the tasks mandated by the Act.”¹²⁴ Conversely, there has been discussion among NPS cohorts 0705 and 0706 that, while the Local Resilience Forums appear to have well-organized and robust planning components, some British fire chiefs indicated to NPS cohort participants that the forums are dominated by the law enforcement representatives, and in reality there is a lack of true collaborative planning and preparation. In addition there may be limited training and exercising coordinated by these councils, which leads to operational disconnects. Like many plans and programs in the U.S. homeland security community, the CCA concepts and plans may appear to be effective, but the practical application to current operations may not be adequate.

5. Costs

A review of available literature indicates that the CCA not been audited for cost in England. Scotland is auditing its version of the CCA, but the results will not be available until sometime in 2009. It appears that the costs of implementation of the CCA were primarily soft labor costs and were incorporated into the current budgets for the organizations participating.

H. RECOMMENDATIONS

Review of the CCA Part One regulations and related guidance documents and a comparison with literature reviewed for this thesis reveals one difference between the U.S. and England’s fire service information-sharing environment: England’s fire service information sharing is mandated and consolidated primarily in one document, the CCA. Under the Civil Contingencies Act, Level 1 (core) and Level 2 (cooperating) responders are mandated to share information with other Level 1 and 2 responders.¹²⁵ The sharing of

¹²⁴ United Kingdom Resilience, Emergency Preparedness, Progress on Implementation of the Civil Contingencies Act.

¹²⁵ United Kingdom, HM Government Emergency Preparedness, 24.

informal and formal information is recognized as being good practice as well as a critical element of preventing man-made or natural disasters.¹²⁶

The U.S. fire service has a history of more than two hundred years of successfully reducing unwanted fires by leading collaborative prevention-oriented risk assessments and pre-planning processes based on open-source informal and formal information sharing. Building on the U.S. fire service history of fire prevention, incorporating the CCA information-sharing requirements (in which England’s fire departments play a role) may increase information sharing among U.S. homeland security partners.

The current National Strategy for Information Sharing (NSIS) “Sharing Information with State, Local and Tribal Governments” section should be modified to include the language shown below (extrapolated from the CCA Part One Regulations 55-57, “Role of London Fire and Emergency Planning Authority”). A new open-source information-sharing plan led by local fire departments may improve formal and informal information sharing between the U.S. fire service and other homeland security partners and may potentially prevent or disrupt terrorism.

Current NSIS Language:

To implement recommendations developed pursuant to Guideline 2 of the President’s Guidelines, and as key participants in the information-sharing mission, State, local, and tribal entities are encouraged to undertake the following activities, in appropriate consultation and coordination with Federal departments and agencies.¹²⁷

Recommended Language:

A. Role of local or regional fire service authority

In communities with established fire service, it shall be the responsibility of fire chief of the fire service to:

(1) Ensure that a collaborative open-source information-sharing plan is created and maintained. The fire chief shall be responsible for ensuring that all agencies, public and private, associated with the area homeland security, emergency services, and critical infrastructure sectors identified in the National Response Framework participate. The information-sharing

¹²⁶ United Kingdom, HM Government Emergency Preparedness, 24.

¹²⁷ White House, National Security Council, National Strategy for Information Sharing, 17.

plan will include informal and formal information-sharing systems or processes associated with potential man-made or natural disasters, including terrorist attacks for the pre-defined area, urban area, state homeland security region, or other mutually accepted area(s).

(2) On behalf of all relevant homeland security, emergency services, and critical infrastructure sector participants who have functions that are exercisable in the identified area, the fire department will be the authority having jurisdiction and will take the lead responsibility for exercising the information-sharing plan in relation to area-wide emergencies in accordance with the Homeland Security Exercise and Evaluation Program;¹²⁸ and

(3) At the request of relevant homeland security, emergency services, or critical infrastructure sector partners who have functions that are exercisable in the area, assist sector and private partners in –

(i) carrying out exercises for the purpose of ensuring that the information-sharing plan maintained by that relevant sector or partner is appropriate for the risk(s);

(ii) the inter-sector training of responders or other persons for the purposes of ensuring that the plan is actionable and effective.¹²⁹

B. Role of other homeland security, emergency services, and critical infrastructure sector partners

Homeland security, emergency services, and critical infrastructure sector partners who have functions that are exercisable in the pre-determined area, shall cooperate with the fire service authority having jurisdiction in connection with the performance by that authority of its functions under paragraph A(1).

¹²⁸ U.S. Department of Homeland Security, Homeland Security Exercise and Evaluation Program Toolkit.

¹²⁹ Ibid.

I. CONCLUSION

The CCA encourages informal information sharing over required or formal information sharing based on the presumption that information should be shared, but the release of some information—and of information to some audiences—should be controlled.¹³⁰

It is the responsibility of Level 1 and 2 responders to understand what should be controlled and how to categorize the various types of information; how the different types of information can be used; how to obtain consent from other homeland security partners; and the limits on disclosure of information.¹³¹

On the other hand, in the United States, information sharing is not required by the various homeland security grant programs available to America's core responders. The net result is that less information is shared in the United States, which increases the risk of successful terrorist attacks. Also, as a consumer of potential terrorist information, the lack of information sharing with the U.S. fire service inhibits optimum preparation and response capabilities as well as citizen and firefighter safety.

¹³⁰ United Kingdom, HM Government Emergency Preparedness, 24–33.

¹³¹ *Ibid.*, 24.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. ANALYSIS AND RECOMMENDATIONS

There is nothing more difficult to take in hand, more perilous to conduct, or more uncertain in its success, than to take the lead in the introduction of a new order of things.

— Niccolò Machiavelli¹³²

The fundamental qualitative premise underlying this thesis is that there are lessons to be learned by the U.S. fire service from existing international, national, and local information-sharing partnerships. This chapter consolidates and analyzes the value of contemporary smart practices.

Based on the findings of this thesis, U.S. fire personnel could serve as both collectors and consumers of information during the prevention, protection, response and recovery missions. They may also assist the information-sharing community through uniform communication of standardized potential terrorist indicators encountered during their normal operations (emergency and non-emergency).

Much like fire brigades in England, U.S. fire departments can use information to evaluate the likelihood of a threat, bring diversified organizations together, and pre-plan a response in the event of an attack. Following an attack, fire marshals may be capable of classifying and distributing vital information to other first responders and other homeland security agencies. Fire marshals may also be a good resource in post-incident investigations leading to arrests, as exemplified in the following case synopsis.

In 2006, a group of Phoenix, Arizona metro-area fire marshals cooperated with the Phoenix Joint Terrorism Task Force in the investigation of an ecoterrorist who set fire to luxury homes under construction in an attempt to stop suburban sprawl.¹³³

¹³² Machiavelli, <http://www.answers.com/topic/quote-4?author=Machiavelli,%20Niccolo&s2=Niccolo%20Machiavelli#copyright>.

¹³³ Churay, Assistant Special Agent in charge of the FBI's Phoenix division, testimony to House Committee on Governmental Reform, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, March 22, 2002.

A. ANALYSIS CRITERIA

Using the qualitative criteria identified below, consideration was given to local, national and international smart practices, gaps and potential blind spots applicable to the U.S. fire service information-sharing environment. The criteria used to compare and contrast the current fire service information sharing with the FDNY Strategy and FSIE and the CCA are listed in Chapter I.

B. CURRENT U.S. FIRE SERVICE, FDNY, FSIE AND CCA INFORMATION-SHARING MATRIX

Information-Sharing Option	Legal Compliance	Political Acceptability	Target Capabilities List Linkage	Operational Impact	Costs
Current U.S. Fire Service	Low/Average	Average	Low	Unacceptable	Low
FDNY Strategy	High	High	High	Average	Average
FSIE	High	Unknown	Good	Unknown	Average
CCA	Unknown	Good	Average	Good	High

Figure 9. Information-Sharing Matrix

The following matrices and information-sharing criteria discussions are organized from highest to lowest for each measure. For example, the matrix for legal compliance is ordered beginning with the FDNY, FSIE, current U.S. fire service, and finally the CCA.

1. Legal Compliance

Information-Sharing Option	Legal Compliance
FDNY Strategy	High
FSIE	High
Current U.S. Fire Service	Low/Average
CCA	Unknown

Figure 10. Legal Compliance

The FDNY Strategy received the highest value due to the use of accepted local, state, and federal strategies, laws, and guidelines. (At the time of this writing, the FDNY Strategy was the only completed U.S. fire service information-sharing document that had received and passed a legal review.)

According to Townsend, “The FSIE is being designed in compliance with all Federal laws and will be reviewed by DHS Privacy, Civil Rights/Civil Liberties, Security, and DHS OGC, as well as the DOJ Global Justice Information Sharing Initiative. We are also adhering to all criminal intelligence laws, when applicable.”¹³⁴ Based on my review of the current FSIE documents and Townsend’s previous work with the FDNY Strategy, I anticipate that the finished FSIE products will meet or exceed the established legal requirements.

The legality of the current information-sharing environment is questionable, since most firefighters do not know what terrorism indicators to look for, when to look for them, or how to report them. Given that most firefighters are not actively aware of or engaged in reporting potential terrorist indicators, the fire service has not created any significant legal exposure or civil liberties violations. Based on Masse’s findings, the fire service has a legal responsibility to report suspicious activity.¹³⁵

The CCA information collection and sharing structure was based on the United Kingdom’s system of government and did not address the legality of information collection. The CCA exceeded the three other options relating to legal information sharing of open-source, sensitive, and classified information between the core and cooperating responders.

¹³⁴ Townsend, personal communication with author, December 16, 2008.

¹³⁵ Masse, “Homeland Security Intelligence,” 12.

2. Political Acceptability

Information-Sharing Option	Political Acceptability
FDNY Strategy	High
CCA	Good
Current U.S. Fire Service	Average
FSIE	Unknown

Figure 11. Political Acceptability

The FDNY Strategy incorporates FDNY policy-level fire officers who use the requirements and guidelines of numerous accepted local, state, and federal documents.

The CCA may be the most politically comprehensive single-source fire service information-sharing document analyzed for this thesis. As stated earlier, in the October 2007 U.S. National Information Sharing Strategy,¹³⁶ the U.S. fire service is not identified anywhere in the forty-page document.¹³⁷ In England's CCA, the fire service roles and responsibilities regarding information sharing are clearly defined at the national, regional, and local levels, and in the case of the London fire brigade, the fire service is mandated to take a lead role.

Applicability of the current fire service information-sharing environment to the U.S. public, policy groups, labor unions, governmental agencies, and other related organizations is in the early stages of development. At the national level, Department of Homeland Security Secretary Michael Chertoff advocated for the inclusion of firefighters in state and local fusion centers.¹³⁸

The December 2008 draft of the FSIE CONPLAN analyzed in Chapter III appears to be a more practical and robust direction for the U.S. fire service.

¹³⁶ White House, National Security Council, National Strategy for Information Sharing, 17.

¹³⁷ Ibid.

¹³⁸ Chertoff, remarks at the International Association of Fire Chiefs, October 26, 2007.

3. Target Capabilities List Linkage

Information-Sharing Option	Target Capabilities List Linkage
FDNY Strategy	High
FSIE	Good
CCA	Average
Current U.S. Fire Service	Low

Figure 12. Target Capabilities List Linkage

The FDNY used the fifteen planning scenarios to enhance their protection and response missions and to compete for DHS grant funding. The FDNY Strategy exceeded the four information-sharing target capabilities criteria by identifying the role of the FDNY in all thirty-six target capabilities identified in the National Preparedness Guidelines.

The current FSIE CONPLAN does not specifically address target capabilities. The FSIE is given a “Good” rating based on information received from the DHS I&A State and Local Program Office that indicated national planning scenarios, attack timelines, and universal adversary profiles are being used to guide the information/intelligence requirements identification, and the target capabilities list is being used to guide the mechanisms of identification, technical assistance, and training.”¹³⁹

Of the four information-sharing target capabilities selected for this project, the CCA addresses three of the four target capabilities fully and the CBRNE capability partially.

Of the four information-sharing target capabilities selected for this project, the current fire service role in the homeland security information-sharing environment formally utilized only the CBRNE detection target capabilities component through the DHS FY 2003 State Homeland Security Grant Program (SHSGP) Program.

¹³⁹ Townsend, personal communication with author, December 16, 2008.

4. Operational Impact

Information-Sharing Option	Operational Impact
CCA	Good
FDNY Strategy	Average
FSIE	Low
Current U.S. Fire Service	Unacceptable

Figure 13. Operational Impact

In England, the 2006 National Capability Survey suggested that local responders have made good progress in enhancing the operational information-sharing impact of the Civil Contingencies Act.¹⁴⁰ “The vast majority of Local Resilience Forums and supporting task groups are up and running and functioning effectively. Almost all local responders are happy that Local Resilience Forums are providing the right level of engagement to enable members to perform the tasks mandated by the Act.”¹⁴¹

The FDNY Strategy may have relevance for increasing the U.S. fire service operational impact in the all-hazards information-sharing environment. For example, the FDNY Bureau of Investigation maintains numerous important connections with the homeland security community; they are implementing a network-centric information-sharing-based command system that has the potential to significantly increase real-time information sharing among a myriad of local, state, and federal partners; and they communicate national and local information to tens of thousands of fire personal and homeland security partners through *Watchline*.

The FSIE CONPLAN contains specific accountability components for the management of the information-sharing tasks. If the current information-sharing gap is

¹⁴⁰ United Kingdom Resilience, Emergency Preparedness, Progress on Implementation of the Civil Contingencies Act.

¹⁴¹ Ibid.

the catalyst for increased information sharing with the homeland security community, then the current FSIE CONPLAN\ is moving towards enhancing the operational impact.

The operational impact of the current information-sharing environment was difficult to quantify. The anecdotal successes associated with information sharing among homeland security and the fire service, combined with the recent emergence of strategies and technical assistance programs, suggests that there is a heightened awareness of the potential for firefighters as sensors of opportunity that identify potential terrorist activities and as consumers of information for specific terrorist targets. Considering that we are at war on two fronts and that domestic and international terrorists have sworn to cripple the United States through terrorism, the current organized information sharing between the fire service and homeland security community is unacceptable.

5. Costs

Information-Sharing Option	Costs
Current U.S. Fire Service	Low
FDNY Strategy	Average
FSIE	Average
CCA	Average

Figure 14. Costs

The United States spends approximately \$100 billion per year on homeland security.¹⁴² Homeland security expenses include federal, state, and local law enforcement, emergency medical, public works, and fire services.¹⁴³ Generally speaking, information regarding the national effort to enhance homeland security through information sharing with the fire service was not available but may involve some relatively small fiscal costs. Most costs appeared to be absorbed by current fire and intelligence personnel responsible for the collection, analysis, and dissemination of information.

¹⁴² White House, National Strategy For Homeland Security, xxii.

¹⁴³ Ibid.

The cost of developing and implementing the FDNY Strategy appears to have been incorporated into the operating budget and supplemented with DHS grant funding for equipment. For example, the cost of producing and distributing *Watchline* as well as the Network-Centric Command System appear to have been developed within the FDNY's FY 06-07 operating budget.

Data identifying costs were not available in the FSIE CONPLAN. Based on information within the CONPLAN framework, requirements, mechanisms, technical assistance and training, the costs may be reasonable considering the DHS budget.

A review of available literature indicated that the CCA not been audited for cost in England. Scotland is auditing their version of the CCA, but the results will not be available until sometime in 2009. The costs of implementation of the CCA may have been primarily soft costs incorporated into the current budgets for the public and private organizations that participated.

C. RECOMMENDATIONS

The following recommendations considered existing programs, political considerations, and financial constraints associated with the four information-sharing options.

1. Current Fire Service Information-Sharing and FSIE Recommendations

Despite all our collective homeland security efforts since 9/11, it appears that the only homeland security partners with established access to information are those with law enforcement connections. If the fire service is to increase its use of all-hazards information in its decision cycles, then homeland security information-sharing partners may wish to open up the information-sharing system both culturally and politically. The best intelligence should be provided to the widest group of decision-makers, including (perhaps especially) those with no historical information-sharing relationships.

The four indicators listed below (as discussed in Chapter III) were common in the more than one hundred fifty current homeland security terrorist-related indicators studied. The four common terrorist indicators could be printed on business cards with contact information of the local information-sharing partner (fire marshal, law enforcement, JTTF, fusion center) on the other side of the card. The cards could then be distributed through the representative organizations such as the International Association of Firefighters, International Association of Fire Chiefs and the National Volunteer Fire Council.

1. Suspicious Behavior - Especially unusual nervousness for the situation and inappropriate or lack of eye contact.

2. Unusual supplies for occupancy type (structure or vehicle) - Especially storing large amounts of chemicals, cash, electronics.

3. Unusual documents for the occupancy type - Especially maps, books, blueprints, literature... of critical infrastructures.

4. Intelligence gathering - Especially surveillance, taking pictures, video, notes, asking questions, attempting to gain access.

A second recommendation is to use local fire marshals as planning-and-logistics officers, specifically for fire personnel (and their families) during extended all-hazards responses lasting longer than two operational periods or twenty-four hours. This will enhance information sharing between families and response personnel. This recommendation may reduce anxiety for fire personnel and their families during high-profile heavily media-covered events.

Regarding the FSIE, the FSIE CONPLAN recommendation—of a national network of fire service and homeland security organizations that share all-hazard information and intelligence in a collaborative effort to enhance the national prevention, preparation, response, and recovery missions—should be implemented. The FSIE should also continue to work within the Global Justice Information Sharing Initiative to ensure that fire service fusion center liaisons (or representatives) act as nodes and that the fusion centers (UASI and state) act as hubs for receiving and disseminating relevant information in a timely and actionable manner.

A final FSIE significant information-sharing recommendation is to increase the current level of information sharing across the fire service through social networking. At the time of this writing, the DHS I&A is designing a homeland security information network portal for fire service-wide dissemination of all locally and federally generated information and intelligence products that relate to the fire and emergency services.¹⁴⁴ If the portal is user-friendly and the information is concise, informative, and pertinent to current fire service all-hazards missions, many fire personnel will use the information to augment their prevention, preparation, and response activities.¹⁴⁵

2. FDNY Strategy Recommendations

Many of the strategies and tactics that FDNY developed for responding to, mitigating, and preventing all-hazard disasters can be leveraged by other emergency services sectors, especially the fire services. The FDNY's fifteen thousand fire personnel responded to over four hundred thousand emergencies and conducted more than one hundred sixty thousand building inspections in 2007.¹⁴⁶ This volume of activity and resources allowed the FDNY to develop strategic approaches and operational activities in preparation, prevention, and response to all hazards.¹⁴⁷ The FDNY Strategy identified numerous ways in which firefighters can produce and consume practical preparedness and response information. Increased synchronization and communication with the homeland security community is one tactic that may enhance the FDNY's and other U.S. fire departments' ability to fulfill their core missions of saving lives and property. A number of the following FDNY strategic objectives may have application to small and large fire departments across the United States.

One strategic objective involves the use of fire marshals as homeland security liaison officers with homeland security partners such as the JTTF, TWIG, FBI, or fusion

¹⁴⁴ Townsend, personal communication with author, December 16, 2008.

¹⁴⁵ Fire Department City of New York, "Terrorism," 19.

¹⁴⁶ Fire Department City of New York, Vital Statistics. 2008.

¹⁴⁷ Fire Department City of New York, "Terrorism," 21.

centers. The fire marshals/security liaison officers would share information in preparation for generalized or non-specific terrorism threats and participate in the investigation of fire or explosion-related terrorism incidents. Fire marshals may be useful at potential terrorist emergency scenes to ensure the safety of workers relating to secondary devices and scene control.

The evolution of FDNY's integrated all-hazards Incident Command System-based information-sharing system for all multi-discipline, multi-agency emergency responses and high-profile or target-rich special events may enhance the current national incident management system currently required by the DHS.

If successful in NYC, consider incorporating the FDNY Network-Centric Command System into the national incident management system for use throughout the U.S. fire service to enhance real-time information sharing among multi-disciplinary operations within a large-scale command. Another recommendation—prompted by the idea of FDNY's Network-Centric Command System—is to enhance information collection and sharing through the use of a diverse suite of small unmanned aerial vehicles (UAVs) for reconnaissance and possibly intervention operations. The Naval War College's Global Hawk or a similar system might be leveraged by the fire service and homeland security partners for real-time information sharing during pre-planning, response, and recovery missions on large scale, natural or man-made disasters.

Finally, with permission of the FDNY and working in conjunction with the DHS/FEMA Emergency Management and Response Information Sharing Analysis Center, modify and expand the distribution of the FDNY *Watchline* for distribution to the U.S. fire service. A national *Watchline*-type program could be coordinated and managed through U.S. Fire Administration. Using the fusion centers as venues for a *Watchline*-type product might enhance relationship building between the fire service and the intelligence community working in the state and regional fusion centers.

3. CCA Recommendations

The primary recommendation derived from the CCA for this thesis was the modification of the current National Strategy for Information Sharing (NSIS) "Sharing

Information with State, Local and Tribal Governments” section to include language extrapolated from the CCA Part One Regulations 55-57, “Role of London Fire and Emergency Planning Authority.” Modification of the NSIS may enhance information sharing through the establishment of formalized local and regional networks similar to those found in England. Unlike England, U.S. information sharing is currently not required among America’s core responders, which may increase the risk of terrorist attacks in the United States. Also, as a consumer of potential terrorist information, the lack of information sharing inhibits optimum preparation and response by the U.S. Fire Service. The recommended language for the NSIS is located in Chapter V.

Other recommendations derived from the CCA involve the development of national U.S. guidance templates for formally requesting information after the CCA three-step informal information-sharing process is not successful. When instances of formalized information sharing might be necessary between the U.S. fire service and its homeland security partners, templates similar to those in Chapter V, Figures 5, 6, and 7 might be useful.

D. CONCLUSION

The international, national, and local smart practices consolidated in this chapter may provide the catalyst for increased systematic, operational, and legal information sharing between the fire service and homeland security partners. Chapter VII discusses strategic planning to enhance information sharing through such practices as those recommended in this thesis between the U.S. fire service and the homeland security information-sharing community.

VII. STRATEGIC PLANNING TO IMPROVE INFORMATION-SHARING BETWEEN THE FIRE SERVICE AND HOMELAND SECURITY COMMUNITY

There is nothing permanent except change.

—Heraclitus of Greece¹⁴⁸

A. WHY STRATEGIC PLANNING?

Fire service/homeland security information-sharing strategic planning is about leading change through the creation of a roadmap to the preferred information-sharing future. Whether relying on the formal concepts, tools, and procedures such as those in the *Blue Ocean Strategy* and *Strategic Planning for Public and Nonprofit Organizations* to get to the preferred future, or using more organically oriented approaches such as those identified in *The Starfish and the Spider*, the results of successful strategic planning are fundamentally based on three leader-orchestrated components.¹⁴⁹ In effective strategic planning the leader should:

1. Have the capacity to develop and mobilize stakeholders around a shared vision,
2. Ensure effective translation of the vision into concrete outcomes, and
3. Demonstrate a commitment to integrity and ethics through the practice of accountability.¹⁵⁰

As Bryson indicated, “There is no substitute for leadership.”¹⁵¹ My experience of twenty-seven years in the fire service demonstrates that having the right type of leader(s)

¹⁴⁸ Heraclitus, <http://www.toinspire.com/author.asp?author=Heraclitus+of+Greece>. Reportedly an observation made by Heraclitus of Greece in 513 B.C.

¹⁴⁹ Kim and Mauborgne, *Blue Ocean Strategy*; Bryson, *Strategic Planning for Public and Nonprofit Organizations*; Brafman and Ceckstrom, *The Starfish and the Spider*.

¹⁵⁰ World Bank Institute, Background Notes on Leadership.

¹⁵¹ Bryson, *Strategic Planning*, 327.

to lead and manage organizational change (in this case, U.S. fire service and homeland security information-sharing) is critical to preventing future terrorism.

Another important component is systematically identifying the gap(s) between where an organization is and where it should be. Having identified the gaps, the next step is developing the road map to get the organization where it needs to be. Fundamentally, the strategic-planning process is really about figuring out where you are, where you want to be, and how you will get there – a bit like planning a career, a vacation, or any voyage to a new destination.¹⁵²

While many cultural, financial, environmental, and process factors must align to increase information sharing between the fire service and the homeland security community, the strategic-planning tipping-point is the point at which dissatisfaction with the current information-sharing environment is greater than moving toward a new or different destination. Many times it is a real or perceived crisis that creates the tipping point and corporate desire to reach a strategic goal. In the case of sharing information with non-traditional intelligence partners, the tipping point may have been 9/11. The 9/11 Commission reported on the failure of the intelligence community to “connect the dots” that may have prevented the terrorist attacks on September 11, 2001.¹⁵³ Could the fire service have assisted in “connecting the dots”? Could the consequences of continued ambiguity related to one million fire personnel collecting, disseminating, and receiving potential terrorist-related “dots” result in future catastrophic loss of life to our citizens and firefighters? We may never know the answers to those questions, but with increased information sharing will come the increased potential for terrorism prevention or mitigation. As exemplified in this thesis, the development of new strategies or roadmaps for sharing potential terrorism-related information initially, and more recently all-hazards information, has assisted the U.S. and England’s fire service in preparing for and

¹⁵² Bryson, *Strategic Planning*, 7.

¹⁵³ National Commission, *9/11 Commission Report*, 426.

responding to man-made and natural disasters. But successful strategic planning is significantly limited without appropriate catalytic leadership as well as the confidence and participation of the crowd.¹⁵⁴

A strong strategic-planning team can successfully facilitate the identification of gaps and then effectively communicate the needed change. A planning team may use a method similar to Bryson's more traditional *Strategic Planning for Public and Nonprofit Organizations*.¹⁵⁵ Or, in some circumstances a strategic-planning team may facilitate the move to a more decentralized flat strategy similar to those used in the development of the Internet and Al Qaeda, as exemplified by Ori Brafman, and Rod Ceckstrom in *The Starfish and The Spider*.¹⁵⁶ The more traditional approaches are those outlined in *Strategic Planning for Public and Nonprofit Organizations* and the *National Fire Academy Strategic Management of Change, Change Management Model*. (The National Fire Academy Model has served me well in leading changes at national, state, and local levels.¹⁵⁷ The *Strategic Planning for Public and Nonprofit Organizations* process is also similar to the *Weidner Planning for Results* performance-based strategic-planning and budgeting system I have used to facilitate or participate in strategic planning and performance-based budgeting.¹⁵⁸)

The current fire service information-sharing environment represents an informal decentralized system similar to those described in *The Starfish and The Spider*; most fire departments are fairly autonomous and experience change independent of other fire departments (who can participate in the change or not). For example over eight hundred

¹⁵⁴ Bryson, *Strategic Planning*, 338. The crowd is defined as “stakeholders with little interest or power.” In the context of information sharing between the fire service and the homeland security community, the crowd is the more than one million U.S. firefighters serving throughout the United States, from the most densely populated urban areas to the vast tracks of wild land.

¹⁵⁵ Bryson, *Strategic Planning*, 327.

¹⁵⁶ Brafman and Ceckstrom, *The Starfish and the Spider*, 141–142.

¹⁵⁷ The attacks of 9/11 as well as the anthrax incidents were the catalysts for strategic planning. As Chairperson of the National Fire Protection Association (NFPA) Technical Committee on Hazardous Materials Protective Clothing and Equipment (NFPA 1991 and 1992), I used strategic planning after the World Trade Center, Pentagon, and anthrax attacks to lead in the development of a new NFPA Standard based on incident specific risk assessments.

¹⁵⁸ Weidner, *Planning for Results*. In Oklahoma City the name of the system was changed to “Leading for Results.” I am one of a cadre of facilitators that assist the twenty-five city departments in strategic planning and budgeting.

thousand of America's more than one million firefighters are volunteers, and most answer to their local policy group. They are loosely affiliated with other fire departments around the world through a fundamental ideology or creed based on saving lives and protecting property for the greater good.¹⁵⁹

The smart practices recommended in this thesis may provide discussion points for increased information sharing between the fire service and homeland security partners during the strategic-planning process.

B. CREATING THE PREFERRED FUTURE

As discussed, the current state of information sharing between the fire service and the homeland security community has considerable gaps that, if not remedied, may result in catastrophic loss of life and property. Figure 15 (below) is a "Blue Ocean Strategy"-based diagnostic tool that compares the current status of information sharing between where the fire service and the homeland security community are and where they could be. The diagnostic tool also includes indicators to gauge information sharing.¹⁶⁰

In the upper right-hand corner of the diagnostic tool is the strategic application of the blue line. The strategic application statements attempt to capture important macro-level functions for creating comprehensive information-sharing networks between the fire service and the homeland security community. The strategic applications used in concert with fire service information-sharing power vs. interest grid participants became the underpinning upon which the planning process section of this chapter was constructed.

The lower half of the tool is the strategy canvas. The strategy canvas is both a diagnostic and a visual framework for building a compelling strategy to increase information sharing. The strategy canvas serves two purposes. First, it graphically communicates the current state of activity in the information-sharing environment (red line), and second, it shows the potential level of information sharing between the fire

¹⁵⁹ National Fire Protection Association, *The United States Fire Service*, 1; U.S. Fire Administration, *Fire Departments*.

¹⁶⁰ Kim and Mauborgne, *Blue Ocean Strategy*, 25-44.

service and the homeland security community (blue line) that is possible, based on the findings and recommendations of this thesis. The space between blue and red lines on the strategy canvas depicts the gap between the current and recommended future of fire service information sharing. The indicators identified on the horizontal axis of the strategy canvas list the five measures defined in Chapter I and used throughout this thesis to evaluate the current status of fire service information sharing, the FDNY Strategy, and the CCA.

In the upper left-hand corner of the tool (Figure 15) is a two-by-two square that identifies four actions that may assist in improving information sharing. The following questions were considered in developing the recommended actions identified in the two-by-two square:¹⁶¹

1. Which current fire service/HS information-sharing factors should be **eliminated**?
2. Which fire service/HS information-sharing factors should be **reduced** well below the existing environment?
3. Which fire service/HS information-sharing factors should be **increased** well above the existing environment?
4. What new aspects should be **created** between the fire service and HS information-sharing community?

1. Elimination

Based on the DHS/U.S. Fire Administration Fire Service Intelligence Enterprise Concept Plan (CONPLAN), the CONPLAN may be a venue to consolidate the current ad hoc systems and lack of open-source information-sharing through the dissemination of intelligence from the intelligence community to state and local fire agencies using state and local fusion centers or joint terrorism task forces.¹⁶²

¹⁶¹ Kim and Mauborgne, *Blue Ocean Strategy*, 29.

¹⁶² U.S. Department of Homeland Security, Office of Intelligence and Analysis, State and Local Program Office, Draft Fire Service Intelligence Enterprise Concept Plan, 5.

2. Reduction

Since the FSIE initiative is part of the larger DHS Intelligence and Analysis Enterprise, the FSIE could become the point of coordination to reduce the sector-specific focus, compartmentalization of information and security-classification challenges. The FSIE may further decrease the reduction challenges identified through collaboration with the eighteen critical infrastructure/key resource sectors.¹⁶³

3. Increase

The integration, cross-cutting approaches, legal, and operational issues for the fire service, law enforcement, ACLU, and others may be increased through the inclusion of non-traditional partners into the FSIE project generally and the CONPLAN specifically.

4. Creation

The draft CONPLAN recommends specific standardized systems and processes for organized and administrated information sharing across the homeland security, fire service, and private sectors using state and local fusion centers as nodes.

¹⁶³ U.S. Department of Homeland Security, Office of Intelligence and Analysis, State and Local Program Office, Draft Fire Service Intelligence Enterprise Concept Plan, Appendix B-4.

5. Fire Service/Homeland Security Information-Sharing Tool

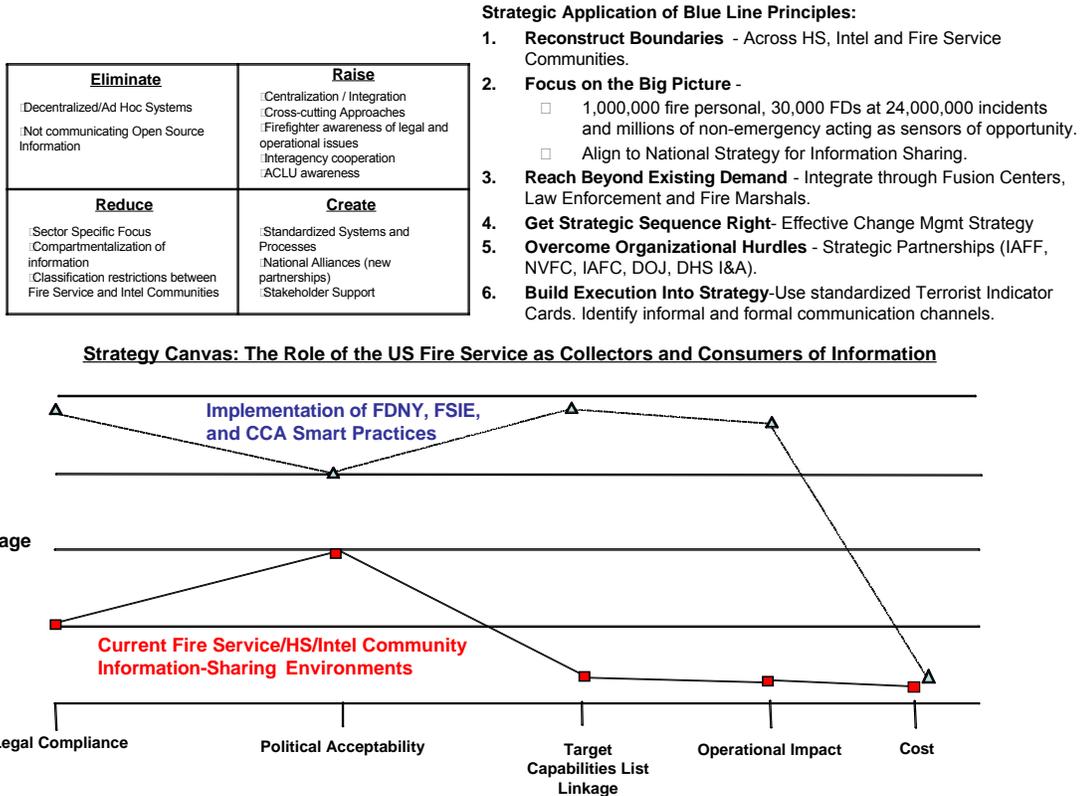


Figure 15. Fire Service/Homeland Security Information-Sharing Tool

Figure 16 is a Fire Service Power versus Interest Grid that was designed to help identify the key participants for the planning process section of this chapter. The key actors are the organizations whose interest and power base must be taken into account in order to successfully overcome fire service/homeland security strategic-planning challenges.¹⁶⁴

The Fire Service Power versus Interest Grid (Figure 16) arranges fire service information-sharing stakeholders in a two-by-two matrix that was based on the Blue Line (preferred future) political acceptability and operational impact indicators identified in

¹⁶⁴ Bryson, *Strategic Planning*, 337–340.

the U.S. fire service. The current homeland security information-sharing community was selected as the subjects due to their interest in mitigating future terrorism through partnerships with nontraditional intelligence-cycle associates.¹⁶⁵

The DHS Intelligence and Analysis Division was selected as the context setters because the DHS Intelligence and Analysis State and Local Section in conjunction with the Department of Justice Global Justice Information Sharing Initiative is currently working to increase firefighter participation in concert with other critical infrastructure and key resource sectors.¹⁶⁶ The crowd is the more than one million fire personnel /stakeholders serving in over thirty thousand fire departments throughout the United States. The crowd currently has little awareness, interest, or power regarding this issue, but with the successful implementation of the terrorist indicator cards and data entry into the National Fire Information Reporting System in combination with the use of fire marshals as homeland security liaison officers, and possibly the implementation of signal intelligence recommendations, the crowd's interest and power should increase.

Below are initial planning-process recommendations based the consolidation of the Fire Service/Homeland Security Information Sharing Tool Blue Line Strategic Application (Figure 15) and the Power vs. Interest Grid (Figure 16).

¹⁶⁵ U.S. Office of Domestic Preparedness, *Guidelines for Homeland Security, Prevention and Deterrence*, 13. The Office of Domestic Preparedness (ODP) defines the Homeland Security Intelligence Cycle as “the process by which information and data is collected, evaluated, stored, analyzed, and then produced or placed in some form for dissemination to the intelligence consumer for use. The cycle consists of: consumer, collector, evaluation, analysis, production, dissemination, consumption, consumer.” According to the ODP the consumer begins and ends the intelligence cycle. To enhance information sharing and prevent terrorism, the ODP Guidelines recommend that “all appropriate agencies and organizations (Public Health, EMA, EMS, Fire, selected Private Sector, etc.) at all tiers (local, regional, and state) receive restricted information on a need-to-know basis, as defined in advance by the task force or central authority.”

¹⁶⁶ Bryson, *Strategic Planning*, 338. For the purposes of the Fire Service Power versus Interest Grid, DHS I&A context setters have considerable power but lower levels of direct interest in the outcome than do players. As context setters, the DHS I&A State and Local group must be convinced to take a greater interest in creating better outcomes for information sharing involving the fire service. In other words, ways must be found to move the players (fire service unions) and the context setters as a group higher on the interest scale. The obvious way to do this is to figure out how to convince the union leaders and DHS that it is somehow in their own best interests to support the recommendations identified in this thesis.

7. Planning Process

The following planning process was developed to “enable you and your organization to effectively address change by identifying where you want to go, determining how to get there, measuring your progress, and recognizing when you’ve arrived.”¹⁶⁷ Using Bryson’s *Strategic Planning For Public and Non-profit Organizations*, the National Fire Academy’s Change Management Model (and my experiences in leading and facilitating change), this planning process should allow a guiding coalition to analyze potential merger(s), anticipate information challenges, and reduce their negative effects. In essence, this is the beginning of a road map that can be used to create the preferred fire service/homeland security information-sharing future.

John Kotter has indicated that one component of unsuccessful change management is “not creating a powerful enough guiding coalition.”¹⁶⁸ Kotter proposes that many organizational changes fail because organizations underestimate the difficulties of producing an effective guiding coalition. Sometimes they have no history of teamwork at the top and therefore undervalue the importance of this type of coalition. Sometimes they expect the team to be led by a staff manager instead of a key line manager. No matter how capable or dedicated the staff head, groups without strong line leadership rarely achieve the power that is required to institute change.¹⁶⁹

The creation of a fire service/homeland security information-sharing guiding coalition¹⁷⁰ will allow players, subjects, and context setters to qualify and quantify the value of increased formalized information-sharing environments at the local, state, and national levels. I suggest that two important components of the guiding coalition are necessary. One is broad representation of all stakeholders (players, subjects and context setters), and the other is a fundamental focus on doing what is best for the citizens.

¹⁶⁷ U.S. Federal Emergency Management Agency, U.S. Fire Administration, National Fire Academy, Change Management Model, 2.

¹⁶⁸ Kotter, “Leading Change,” 1–11.

¹⁶⁹ Ibid.

¹⁷⁰ U.S. Federal Emergency Management Agency, U.S. Fire Administration, National Fire Academy, Change Management Model, 2–7.

Examples of representation may include interested citizens, union representatives, elected officials, law enforcement, ACLU, NFPA, fusion centers, emergency services and critical infrastructure/key resources representatives, business, law enforcement, fire service, and others who have a stake in information sharing to prevent or disrupt terrorism.

The planning process should allow the guiding coalition to evaluate the pros and cons of organizational conditions, potential destabilizing forces, and the impact of potential information sharing to the fire service and homeland security community. The analysis phase may help the guiding coalition in determining necessary information-sharing change requirements and reveal when information sharing is not in the best interest of the citizens (the ultimate customer). The specific tasks and steps listed below can and should be modified as appropriate by the guiding coalition.

Leadership commitment from context setters and players identified in the Fire Service Information-Sharing Power vs. Interest Grid (Figure 16) is critical. Executive leadership of the context setters and players may or may not participate in the guiding coalition discussed in the planning process below, but they must demonstrate commitment and invest their time in the process. Regarding the importance of leadership commitment during change, Gene Hall, Jim Rosenthal, and Judy Wade wrote, “A reengineering project will fail without the full commitment of senior executives.”¹⁷¹ Hall, Rosenthal and Wade went on to say that successful change managers make a few compromises and are generous with resources. Most important, the executives invest their own time in the project. Top executives spend between 20% and 60% of their time on the project. At less successful companies, the leadership has nominal sponsorship of someone two to four layers down in the organization. The ultimate change ends up focusing on issues that never go anywhere.¹⁷² With Hall’s statement in mind, it is important for players and context setters to make a significant, possibly written commitment, to the information-sharing process below.

¹⁷¹ Hall, Rosenthal, and Wade, “How to Make Reengineering Work,” 1–13.

¹⁷² Ibid.

8. Guiding Coalition

The guiding coalition may consist of representatives from fire service and homeland security players and context setters identified in the power vs. interest grid. The participants should be powerful in terms of information, expertise, reputations, and relationships. Guiding coalition participants might include representatives from the following homeland security information-sharing community: DOJ Global Justice Information Sharing Initiative (Global), the State, Local, and Tribal Integration Working Group (SLTIWG), the Criminal Intelligence Coordinating Council (CICC), the National Fusion Center Coordination Group (NFCCG) and the Senior Level Interagency Advisory Group (SLIAG).¹⁷³

C. DETERMINE WHERE WE ARE

The first objective is to conduct an overall needs assessment to get a sense of the scale of the current information-sharing environment, or as Bryson indicated in the “A” phase of the “ABCs of Strategic Planning,” “figuring out where you are.”¹⁷⁴

1. The first task is to assess the existing information-sharing environment within the fire service to determine whether the fire service should participate in the homeland security information-sharing effort, and if so how much participation is appropriate based on the needs and expectations of the citizens. This is achieved by evaluating the current conditions within the fire service as identified in the red line of the strategy canvas (Figure 14) and the current fire service option of the information-sharing matrix (Figure 1).
 - 1.1. Evaluate fire service information-sharing adherence to national, state, and departmental laws and national consensus standards.
 - 1.2. Interview or survey selected departments from the crowd on how information-sharing decisions are made.

¹⁷³ U.S. Department of Homeland Security, Office of Intelligence and Analysis, State and Local Program Office, Draft Fire Service Intelligence Enterprise Concept Plan.

¹⁷⁴ Bryson, *Strategic Planning*, 6.

- 1.2.1. May wish to use FSIE federal/national, or state/local representatives.¹⁷⁵
- 1.3. Interview or survey selected departments from the crowd on how often legal, moral, and ethical standards guide their information-sharing decision-making process.
 - 1.3.1. May wish to use federal/national or state/local representatives, including FSIE working group departments.
- 1.4. Interview or survey selected departments from the crowd on overall morale of their departments.
 - 1.4.1. May wish to use federal/national or state/local representatives, including FSIE working group departments.
- 1.5. Solicit input on how fire service–wide changes take place.
- 1.6. The guiding coalition identifies how recent fire service–wide changes have occurred.
- 1.7. Other indicators that may affect information-sharing changes.
 - 1.7.1. Impact of historical fire service mission, value, and norms relating to fire personnel saving lives and property without collecting potential terrorist information.
 - 1.7.2. Determine, define and comply with national, state, and local values.

D. IDENTIFYING POTENTIAL DESTABILIZING FORCES

- 2. After identifying and comparing current fire service information-sharing conditions, the second task is to identify and forecast potential destabilizing forces external to the fire service that may have an effect on information sharing. This task focuses primarily on forces originating outside the fire service, but not necessarily outside the influence of the crowd, subjects, players, or context setters, and compares the external forces to information-sharing benchmarks

¹⁷⁵ U.S. Department of Homeland Security, Office of Intelligence and Analysis, State and Local Program Office, Draft Fire Service Intelligence Enterprise Concept Plan, Appendix A-2.

identified in the information-sharing outcome matrix (Figure 11), the strategy canvas blue line (Figure 15), and the draft FSIE CONPLAN.

- 2.1. Identify technological factors, including the recommendations identified in this thesis.
- 2.2. Identify influential economic factors.
- 2.3. Identify influential social factors.
- 2.4. Identify relevant political/legal factors, including the recommendations identified in this thesis.
- 2.5. Survey or interview.
 - 2.5.1. Citizens on fire service information-sharing expectations.
 - 2.5.2. Players on fire service information-sharing expectations.
 - 2.5.3. Context setters on fire service information-sharing expectations.
 - 2.5.4. Subjects on fire service information-sharing expectations.
 - 2.5.5. The crowd on fire service information-sharing expectations.
 - 2.5.6. Other stakeholders.

E. DETERMINE WHERE WE WANT TO BE

3. The third task was described by Bryson as “where you want to be.”¹⁷⁶ In the third planning task, the guiding coalition compares and contrasts the impact of current conditions (internal fire service) and potential destabilizing forces (external to fire service) related to sharing information with the homeland security community. This third task attempts to broadly define the level of need (if any) for information sharing between the homeland security community and fire service based on the internal conditions and external forces identified in tasks 1 and 2 above.

¹⁷⁶ Bryson, *Strategic Planning*, 6.

Successful comparison of tasks 1 and 2 should result in future requirements and challenges relating to fire service information sharing. The challenges would be addressed in the fourth task.

- 3.1. Compare tasks 1 and 2 to establish their impact on potential information sharing.
 - 3.1.1. Consider using the fire service/homeland security information-sharing tool.
- 3.2. Assess near-term future requirements if information-sharing changes are likely.
 - 3.2.1. Describe specific, measurable, achievable, realistic, and time-certain information-sharing services that fire personnel and the homeland security community will collaborate on.
- 3.3. Assess long-term future requirements if information sharing is likely.
 - 3.3.1. Describe specific, measurable, achievable, realistic, and time-certain information-sharing services that the fire personnel and the homeland security community will collaborate on.
- 3.4. Determine an evaluation strategy. How will you know when you have arrived? What metrics should the guiding coalition use to determine success?
 - 3.4.1. The criteria identified for this thesis and located in the information-sharing matrix may be a starting point for discussion.

F. DETERMINE HOW TO GET THERE

4. Described by Bryson as “how to get there,” the fourth task will direct the guiding coalition in determining specific information-sharing change requirements needed to create the preferred information-sharing future.¹⁷⁷ At this point the guiding coalition will move away from the highest-level strategic planning and begin setting goals and objectives that identify the operational mile-markers on the road to creating the preferred information-sharing future.

¹⁷⁷ Bryson, *Strategic Planning*, 6.

- 4.1. The guiding coalition should develop a final draft information-sharing statement (mission, vision, scope of work statement) for executive leadership, citizens, crowd, players, subjects, context setters, and other stakeholders to approve.
 - 4.1.1. Generate ideas for inspiration and emotional appeal of the information-sharing project. Don't underestimate the value of this step. Creating buy-in for the vision can be as important as the vision itself.
- 4.2. Magnitude of fire service/homeland security information sharing can be identified by using the following considerations.
 - 4.2.1. Pace. Will the future information-sharing environment be enterprise-wide or partial?
 - 4.2.1.1. Will the future information-sharing environment be phased in by function (fire marshal, department size, geographically), gradual, rapid, pilot projects?
 - 4.2.2. Depth. Determine the number of changes that can be introduced before the number itself creates resistance to increased information sharing between the fire service and homeland security information-sharing community.
 - 4.2.2.1. Consider engineering controls, behavior modifications, training education.
- 4.3. Select the best or highest probability methods to achieve the stated information-sharing vision.
 - 4.3.1. Technological methods of change.
 - 4.3.1.1. Use of centralized data collection systems or decentralized type information-sharing systems.
 - 4.3.1.1.1. Compare centralized HSIN, NFIRS with decentralized Wikipedia, EBay, Skype information-sharing systems. Something in between?
 - 4.3.2. Structural methods of change.
 - 4.3.2.1. Hierarchical, scalar, flat, asymmetric.

- 4.3.2.2. Formalization, and coordination of information-sharing methods.
 - 4.3.2.2.1. Degree to which centralized rules, processes, and guides are used, compared to open-source information-sharing systems or processes.
- 4.3.3. Managerial methods of change.
 - 4.3.3.1. Compensation, promotions, benefits, status, power, influence.
- 4.3.4. People-oriented methods of change.
 - 4.3.4.1. Education or training to increase collection, dissemination, and consumption of potential terrorist-related information.
- 4.3.5. Assess and select the techniques to promote the specific, measurable, time-certain information-sharing goals.
 - 4.3.5.1. Facilitative.
 - 4.3.5.1.1. The players, subjects, and context setters in the fire service information-sharing power vs. interest grid (Figure 15) act as conduits, assisting the crowd to achieve the identified goals.
 - 4.3.5.1.2. Attitudinal.
 - 4.3.5.1.2.1. Influencing the crowd and the public's attitudes and behaviors toward potential terrorist activities and the need for information sharing.
 - 4.3.5.1.3. Political.
 - 4.3.5.1.3.1. Artistic negotiating and aligning of the crowd, subjects, players, and context setters to the specific, measurable, and time-certain goals of the guiding coalition.
 - 4.3.5.1.3.2. Coercive techniques may be useful when competing for scarce resources.
 - 4.3.5.1.3.2.1. This might include DHS grant eligibility or awards.

G. FIRE SERVICE INFORMATION-SHARING IMPLEMENTATION AND EVALUATION PHASES

Implementation and evaluation tasks were not considered in the scope of this thesis but should be considered if applicability of the analysis and planning tasks are recognized by the DHS I&A, DOJ, or other information-sharing partners.

VIII. CONCLUSION

This thesis presents an analysis of a number of information-sharing options relating to terrorism and all-hazard strategies, policies, and programs, in an attempt to identify if U.S. fire personnel should participate in terrorism-related information sharing and—if they should participate—consider the legal, political, and operational boundaries.

The research produced three macro-level findings, four information-sharing matrices, two strategic applications, and nine smart practices. The findings, matrices, applications, and smart practices are a result of comparing and contrasting legal compliance, political acceptability, target capabilities list linkage, operational impact, and cost of the current U.S. fire service information-sharing environment, the New York City Fire Department's Terrorism and Disaster Preparedness Strategy, the U.S. fire service Intelligence Enterprise draft concept plan and the UK's Civil Contingencies Act of 2004.

The first universal or macro-level finding indicates that U.S. firefighters have legal, moral, and ethical responsibilities to gather and share potential terrorist-related information that could assist the homeland security community in preventing and disrupting terrorist attacks. Second, these responsibilities must be conducted within the context of a two hundred fifty-year U.S. fire service enterprise founded on saving lives and property while maintaining exemplary trustworthiness, reliability, and credibility with the public. The third inclusive finding was that legal and operational issues may be addressed by firefighters using standardized terrorist indicators while operating as sensors of opportunity during emergency and non-emergency operations, but fire personnel must not be specifically asked or assigned to gather information on suspected terrorists or terrorist activities.

The first strategic recommendation of this thesis is to modify the National Strategy for Information Sharing (NSIS) to include the fire service as an information-sharing partner in some situations. The second strategic recommendation presents a strategic information-sharing plan to enhance the current homeland security community and fire service ad hoc information-sharing environment.

The nine suggested smart practices are located in the analysis-and-recommendations chapter of this thesis and range from four common terrorist indicators that every firefighter should know to national U.S. guidance templates for formally requesting classified information.

Possibly more important than all the findings, recommendations, plans, and smart practices identified in this thesis is the recognition of who firefighters are and what they can do to prevent or disrupt terrorism through information sharing. Since before the time of Fire Chief Benjamin Franklin, the fire service has been built on the legal, moral, and ethical commitment to protect U.S. citizens through prevention and response. The continued sporadic, unstructured information sharing of potential terrorist-related information is unacceptable. We are at war, and war calls for risks if we want to prevail. One of the risks of using fire personnel to collect information in plain sight is the tarnishing of our reputation or possible legal action. I propose that the risk is considerably less than dealing with the consequences of the attacks on the Murrah Building or the World Trade Center, or more horrendous acts of terrorism. We must continue to build on the U.S. fire service's long and successful history of prevention.

More than seven years ago the terrorist attacks of 9/11 became the catalyst for the U.S. expansion of information gathering and sharing with non-traditional partners such as the fire service. Now is the time for action. The significant value of fire personnel's prevention of life and property loss from terrorism through the use of standardized terrorist indicators and formalized collaboration with the homeland security community should not be underestimated. The more than one million U.S. fire personnel serving in over thirty thousand fire departments may be a phenomenal resource for our homeland security partners, and our homeland security partners could be a valuable resource for firefighters. If the strategic and operational recommendations identified in this thesis are implemented by the nation's fire personnel, the volume of suspicious-activity reporting should increase and with it the potential for preventing or disrupting future terrorism in the United States. Citizens will be safer and, in my opinion, will appreciate their firefighters stepping up, as they have historically done to prevent life and property loss in

our country. The terrorist beat us on at least two days, April 19, 1995, and September 11, 2001. We should not let it happen again just because we do not choose to overcome our information-sharing challenges.

THIS PAGE INTENTIONALLY LEFT BLANK

BIBLIOGRAPHY

- Bellavita, Christopher. "Changing Homeland Security: What is Homeland Security?" *Homeland Security Affairs* IV, no. 2 (June 2008).
<http://www.hsaj.org/?article=4.2.1> (accessed October 7, 2008).
- Brafman, Ori and Rod Ceckstrom. *The Starfish and the Spider*. New York: Penguin Group, 2006.
- British Broadcasting (BBC) News. "Police Avert Car Bomb Carnage."
<http://news.bbc.co.uk/1/hi/uk/6252276.stm> 1 (accessed June 20, 2008).
- Bryson, John. *Strategic Planning for Public and Nonprofit Organizations*. 3rd ed. San Francisco, CA: Jossey-Bass, 2004.
- Bush, George W. Office of the White House. Memorandum for the Heads of Executive Departments and Agencies: Guidelines and Requirements in Support of the Information Sharing Environment. December 2005.
<http://www.whitehouse.gov/news/releases/2005/12/20051216-10.html> (accessed July 13, 2008).
- Camara v. Municipal Court of the City and County of San Francisco*, 387 U.S. 523 (1967). <http://supreme.justia.com/us/387/523/case.html> (accessed January 25, 2008).
- Chertoff, Michael. Remarks at the 2006 Bureau of Justice Assistance, U.S. Department of Justice and SEARCH Symposium on Justice and Public Safety Information Sharing. March 14, 2006. http://www.dhs.gov/xnews/speeches/speech_0273.shtm (accessed December 13, 2008).
- . U.S. Department of Homeland Security. Remarks by Secretary Michael Chertoff at the International Association of Fire Chiefs. October 26, 2007.
http://www.dhs.gov/xnews/speeches/sp_1193431068145.shtm (accessed January 21, 2008).
- Churay, Ray P. Testimony to House Committee on Governmental Reform, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations. Terrorism Preparedness. March 22, 2002. http://www.manhattan-institute.org/html/ptr_03.htm#notes (accessed October 4, 2008).

East Bay Terrorism Early Warning Group (EBTEWG) and the Washington Regional Threat Analysis Center (WRTAC). Daily Open Source Brief. November 5, 2008. nzamora@eastbaytewg.org (accessed November 5, 2008).

Edwards, David and Muriel Kane, Firefighters Asked to Report People Who Express Discontent with the Government, http://rawstory.com/news/2007/Homeland_Security_turns_firefighters_into_domestic_1129.html (accessed February 27, 2009).

Fire Department City of New York. Terrorism and Disaster Preparedness Strategy. 2007. http://www.nyc.gov/html/fdny/pdf/events/2007/tdps/terrorism%20strategy_complete.pdf (accessed June 20, 2008).

———. Vital Statistics. 2008. <http://nyc.gov/html/fdny/html/home2.shtml> (accessed October 4, 2008).

———. *Watchline*. October 9, 2008. watchline@fdny.nyc.gov (accessed October 9, 2008). Contact FDNY for a copy of *Watchline*.

Gibson, Ashley. “Fire Ravages Oklahoma City, Texas Towns.” Associated Press. January, 2006. <http://www.firerescue1.com/wildland/articles/14630-Fires-ravage-Oklahoma-City-texas-towns/> (accessed September 27, 2008).

Hall, Eugene A., James Rosenthal, and Judy Wade. “How to Make Reengineering Work,” *Harvard Business Review* (1993). http://harvardbusinessonline.hbsp.harvard.edu/b02/en/common/item_detail.jhtml;jsessionid=VLOYJMJOU5LIUAKRGWDSELQBKE0YIISW?id=93604 (accessed December 13, 2008).

Hardesty, David C. “Spaced Based Weapons, Long Term Strategic Implications and Alternatives,” *Naval War College Review* (Spring 2005). http://findarticles.com/p/articles/mi_m0JIW/is_2_58/ai_n14705061 (accessed September 27, 2008).

Heraclitus, <http://www.toinspire.com/author.asp?author=Heraclitus+of+Greece> (accessed October 28, 2008).

Kim, W. Chan and Renee Mauborgne. *Blue Ocean Strategy*. Boston, MA: Harvard Business School Publishing, 2005.

- Kotter, John. "Leading Change: Why Transformation Efforts Fail," *Harvard Business Review*: March 1995, 1–11.
http://harvardbusinessonline.hbsp.harvard.edu/b02/en/common/item_detail.jhtml;jsessionid=XF3NFBCIWXACMAKRGWDR5VQBKE0YIISW?id=R0701J&requestid=37402 (accessed December 13, 2008).
- Kruta, Jim and John Williams. Personal communications with National Fire Information Reporting System Board Member John Williams and Oklahoma City Fire Department Information Technology Captain Jim Kruta. February through March 2008.
- Machiavelli, Niccolò. <http://www.answers.com/topic/quote-4?author=Machiavelli,%20Niccolo&s2=Niccolo%20Machiavelli#copyright> (accessed October 28, 2008).
- Masse, Todd. "Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches," Congressional Research Service Report for Congress. August 18, 2006.
<https://www.hsdl.org/?search=&offset=0&submitted=Search&publisher=&format=&language=&collection=&all=+Homeland+Security+Intelligence%3A+Perceptions%2C+Statutory&searchfield=title&placeholder=&submitted=Search> (accessed January 13, 2008).
- Michigan v. Clifford*, 464 U.S. 287 (1984). <http://caselaw.lp.findlaw.com/cgi-bin/getcase.pl?friend=nytimes&navby=case&court=U.S.&vol=464&invol=287> (accessed January 25, 2008).
- Michigan v. Tyler*, 436 U.S. 499 (1978). <http://supreme.justia.com/us/436/499/case.html> (accessed January 25, 2008).
- Miller, Andrew. Miller Center for Homeland Security and Defense. More Media Reaction to FIRE-INT (Intel gathered by Fire/Rescue) thread.
<https://www.chds.us/?auth/login&dest=auth%2Floggedin> (accessed December 20, 2007). Contact author for a copy.
- National Commission on Terrorist Attacks upon the United States. *The 9/11 Commission Report*. Washington, D.C., July 2004.
<http://govinfo.library.unt.edu/911/report/index.htm> (accessed August 29, 2008).
- National Fire Protection Association. The United States Fire Service.
<http://www.mdchief.org/fire06.pdf> (accessed January 4, 2008).

- National Fire Protection Association. U.S. Fire Department Profile Through 2006. November 2007. <http://www.nfpa.org/assets/files/PDF/FDprofilefactsheet.pdf> (accessed October 4, 2008).
- National Security Council. National Strategy for Information Sharing. Washington, D.C. October 2007. http://www.whitehouse.gov/nsc/infosharing/NSIS_book.pdf (accessed June 19, 2008).
- National Terror Alert Response Center. Firefighters to Help in Fight against Terrorism – ACLU Speaks Out. <http://www.nationalterroralert.com/updates/2007/11/23/firefighters-to-help-in-fight-against-terrorism-aclu-speaks-out/> (accessed December 20, 2007).
- New York State Metropolitan Transit Authority. If You See Something, Say Something. www.mta.info/mta/security/index.html (accessed January 21, 2008).
- Olberman, Keith. Interview with Mike German on MSNBC’s *Countdown*. Broadcast November 28, 2007. http://rawstory.com/news/2007/Homeland_Security_turns_firefighters_into_domestic_1129.html (accessed December 20, 2007).
- Posner, Gerald. *Why America Slept: The Failure to Prevent 9/11*. New York, NY: Random House, 2003.
- Scoppetta, Nicholas. Testimony of Fire Commissioner Nicholas Scoppetta before the National Commission on Terrorist Attacks upon the United States. May 18, 2004. www.9-11commission.gov (accessed January 21, 2008).
- Townsend, Keeley. Personal communication with Ms. Keeley Townsend, U.S. Department of Homeland Security, Office of Intelligence and Analysis, State and Local Program Office. December 16, 2008.
- United Kingdom. Cabinet Office, Civil Contingencies Secretariat. Civil Contingencies Act 2004, Part 1: Local Arrangements for Civil Protection. London, United Kingdom. http://www.opsi.gov.uk/acts/acts2004/plain/ukpga_20040036_en#pt1 (accessed July 14, 2008).
- . Cabinet Office, Civil Contingencies Secretariat, Civil Contingencies Act 2004, Contingency Planning Regulations 2005, Statutory Instrument 2005 No. 2042. London, United Kingdom. <http://www.opsi.gov.uk/si/si2005/20052042.htm#1> (accessed July 14, 2008).

- . Cabinet Office, Civil Contingencies Secretariat. Civil Contingencies Act 2004, Short Guide. London, United Kingdom.
www.ukresilience.gov.uk/~media/assets/www.ukresilience.info/15mayshortguide%20pdf.ashx (accessed July 14, 2008).
- . HM Government Emergency Preparedness Guidance on Part 1 of the Civil Contingencies Act 2004. Easingwold, England: Library & Information Centre, Emergency Planning College.
<http://www.ukresilience.gov.uk/preparedness/ccact/eppdfs.aspx> (accessed July 8, 2008).
- . Resilience, Emergency Preparedness. Progress on Implementation of the Civil Contingencies Act.
<http://www.ukresilience.gov.uk/preparedness/ccact/progress.aspx> (accessed July 18, 2008).
- U.S. Department of Homeland Security. Interim National Preparedness Goal (INPG). Washington, D.C.: Department of Homeland Security, 2005.
www.ojp.usdoj.gov/odp/docs/InterimNationalPreparednessGoal_03-31-05_1.pdf (accessed December 13, 2008).
- . Office of Intelligence and Analysis, State and Local Program Office. Draft Fire Service Intelligence Enterprise Concept Plan. December 2008. Contact author for a copy.
- . Office of Intelligence and Analysis, State and Local Program Office. Fire Service Intelligence Enterprise—Executive Briefing. November 2008. Contact author for a copy.
- . FY 2003 State Homeland Security Grant Program (SHSGP).
http://www.ojp.usdoj.gov/odp/grants_equipment.htm (accessed February 27, 2009).
- . Homeland Security Exercise and Evaluation Program Toolkit.
https://hseep.dhs.gov/pages/1001_Toolk.aspx (accessed July 27, 2008).
- . Interim National Preparedness Goal. March 31, 2005.
http://www.ojp.usdoj.gov/odp/docs/InterimNationalPreparednessGoal_03-31-05_1.pdf (accessed December 13, 2008).
- . Office of Science and Technology. Interoperability Initiatives Fact Sheet.
www.safecomprogram.gov/.../0/DHSInteroperabilityInitiativesFactSheet.pdf (accessed August 31, 2008).

- . National Preparedness Guidelines. September 2007. http://www.dhs.gov/xlibrary/assets/National_Preparedness_Guidelines.pdf (accessed June 8, 2008).
- . National Planning Scenarios. July 2004. <http://cryptome.org/hi-docs.htm> (accessed September 1, 2008).
- U.S. Department of Justice. Fusion Center Guidelines—Developing and Sharing Information in a New Era. No date. http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf (accessed August 4, 2008).
- U.S. Department of Labor, Bureau of Labor Statistics. “Fire Fighting Occupations,” in *Occupational Outlook Handbook*. <http://www.bls.gov/oco/ocos158.htm> (accessed October 4, 2008).
- U.S. Federal Emergency Management Agency, U.S. Fire Administration, National Fire Academy. Change Management Model. NFA, CMM. 1996. Contact author or <http://www.lrc.fema.gov/index.html> for copies.
- U.S. Fire Administration. About INFIRS: Facts About NFIRS. December 28, 2006. <http://www.usfa.dhs.gov/fireservice/nfirs/about.shtm> (accessed February 5, 2008).
- . Fire Departments. No date. <http://www.usfa.dhs.gov/statistics/departments/index.shtm> (accessed December 15, 2007).
- U.S. Homeland Security Act 2002, PUBLIC LAW 107–296. Subtitle I—Information Sharing. November 25, 2002. www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf (accessed June 29, 2008).
- U.S. Homeland Security Council. National Strategy for Homeland Security. Washington, D.C.: White House, October, 2007. <http://www.whitehouse.gov/infocus/homeland/nshs/2007/index.html> (accessed December 22, 2007).
- . National Strategy for Homeland Security Goal to Prevent and Disrupt Terrorist Attacks. 2007. www.whitehouse.gov/infocus/homeland/nshs/2007/index.html 15 (accessed May 17, 2008).

- U.S. Homeland Security Presidential Directive HSPD-8. Washington D.C.: White House, December 2003. <http://www.whitehouse.gov/news/releases/2003/12/20031217-6.html> (accessed December 13, 2008).
- U.S. Office of the Director of National Intelligence. Information Sharing Environment Information Sharing Plan. Washington, D.C. November 2006. <http://www.ise.gov/docs/reports/ise-impplan-200611.pdf> (accessed July 13, 2008).
- U.S. Office of Domestic Preparedness. Guidelines for Homeland Security, Prevention and Deterrence. Washington, D.C. June 2003. www.ojp.usdoj.gov/odp/docs/ODPPrev1.pdf
- Weidner, Marv. Planning for Results. <http://www.weidnerinc.com/planning.php> (accessed October 12, 2008).
- White House. National Strategy for Homeland Security. Washington, D.C.: White House, July, 2002. http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf (accessed October 7, 2008).
- White House. National Strategy for Information Sharing. Washington, D.C.: White House, 2003. http://www.whitehouse.gov/nsc/infosharing/NSIS_book.pdf (accessed June 20, 2008).
- White House, National Security Council. National Strategy for Information Sharing. Washington, D.C., October 2007. <http://www.whitehouse.gov/nsc/infosharing/index.html> (accessed July 25, 2008).
- Whitely, John and Gerold Yonas. *The War on Terrorism and What We can Learn From the War on Fire*. Albuquerque, NM: Sandia National Laboratories, July 2002. <https://www.hSDL.org/?abstract&url=https%3A%2F%2Fwww.hSDL.org%2Fhome%2Fdocs%2Fdocs%2Fdocs%2Fnps08-020905-13.pdf&coll=documents> (accessed January 13, 2008).
- World Bank Institute. Background Notes on Leadership. Washington, D.C.: International Bank for Reconstruction and Development/The World Bank, 2007. https://www.chds.us/courses/file.php/340/0601-0602_readings/leadershipworldbank.pdf (accessed October 19, 2008).

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, VA
2. Dudley Knox Library
Naval Postgraduate School
Monterey, CA
3. Chief G. Keith Bryant
Oklahoma City Fire Department
Oklahoma City, OK
4. Keeley Townsend
Department of Homeland Security, Intelligence and Analysis
Washington, DC
5. Bruce Teele
National Fire Protection Association
Boston, MA
6. Rich Duffy
International Association of Firefighters
Washington, DC
7. Paul Smith
Federal Bureau of Investigation
Washington, DC
8. Kelley Wilson
Washington Regional Threat & Analysis Center
Washington, DC
9. David Cid
Memorial Institute for the Prevention of Terrorism
Oklahoma City, OK
10. John Rollins
Library of Congress
Washington, DC

11. Christopher Bellavita
Naval Postgraduate School
Monterey, CA
12. Richard Parenty
Center for Terrorism and Emergency Preparedness
Fort Totten, NY