NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

FIRE SERVICE INTELLIGENCE:
INFORMED STRATEGIES, OPERATIONS, AND TACTICS

by

Derrick D. Phillips

December 2020

Co-Advisors: Robert L. Simeral (contractor)
Erik J. Dahl

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC, 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2020	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE FIRE SERVICE INTELLIGENCE: INFORMED STRATEGIES, OPERATIONS, AND TACTICS			**5. FUNDING NUMBERS**
6. AUTHOR(S) Derrick D. Phillips			
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)

Fire service agencies struggle to receive and use relevant, agency-specific intelligence, which hampers their ability to prevent attacks, protect the community, mitigate an attack's impact, respond safely, and recover from such events. This thesis presents the intelligence requirements necessary to support the fire service and specifies how the fire service can use intelligence to guide strategic policy development, operational planning, and tactical decision-making. It employed a qualitative gap analysis, using a 15-question survey of fire service personnel, to compare the current state of the fire service intelligence apparatus with a desired future state. This thesis also used case analysis to identify current intelligence products to understand how well they support strategic, operational, and tactical decisions. This thesis identifies intelligence gaps from a broader fire-service audience and offers a holistic set of recommendations, thus contributing to intelligence research. The gaps involve collaborating with law enforcement on intelligence, establishing intelligence requirements to better support the fire service, handling sensitive information, and using finished intelligence for decision-making. This thesis recommends identifying and distributing intelligence requirements to the fire service, developing training and policy guidance on intelligence handling, and creating a joint intelligence guide.

14. SUBJECT TERMS fire service, intelligence, fusion center, homeland security, DHS, information sharing, information needs, strategic intelligence, operational intelligence, tactical intelligence, fire service intelligence enterprise, intelligence driven decision-making, domestic intelligence, information sharing environment			**15. NUMBER OF PAGES** 165
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

FIRE SERVICE INTELLIGENCE: INFORMED STRATEGIES, OPERATIONS, AND TACTICS

Derrick D. Phillips
Battalion Chief, St. Louis Fire Department
BS, Columbia College, 2017

Submitted in partial fulfillment of the
requirements for the degree of

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

from the

NAVAL POSTGRADUATE SCHOOL
December 2020

Approved by: Robert L. Simeral
Co-Advisor

Erik J. Dahl
Co-Advisor

Erik J. Dahl
Associate Professor, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Fire service agencies struggle to receive and use relevant, agency-specific intelligence, which hampers their ability to prevent attacks, protect the community, mitigate an attack's impact, respond safely, and recover from such events. This thesis presents the intelligence requirements necessary to support the fire service and specifies how the fire service can use intelligence to guide strategic policy development, operational planning, and tactical decision-making. It employed a qualitative gap analysis, using a 15-question survey of fire service personnel, to compare the current state of the fire service intelligence apparatus with a desired future state. This thesis also used case analysis to identify current intelligence products to understand how well they support strategic, operational, and tactical decisions. This thesis identifies intelligence gaps from a broader fire-service audience and offers a holistic set of recommendations, thus contributing to intelligence research. The gaps involve collaborating with law enforcement on intelligence, establishing intelligence requirements to better support the fire service, handling sensitive information, and using finished intelligence for decision-making. This thesis recommends identifying and distributing intelligence requirements to the fire service, developing training and policy guidance on intelligence handling, and creating a joint intelligence guide.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
- A. RESEARCH QUESTIONS....2
- B. LITERATURE REVIEW....2
- C. RESEARCH DESIGN....13
- D. CHAPTER LAYOUT....14

II. GAPS IN FIRE SERVICE INTELLIGENCE SUPPORT, TECHNIQUES, AND PROCEDURES....17
- A. SURVEY OVERVIEW....17
- B. DEMOGRAPHIC QUESTIONS....18
- C. INTELLIGENCE QUESTIONS....21
- D. PESTEL ANALYTICAL FRAMEWORK....30
- E. CONCLUSION....34

III. CURRENT FIRE SERVICE OPERATIONAL INTELLIGENCE POLICIES AND PRACTICES....37
- A. INTELLIGENCE OVERVIEW....37
- B. INTELLIGENCE COMMUNITY....45
- C. FIRE SERVICE INTELLIGENCE ENTERPRISE CONCEPT PLAN....48
- D. FIRE SERVICE INTEGRATION FOR FUSION CENTERS....51
- E. INTELLIGENCE GUIDE FOR FIRE CHIEFS....51
- F. INTELLIGENCE GUIDE FOR FIRST RESPONDERS....52
- G. CONCLUSION....54

IV. CASE STUDIES OF EFFECTIVE FIRE INTELLIGENCE USE, POLICIES, AND PRACTICES....57
- A. CHICAGO FIRE DEPARTMENT TOIC....58
- B. FDNY INTELLIGENCE....62
- C. NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM....66
- D. CONCLUSION....69

V. DISCUSSION, CONCLUSIONS, AND RECOMMENDATIONS....71
- A. DISCUSSION....71
- B. CONCLUSIONS....75
- C. RECOMMENDATIONS....81

APPENDIX A. FIRE SERVICE INTELLIGENCE REQUIREMENTS 85
A. STANDING INFORMATION NEEDS/REQUIREMENTS 85
B. STRATEGIC INTELLIGENCE REQUIREMENTS 86
C. OPERATIONAL INTELLIGENCE REQUIREMENTS 87
D. TACTICAL INTELLIGENCE REQUIREMENTS.....88

APPENDIX B. JOINT INTELLIGENCE GUIDE OUTLINE 89

APPENDIX C. SURVEY RESULTS 93

LIST OF REFERENCES.....135

INITIAL DISTRIBUTION LIST 141

LIST OF FIGURES

Figure 1. Fire Service Agencies Represented in the Survey 19

Figure 2. Number of Personnel in the Represented Departments 20

Figure 3. Geographic Regions of the Fire Departments.....21

Figure 4. Perception That the Organization Supplying Intelligence Understands Fire Service Needs 26

Figure 5. Sources of Intelligence for Survey Participants.....27

Figure 6. Percentage That Believe Received Intelligence Is of Value.....28

Figure 7. Agencies of the Intelligence Community 46

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. List of FSIE-Related Directives, Policies, Strategies, and Legislation.....49

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACLU	American Civil Liberties Union
CNSI	classified national security information
CPIC	Crime Prevention and Information Center
CTDP	Center for Terrorism and Disaster Preparedness
CUI	controlled unclassified information
DCFEMS	District of Columbia Fire and Emergency Medical Services
DHS	Department of Homeland Security
DIB	district intelligence bulletin
DOJ	Department of Justice
EMS	emergency medical services
FBI	Federal Bureau of Investigation
FDNY	New York City Fire Department
FOUO	for official use only
FSIE	Fire Service Intelligence Enterprise
HSIN	Homeland Security Information Network
HUMINT	human intelligence
IAFC	International Association of Fire Chiefs
IC	Intelligence Community
IRTPA	Intelligence Reform and Terrorism Prevention Act
ISE	Information Sharing Environment
JCAT	Joint Counterterrorism Assessment Team
JTTF	Joint Terrorism Task Force
LES	law enforcement sensitive
NTIC	National Capital Region Threat Intelligence Consortium
PESTEL	political, economic, sociocultural, technological, environmental, legal
PII	personally identifiable information
SAR	suspicious activity report/reporting
SIGINT	signals intelligence
SIN	standing information needs

SLTT	state, local, tribal, and territorial
SSI	sensitive security information
TOIC	Tactical Operations Intelligence Center
TRIPwire	Technical Resources for Incident Prevention
WMD	weapon of mass destruction

EXECUTIVE SUMMARY

Fire service agencies struggle to receive relevant, agency-specific intelligence, which hampers their ability to prevent adversarial attacks, protect the community, mitigate the impact, respond safely, and recover from such events. Accordingly, the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) directed the president of the United States to establish the Information Sharing Environment, which "provides and facilitates the means for sharing terrorism information among all appropriate Federal, State, local, and tribal entities, and the private sector through the use of policy guidelines and technologies."[1] The goal of IRTPA was to eliminate the intelligence community's information and intelligence gaps between levels of governments that failed to provide the intelligence necessary to prepare for and prevent the 9/11 terrorist attacks.

This thesis identifies the intelligence requirements needed to support the fire service and describes how the fire service can use intelligence to guide strategic policy development, operational planning, and tactical decision-making. Additionally, this thesis uses qualitative gap analysis to compare the current state of the fire service intelligence apparatus with a desired future state.[2] This method guided the development of recommendations by analyzing processes, practices, structures, and missing strategies.[3] As part of the analysis, I conducted a survey of fire service members through the International Association of Fire Chiefs and the Fire Service Section of the National Fire Protection Association. The survey aimed to identify the current intelligence requirements and uses of intelligence to inform decision-making.

Additionally, this research analyzed current intelligence products developed by the Chicago Fire Department's Tactical Operations Intelligence Center, the New York City Fire Department's *Watchline*, and the National Capital Region Threat Intelligence

[1] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108–458, §1016, 118 Stat. 3665 (2004), https://www.dni.gov/files/NCTC/documents/RelatedContent_documents/Intelligence_Reform_Act.pdf.

[2] "The Complete Guide to Gap Analysis," Smartsheet, accessed February 24, 2020, https://www.smartsheet.com/gap-analysis-method-examples.

[3] Smartsheet.

Consortium's first responder bulletin. The analysis identified the current state of intelligence products to gain an understanding of how well the products support strategic, operational, and tactical decision-making.

To guide the gap analysis, this thesis used the political, economic, sociocultural, technological, environmental, legal (PESTEL) framework, facilitating the analysis of numerous factors for a more comprehensive study. This thesis used the results to develop a set of recommendations, including the creation of a fire service intelligence requirements document and a joint intelligence guide for first response organizations.

Demographically, respondents represented career, volunteer, and combination departments, as well as a state fire academy, a paid on-call agency, and a state forestry agency. Additionally, participants represented various sized fire departments from every geographic region in the United States. Identifying shortcomings in fire service intelligence practices as a whole made the representation from different types, sizes, and geographic regions vital to the development of solutions that most departments can use.

The survey data revealed several effective intelligence practices. First, a majority of participants reported receiving intelligence from at least one source, with several reporting multiple sources. The most prevalent sources were state or local fusion centers, police intelligence units, the Homeland Security Information Network, and the Federal Bureau of Investigation's JTTFs. To a lesser extent, others highlighted agency use of internally created intelligence, arson task forces, technical resources for incident prevention, bomb and arson tracking systems, and the Interagency Fire Intelligence Exchange. These findings challenge the work of earlier researchers who suggested that the fire service lacked access to intelligence products because of limited security clearances or other reasons.[4] Second, several participants noted successful integration by their agencies with state or local fusion centers, with some having a fire service representative or terrorism liaison officer assigned as well. Additionally, 88.24 percent of participants recognized that their departments receive intelligence of some value—despite data that suggest 52 percent

[4] Thomas A. Robson, "A Burning Need to Know: The Use of Open Source Intelligence in the Fire Service" (master's thesis, Naval Postgraduate School, 2009), 2, http://hdl.handle.net/10945/4913.

of fire agencies perceive intelligence providers as unaware of fire service intelligence requirements.

On the other hand, barriers to information sharing persist within fire service agencies and between their law enforcement counterparts. Internally, fire service agencies withhold information from the rank and file, disseminating it only to high-ranking personnel. Regarding law enforcement, many survey participants highlighted a lack of trust between the fire service and law enforcement as an important information-sharing barrier. The problem endures despite several guidance documents recognizing the fire service as an equal and fully trusted partner.[5] Additionally, fire service agencies advised that they do not receive the same type of intelligence as law enforcement does, suggesting that decision-makers value it less. Likewise, the fire service interaction with fusion centers remains fragmented, another notable weakness. In particular, participants from Washington State and New York underscored that the fire service has been left out of the information-sharing loop altogether. Still, others stated their fusion centers deal mainly with criminal issues such as drug trafficking.

Collaborating with law enforcement on intelligence processes, establishing intelligence requirements to better support the fire service, handling sensitive information, and using finished intelligence for decision-making represent the key findings of this thesis. As a result of the study, the fire service overwhelmingly suggests that intelligence and operational planning must be a collaborative effort. Numerous participants proposed reserving a seat at the table for fire service agencies to engage in intelligence and information-sharing initiatives. Furthermore, participants suggested tying in intelligence activities with integrated response planning for events that may affect their jurisdictions.

The survey uncovered several interrelated fire service requirements. First, fire service agencies argued that the intelligence they do receive lacks relevance, timeliness, and coordination between fire and law enforcement agencies. Second, participants claimed that intelligence agencies are not aware of fire service intelligence needs. These claims

[5] Executive Office of the President, *National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing* (Washington, DC: White House, 2007), 3, https://apps.dtic.mil/dtic/tr/fulltext/u2/a473664.pdf.

raise concern because they reveal misperceptions within the fire service about intelligence requirements. Additionally, the survey revealed some confusion over intelligence requirements for standing information needs and strategic, operational, and tactical levels. An associated concern was the lack of understanding of the handling requirements for sensitive information, as many agencies do not have an information security officer position. Several participants highlighted security concerns about leaks of sensitive information to the general public.

Regarding the use of finished intelligence, participants identified several shortcomings in the survey. First, participants pointed out that fire service members need additional training in how to understand, interpret, and act on intelligence. Second, participants suggested that the overabundance of information drowns out the more pertinent details. Additionally, participants stressed the need to practice using intelligence in training scenarios to improve understanding. Furthermore, participants recognized that without knowing how to use intelligence, fire personnel could respond blindly to incidents that might have grave consequences.

According to Thomas Robson, "The ability of the fire service to execute its sworn duty to protect life and property in the local community, as well as, to the extent possible, protect the firefighters who serve there from the consequences of terrorism, is dependent on the efficient usage of intelligence."[6] As such, intelligence supports mission-critical decisions at all levels of fire service organizations. More specifically, intelligence aims to inform long-range strategic planning, gain an understanding of threats and their implications for the organization, and protect the lives of personnel operating on the ground. Given the importance of intelligence, this thesis provides recommendations for the three most critical issues identified in the survey and analysis of professed intelligence problems: determining intelligence requirements, handling sensitive information, and more effectively collaborating with law enforcement in developing intelligence products.

[6] Robson, "Burning Need to Know," 14.

1. The International Association of Fire Chiefs should identify and distribute a list of baseline fire service intelligence requirements to all fire service organizations for submission to their intelligence producers.
2. The Department of Homeland Security and the Department of Justice should develop a training brief and policy guidance on intelligence-handling requirements and operational security.
3. The Department of Homeland Security, Department of Justice, International Association of Fire Chiefs, and International Association of Chiefs of Police should develop a joint intelligence guide for use by fire, law enforcement, emergency medical services, and other first response agencies.

In sum, identifying and distributing baseline intelligence requirements to fire service agencies will ensure the received intelligence is timely and relevant to support decision-making at all levels of fire service organizations. Also, training on handling sensitive information and internal security policies may eliminate barriers to information sharing between the fire service and law enforcement. Finally, developing a joint planning doctrine and guide will allow for more effective coordination and collaboration at the local level to ensure the completion of homeland security missions in the most effective and efficient ways possible.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

First, I want to thank the Center for Homeland Defense and Security at the Naval Postgraduate School for allowing me to embark on the most rewarding educational experience of my life. The experience was genuinely academic and rewarding, and I will never forget the challenges I faced, the experience I gained, the people I met, and the life-altering lessons I learned.

Second, I want to thank my thesis co-advisors, Dr. Erik Dahl and Captain Robert Simeral (retired), whose patience, guidance, and insight made the process less foreboding. Their combined experiences challenged me to think outside the box, and hopefully, I contributed something to the field of intelligence. Additionally, I want to thank Dr. Carolyn Halladay, my academic associate in the research process, for challenging and shaping my research and writing skills. In addition, I want to extend my appreciation for my writing coach Marianne Taflinger for her expertise in wordsmithing my writings. Furthermore, I want to extend thanks to Noel Yucuis for serving as my thesis editor. The combined team was a joy to work with on this project.

Finally, I want to thank all the professors and guest instructors for transferring their knowledge and experiences to my brain. I especially enjoyed the Branders courses with Dr. David Brannan and Dr. Anders Strindberg. We had some of the best and most heated discussions, and they really helped me to challenge my assumptions. I am also a believer in social identity theory, which helps to explain a great deal in the world generally and in homeland security more specifically. I would be remiss if I did not mention other professors who left a great impression on me: Richard Bergin, Dr. Shannon Brown, Dr. Rudy Darken, Dr. Nicholas Dew, Dr. Tom Housel, Dr. Seth Jones, Dr. Tom Mackin, Dr. Cristiana Matei, Patrick Miller, Dr. Nadav Morag, Dr. Rodrigo Nieto-Gómez, Lynda Peters, John Rollins, Paul Jonathan Smith, Dr. Lauren Wollman, and Glen Woodbury. Thank you for shaping me and the future of homeland security.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Fire service agencies struggle to receive and utilize relevant, agency-specific intelligence, which affects their ability to prevent adversarial attacks, protect the community, mitigate the impact, respond safely, and recover from such events. Accordingly, the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) directed the president of the United States to establish the Information Sharing Environment (ISE), which "provides and facilitates the means for sharing terrorism information among all appropriate Federal, State, local, and tribal entities, and the private sector through the use of policy guidelines and technologies."[1] The goal of IRTPA was to eliminate the Intelligence Community (IC)'s information and intelligence gaps between levels of governments that failed to provide the intelligence necessary to prepare for and prevent the 9/11 terrorist attacks.

To comply with the information-sharing mandates, the ISE leveraged existing mechanisms across the government. One such mechanism was the expanding network of state and local fusion centers. A fusion center is a cooperative group of agencies that work to prevent terrorist acts by pooling their resources and expertise to provide actionable intelligence to appropriate state, local, tribal, and territorial agencies (SLTT).[2] The latter include law enforcement, public health, emergency medical services, and the fire service, among others. The fusion center is designed to promote a two-way exchange of information with SLTT agencies. The government considers SLTT agencies as contributors, collaborators, and consumers of intelligence information, of which the fire service plays a significant role. In turn, fire service agencies use intelligence to drive strategic, operational, and tactical decision-making.

---

[1] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108–458, §1016, 118 Stat. 3665 (2004), https://www.dni.gov/files/NCTC/documents/RelatedContent_documents/Intelligence_Reform_Act.pdf.

[2] Department of Justice and Department of Homeland Security, *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era* (Washington, DC: Department of Justice and Department of Homeland Security, 2006), 2, https://www.it.ojp.gov/documents/d/fusion_center_guidelines.pdf.

A. RESEARCH QUESTIONS

1. What are the intelligence requirements necessary to provide the fire service direct support to inform strategic, operational, and tactical decision-making?

2. How can the fire service use intelligence to guide strategic policy development, operational planning, and tactical decision-making?

B. LITERATURE REVIEW

This literature review explores the growing body of academic literature related to the fire service and the broader intelligence enterprise. The first section discusses government and organizational reports that serve as foundational information for the domestic intelligence enterprise. The second section analyzes academic research and government reports regarding the role of fusion centers in domestic intelligence generally, and fire service intelligence more specifically. The third section explores academic research and government reports that outline the current body of knowledge regarding the Fire Service Intelligence Enterprise.

1. Intelligence Community and Information Sharing Environment

The 9/11 Commission Report and the Intelligence Reform Act fueled the reorganization of the IC and the development of the ISE to prevent surprise attacks by aligning all IC agencies. The 9/11 Commission recognized a lack of organization among the IC and six problems before and after 9/11: structural barriers to joint work, management division, lack of common practices and standards, a limited ability to establish priorities, secrecy, and too many roles concentrated in one leadership position.[3] The Intelligence Reform Act sought to eliminate the systemic barriers by giving the president the authority to develop the ISE and appoint a director of national intelligence.[4]

[3] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States* (Washington, DC: Government Printing Office, 2004), 408–10, https://digital.library.unt.edu/ark:/67531/metadc123526/.

[4] Intelligence Reform and Terrorism Prevention Act of 2004.

Erik Dahl suggests that terrorism challenged the IC well before 9/11.[5] To support his claim, he argues that "the intelligence community is limited in its ability to use traditional tools and techniques to gain insight into terrorist intentions and capabilities."[6] Furthermore, Dahl recognizes that there has been very little academic research on the importance of intelligence in combatting terrorism.[7] Dahl also advocates the need for actionable intelligence and policymaker action as essential elements to prevent surprise attacks.[8]

Likewise, Amy Zegart attributes this IC limitation to organizational issues within and among IC agencies before 9/11. More specifically, Zegart suggests that decades-old structural weaknesses, misaligned incentives and rewards, and resistance to new technologies worsened organizational deficiencies.[9] Zegart contends that since 9/11, the government and IC have undergone several adaptation failures.[10] She further suggests that bickering policymakers and posturing by the Department of Defense have weakened the IRTPA and led to continued shortcomings of the IC.[11]

Mark Lowenthal echoes the common theme of organizational issues, with the director of national intelligence having to contend with the discrepancy between his responsibilities and authority over intelligence agencies.[12] Essentially, the director of national intelligence has responsibility for the IC but does not have jurisdiction over the individual agencies. Lowenthal also points out that 80 percent of the IC is under the control of the secretary of defense.[13]

---

[5] Erik J. Dahl, *Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond* (Washington, DC: Georgetown University Press, 2013), 17.

[6] Dahl, 17.

[7] Dahl, 17.

[8] Dahl, 20.

[9] Amy B. Zegart, *Spying Blind: The CIA, the FBI, and the Origins of 9/11* (Princeton, NJ: Princeton University Press, 2007), 4.

[10] Zegart, 170.

[11] Zegart, 170–82.

[12] Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 7th ed. (Los Angeles: CQ Press, 2017), 41.

[13] Lowenthal, 43.

Despite claims of improvements to information sharing in government documents, such sharing continues to pose challenges. The *Review of the Domestic Sharing of Counterterrorism Information* suggests that the implementation of the nation's information-sharing strategy has been patchy.[14] Additionally, the report finds, "The Department of Homeland Security (DHS) Intelligence Enterprise is not as effective and valuable to the IC as it could be."[15] Other challenges include a counterterrorism mission overlap between the Federal Bureau of Investigation (FBI) and DHS, large geographic regions, a lack of clear vision, and a focus on sustainment over enhancement.[16]

The academic literature and the government review concur on the many structural impediments and organizational deficiencies within the IC. The continued problems within the IC limit the utility of such intelligence products.

2. Fusion Centers

The literature regarding fusion centers identifies connections from the IC to state and local agencies, with fusion centers serving as the hub. It informs the reader of the design and makeup of fusion centers and highlights several legal challenges facing fusion center coordinators. Furthermore, the research firmly establishes the role of the fire service within fusion centers. Unfortunately, the actual engagement of fusion centers with local agencies is sporadic. The literature is limited in that it highlights methods for integration, but it stops short of informing the fire service on how to use finished intelligence.

The 2010 "Fire Service Integration for Fusion Centers" appendix by the Department of Justice represents the first and only comprehensive government document that advocates fire service intelligence integration. The Department of Justice suggests that

[14] Offices of the Inspectors General of the Intelligence Community, Department of Homeland Security, and Department of Justice, *Review of Domestic Sharing of Counterterrorism Information* (Washington, DC: Inspectors General of the Intelligence Community, Department of Homeland Security, and Department of Justice, March 2017), i, https://www.dni.gov/files/documents/Newsroom/Domestic_Sharing_Counterterrorism_Information_Report.pdf.

[15] Offices of the Inspectors General, 9.

[16] Offices of the Inspectors General, 8–9.

the fire service's subject-matter expertise can help fusion centers meet their capabilities.[17] Specifically, the document proposes that the fire service report criminal acts and provide input on risk assessments to achieve fusion center goals.[18] Additionally, it spells out the need for intelligence to provide situational awareness to emergency personnel.[19] However, the Department of Justice highlights fire service contributions to fusion centers rather than fusion center support to the fire service. Nevertheless, citing the *National Strategy for Information Sharing*, Castro Garcia, Matei, and Bruneau suggest, "Fusion centers serve as the primary focal points within states and localities for the receipt and sharing of information on terrorism."[20]

Furthermore, the *2013 National Network of Fusion Centers Final Report* by DHS asserts, "Fusion centers are uniquely situated to enhance the national threat picture and enable local officials to better protect their communities from a variety of threats."[21] Accordingly, organizations that identify their intelligence needs for fusion centers receive the maximum benefit. Similarly, the report proposes that fusion centers' access to unique systems and local personnel allows for a complete threat picture.[22] DHS further recommends that "fusion center services must be timely and tailored to both the standing and emergent needs of requestors sufficient to accomplish desired end states and deliverables."[23] Additionally, the report offers that intelligence requirements govern the information provided by fusion centers to state and local jurisdictions. The specific

---

[17] Department of Justice, "Fire Service Integration for Fusion Centers: An Appendix to the *Baseline Capabilities for State and Major Urban Area Fusion Centers*" (Washington, DC: Department of Justice, 2010), 2.

[18] Department of Justice, 2.

[19] Department of Justice, 3.

[20] Andres de Castro Garcia, Florina Cristiana Matei, and Thomas C. Bruneau, "Combatting Terrorism through Fusion Centers: Useful Lessons from Other Experiences?" *International Journal of Intelligence and CounterIntelligence* 30, no. 4 (2017): 733, https://doi.org/10.1080/08850607.2017.1297119.

[21] Department of Homeland Security, *2013 National Network of Fusion Centers Final Report* (Washington, DC: Department of Homeland Security, 2014), v, https://www.dhs.gov/sites/default/files/publications/2013%20National%20Network%20of%20Fusion%20Centers%20Final%20Report.pdf.

[22] Department of Homeland Security, *2015 National Network of Fusion Centers Final Report* (Washington, DC: Department of Homeland Security, 2016), i, https://www.archives.gov/files/isoo/oversight-groups/sltps-pac/national-network-of-fusion-centers-2015.pdf.

[23] Department of Homeland Security, *2013 National Network of Fusion Centers*, 26.

requirements may take the form of standing information needs, strategic intelligence, operational intelligence, and tactical intelligence.

Recent academic studies have evaluated the efficacy of fusion centers in supporting fire service intelligence needs. Scott Goldstein contends that fusion centers are responsible for the analysis and distribution of intelligence.[24] Additionally, he suggests, "Fire and EMS [emergency medical services] responders have had little involvement with fusion center operations, and this directly impacts the country's safety."[25] Thomas Richardson supports Goldstein's claim in suggesting that fire service involvement in intelligence is slow and challenging.[26] Moreover, Goldstein offers that fire and EMS personnel are inconsistent in their use of information in the face of expanding roles.[27] Ultimately, Goldstein finds that using fire and EMS agencies could increase the effectiveness of fusion centers.[28] Thus, while everyone agrees that fusion centers can support fire service intelligence, barriers on the fire service side hamper such efforts.

Alternatively, Richardson suggests that the intelligence-sharing gap is between fire and law enforcement, not necessarily between fusion centers and the fire service.[29] He posits three reasons intelligence sharing is insufficient between fire and law: the need to safeguard investigations, limit the exposure of sources, and protect civil liberties.[30] To counter these assertions, Richardson acknowledges that fire and EMS personnel understand how to control privileged information.[31] In the end, Richardson finds that despite progress, dissemination of intelligence to line personnel remains inadequate.[32]

---

[24] Scott E. Goldstein, "Comparative Analysis of Fusion Center Outreach to Fire and EMS Agencies" (master's thesis, Naval Postgraduate School, 2015), xv, http://hdl.handle.net/10945/47952.

[25] Goldstein, v.

[26] Thomas J. Richardson, "Identifying Best Practices in the Dissemination of Intelligence to First Responders in the Fire and EMS Services" (master's thesis, Naval Postgraduate School, 2010), v, http://hdl.handle.net/10945/5137.

[27] Goldstein, "Comparative Analysis," xv.

[28] Goldstein, xvii.

[29] Richardson, "Identifying Best Practices," 1.

[30] Richardson, 2.

[31] Richardson, 2.

[32] Richardson, 57.

Although fusion centers serve as the focal point for state and local information sharing, numerous problems still exist. Shane Salvatore attributes these deficiencies to inadequate collaboration, no standard dissemination model, and a lack of focus on counterterrorism efforts.[33] Moreover, Salvatore finds that competing mandates, the incorporation of all-crimes or all-hazards approaches, and the lack of mutually beneficial relationships create significant hurdles.[34] Consequently, Regan and Monahan suggest, "Fusion centers that were originally oriented toward 'counterterrorism' have quickly broadened their scope to include all-crimes."[35] The implication of this shift is that fusion centers rarely provide for the intelligence needs of local agencies outside of law enforcement.

Privacy and civil liberties proponents are more critical of the role of fusion centers in intelligence processes. Regan, Monahan, and Craven find that involving the private sector, limiting transparency, and mixing law enforcement with intelligence gathering cause concern for such agencies.[36] Likewise, the American Civil Liberties Union (ACLU) raises questions regarding the efficacy of fusion center activities in preventing terrorism. They suggest that the lack of policy and oversight may lead to manipulation in the form of policy shopping.[37] The ACLU further indicates ambiguous lines of authority, participation by the private sector and the military, and excessive secrecy as encroachments on civil

---

[33] Shane A. Salvatore, "Fusion Center Challenges: Why Fusion Centers Have Failed to Meet Intelligence Sharing Expectations" (master's thesis, Naval Postgraduate School, 2018), 4, http://hdl.handle.net/10945/58358.

[34] Salvatore, 76–77.

[35] Priscilla M. Regan and Torin Monahan, "Beyond Counterterrorism: Data Sharing, Privacy, and Organizational Histories of DHS Fusion Centers," *International Journal of E-Politics* 4, no. 3 (2013): 10, https://doi.org/10.4018/jep.2013070101.

[36] Priscilla M. Regan, Torin Monahan, and Krista Craven, "Constructing the Suspicious: Data Production, Circulation, and Interpretation by DHS Fusion Centers," *Administration & Society* 47, no. 6 (2015): 742, https://doi.org/10.1177/0095399713513141.

[37] Michael German, *What's Wrong with Fusion Centers* (New York: American Civil Liberties Union, 2007), 9, https://www.aclu.org/files/pdfs/privacy/fusioncenter_20071212.pdf.

liberties.[38] Monahan and Palmer support the claims of the ACLU while adding that mission creep is also a serious concern.[39]

Despite being recognized as the focal point for dissemination of information to state and local agencies, fire and EMS integration continues to be challenging. Common themes in associated literature suggest that fusion centers work best with appropriate collaboration and by tailoring the information to the needs of said partners. Unfortunately, law enforcement does not trust its counterparts with sensitive information, and fire and EMS services do not use intelligence consistently.[40] Although these issues might seem only to involve fire and EMS agencies, other local agencies that rely on fusion centers for their intelligence needs should share this concern.

3. Local Intelligence-Led Public Safety Initiatives

A growing body of research addresses improving local public safety operations with the incorporation of intelligence processes. According to the National Consortium for the Study of Terrorism and Response to Terrorism, the expansion of intelligence in state and local agencies corresponds with growing sentiment by the IC that intelligence enhances the value of local agencies.[41] The study finds that the local level needs actionable intelligence because terrorism is a local event.[42] Other significant findings suggest that organizational leadership, viable strategic intelligence, and better leveraging of intelligence networks will improve intelligence use at the local level.[43] Rosemary Cloud echoes the need for organizational leadership in her thesis.[44] Cloud states, "The future role of the fire

---

[38] German, 4–5.

[39] Torin Monahan and Neal A. Palmer, "The Emerging Politics of DHS Fusion Centers," *Security Dialogue* 40, no. 6 (2009): 632, https://doi.org/10.1177/0967010609350314.

[40] Goldstein, "Comparative Analysis," xv.

[41] David Carter et al., *Understanding Law Enforcement Intelligence Processes: Report to the Office of University Programs, Science and Technology Directorate* (College Park, MD: National Consortium for the Study of Terrorism and Responses to Terrorism, 2014), 3, https://www.start.umd.edu/pubs/START_UnderstandingLawEnforcementIntelligenceProcesses_July2014.pdf.

[42] Carter et al., 3.

[43] Carter et al., 15–16.

[44] Rosemary R. Cloud, "Future Role of Fire Service in Homeland Security" (master's thesis, Naval Postgraduate School, 2008), http://hdl.handle.net/10945/3935.

service in homeland security will demand the need for progressive leadership, effective collaboration, intelligence engagement, and the adoption of a shifting mission that supports preparedness, prevention, response, and recovery of terrorist attacks."[45]

Alternatively, Rebecca Gonzales finds systemic barriers to involving the fire service in intelligence, and many fire service members resist the expansion of their responsibilities.[46] Gonzales suggests culture, intergroup dynamics, and the need to collaborate as stumbling blocks for the fire service.[47] Moreover, Gonzales finds that fire service leadership organizations oppose such intelligence programs, stemming from a lack of knowledge about how intelligence aids fire departments in meeting their missions.[48] Gonzales correctly notes that many experts believe intelligence is only for law enforcement as it is outside the traditional domain of the fire service.[49]

4. Public Health

Despite the challenges, numerous efforts are underway to develop locally based intelligence operations in public health, law enforcement, and the fire service. Public health agencies have struggled to gain access to information through state and local intelligence agencies. Cody Minks finds that among public health agencies surveyed, some favor integrating with fusion centers and Joint Terrorism Task Forces (JTTFs), but they currently lack representation with either unit.[50] Additionally, Minks suggests that information sharing between state agencies and local public health agencies is not improving, and no current plans focus on improving such sharing.[51] Moreover, he finds that fusion centers do

---

[45] Cloud, v.

[46] Rebecca L. Gonzales, "Transforming Executive Fire Officers: A Paradigm Shift to Meet the Intelligence Needs of the 21st Century Fire Service" (master's thesis, Naval Postgraduate School, 2010), 87–88, http://hdl.handle.net/10945/5157.

[47] Gonzales, 88.

[48] Gonzales, 89–90.

[49] Gonzales, 90.

[50] Cody Minks, "Hacking the Silos: Eliminating Information Barriers between Public Health and Law Enforcement" (master's thesis, Naval Postgraduate School, 2018), 50, http://hdl.handle.net/10945/58345.

[51] Minks, 51.

not see the added benefit of including public health agencies in fusion center operations.[52] Perhaps the fusion center's set-up as an all-crimes center and not an all-hazards center explains this reluctance to embrace public health. Finally, he concludes that fusion centers continue to present barriers to public health integration, and little public health information flows into or out of fusion centers.[53]

5. Law Enforcement

According to Marilyn Peterson, "Intelligence-led policing is a collaborative enterprise based on improved intelligence operations and community-oriented policing and problem solving, which the field has considered beneficial for many years."[54] The author contends that officers can respond more effectively to crimes by using intelligence.[55] Additionally, Peterson proposes that law enforcement agencies benefit from the increased use of fusion centers.[56] Carter describes two primary purposes for law enforcement intelligence: 1) planning and resource allocation and 2) prevention.[57] Carter states that strategic and tactical intelligence aid officers in their prevention roles.[58]

Unfortunately, law enforcement continues to distrust the fire service with intelligence information. Carter suggests that law enforcement is skeptical about the role of the fire service and unclear about what information it might share with fire service counterparts.[59] Alternatively, Peterson notes that a lack of policies, procedures, and training is the main issue with law enforcement intelligence processes.[60] Despite the problems,

---

[52] Minks, 56.

[53] Minks, 57.

[54] Marilyn Peterson, *Intelligence-Led Policing: The New Intelligence Architecture*, NCJ 210681 (Washington, DC: Bureau of Justice Assistance, 2005), vii, https://www.ncjrs.gov/pdffiles1/bja/210681.pdf.

[55] Peterson, vii.

[56] Peterson, 9.

[57] David Carter, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, 2nd ed. (Washington, DC: Department of Justice, 2004), 9, https://it.ojp.gov/documents/d/e050919201-IntelGuide_web.pdf.

[58] Carter, 9.

[59] Carter, 19.

[60] Peterson, *Intelligence-Led Policing*, vii.

Peterson submit that law enforcement needs to move away from informal practices for official policy.[61] Moreover, the Office of Community Oriented Policing Services advises local agencies to promote interoperability.[62] Finally, Carter summarizes the benefits of this cooperation: "Through sharing pre-incident information and intelligence and real-time incident updates, situational awareness will be enhanced to support the preparedness efforts of both local fire departments and the DHS."[63]

6. Fire Service

For the fire service, a large body of research highlights intelligence and information sharing at the local level. As the *Intelligence Guide for Fire Chiefs* states, "Many fire chiefs have struggled to identify a reliable source of terrorism threat intelligence that can address the specific needs of their jurisdictions and fire service operations."[64] The report also finds that the ISE continues to be improvised despite the possible benefits of including thousands of firefighters in the effort.[65] Specifically, "Law enforcement [fusion] centers are not familiar with fire service needs and generally do not interact with fire service personnel."[66] The most important finding is that the IC must understand the intelligence requirements needed by the fire service to make an informed strategic, operational, and tactical decision.[67]

Alternatively, Robson argues that because the fire service wants to distribute intelligence widely, it should exploit open-source information.[68] He offers that efficiently

---

[61] Peterson, vii.

[62] Robert Chapman et al., "Local Law Enforcement Responds to Terrorism Lessons in Prevention and Preparedness," *COPS Innovations*, last updated April 5, 2002, 2, https://cops.usdoj.gov/RIC/Publications/cops-w0125-pub.pdf.

[63] Carter, *Law Enforcement Intelligence*, 23.

[64] International Association of Fire Chiefs, *Homeland Security: Intelligence Guide for Fire Chiefs* (Fairfax, VA: International Association of Fire Chiefs, 2012), 3, http://the-security-institute.org/userfiles/file/IntelGuide4FireChiefs.pdf.

[65] International Association of Fire Chiefs, 5.

[66] International Association of Fire Chiefs, 8.

[67] International Association of Fire Chiefs, 7.

[68] Thomas A. Robson, "A Burning Need to Know: The Use of Open Source Intelligence in the Fire Service" (master's thesis, Naval Postgraduate School, 2009), 2, http://hdl.handle.net/10945/4913.

using intelligence allows the fire service to accomplish its mission of protecting communities.[69] Furthermore, he claims that the overall goal of utilizing intelligence is to save lives.[70]

On the other hand, Joseph Russo recommends that before the fire service engages the IC, it should establish internal protocols for collecting and disseminating intelligence information.[71] Additionally, he attests that valuable information rarely finds its way to operational personnel, severely limiting their situational awareness.[72] Richardson supports this need for situational awareness with an overwhelming majority of answers to his survey question.[73] Richardson adds that intelligence aids deployment decisions and strategic planning and increases the awareness of line personnel.[74] Brian Heirston suggests that information-sharing partners need to open up culturally and politically to improve fire service use of intelligence to inform decision-making.[75] Additionally, Kevin Harrison claims that absent procedures, differing technology used, and a lack of information sharing across missions have hampered operations in real-world incidents.[76]

Despite purported improvements to information sharing, the literature shows that local public health, law enforcement, and fire service agencies struggle to get the information needed. A limiting factor of the academic writing is that very few discuss public health intelligence engagement. Additionally, the research offers numerous methods for integrating and using intelligence but provides very little empirical evidence as to the efficacy of information for local agencies.

---

[69] Robson, 14.

[70] Robson, 31.

[71] Joseph Russo, "Out from Under the Rock: Improving FDNY Information Sharing" (master's thesis, Naval Postgraduate School, 2017), 64, http://hdl.handle.net/10945/53042.

[72] Russo, 64.

[73] Richardson, "Identifying Best Practices," 19.

[74] Richardson, 20.

[75] Bryan Heirston, "Terrorism Prevention and Firefighters: Where Are the Information-Sharing Boundaries?" (master's thesis, Naval Postgraduate School, 2009), 82, https://calhoun.nps.edu/handle/10945/4930.

[76] Kevin Harrison, "Improving Information Sharing in the NYC Emergency Response Community" (master's thesis, Naval Postgraduate School, 2018), 1, https://www.hsdl.org/?view&did=814723.

C. RESEARCH DESIGN

This thesis differs from the literature in that it does not seek integration, nor does it address organizational behavior deficiencies, as several academic papers already address these subjects. This thesis examines fire service intelligence requirements to improve the quality of information, making it more actionable for the fire service. Additionally, this thesis provides a practical user guide for fire service leaders detailing how to use intelligence once they receive it.

Using a qualitative gap analysis model to answer the research questions, I compared the current fire service intelligence apparatus with the desired future state.[77] This method aided in developing recommendations by analyzing processes, practices, structures, and missing strategies.[78] As part of the analysis, I surveyed fire service members through the International Association of Fire Chiefs (IAFC) and the Fire Service Section of the National Fire Protection Association. The primary goal of the inquiry was to identify the current intelligence requirements and uses of intelligence to inform decision-making. The Naval Postgraduate School's Institutional Review Board assessed my research proposal and determined that it did not constitute human subjects research.

Additionally, this research analyzed current intelligence products developed by the Chicago Fire Department's Tactical Operations Intelligence Center, New York City Fire Department (FDNY)'s *Watchline*, and the National Capital Region Threat Intelligence Consortium's first responder bulletin. The analysis identified the state of intelligence products to gain an understanding of how well the products support strategic, operational, and tactical functions.

To guide the gap analysis, this thesis employed the political, economic, sociocultural, technological, environmental, legal (PESTEL) framework. According to Ovidijus Jurevivius, "PEST or PESTEL analysis is a simple and effective tool used in situation analysis to identify the key external (macro environment level) forces that might

[77] "The Complete Guide to Gap Analysis," Smartsheet, accessed February 24, 2020, https://www.smartsheet.com/gap-analysis-method-examples.

[78] Smartsheet.

affect an organization."[79] The gap analysis with the PESTEL framework facilitated a more comprehensive evaluation. Nevertheless, because the gap analysis method does not identify root causes and the PESTEL forces are in constant flux, researchers must repeat the process. As such, researchers attempting to replicate this research must consider changes in political, economic, sociocultural, technological, environmental, and legal forces to draw the same conclusions. This thesis used information from the study to develop a set of recommendations, including the creation of a fire service intelligence requirements document and a joint intelligence guide for first response organizations.

D. CHAPTER LAYOUT

Chapter II explores the information-sharing gaps in the fire service. The first part of the chapter presents the results of a survey administered to members of the fire service. It then analyzes the results using a PESTEL analytical framework. Finally, the chapter highlights significant issues learned from the survey.

Chapter III provides an overview of intelligence, including a working definition and descriptions of the intelligence cycle and intelligence types, markings, and handling procedures. Next, it provides an overview of the intelligence community and how it integrates with the fire service. It then focuses on fire service–specific guidelines, policies, and practices. Finally, it concludes with key takeaways from the discussion.

Chapter IV uses case studies to evaluate the specific fire service intelligence products that agencies produce. The case studies assess how well agency product lines meet the criteria for intelligence at the strategic, operational, and tactical levels. For additional analysis, Chapter IV uses Mark Lowenthal's framework for identifying good intelligence. The framework analyzes intelligence products for their timeliness, suitability, digestibility, and clarity regarding knowns and unknowns.[80]

Chapter V synthesizes the information from the previous chapters, evaluates current fire intelligence support, and offers concrete recommendations for building future

[79] Ovidijus Jurevicius, "PEST & PESTEL Analysis," Strategic Management Insight, February 13, 2013, https://www.strategicmanagementinsight.com/tools/pest-pestel-analysis.html.

[80] Lowenthal, *Intelligence*, 214–15.

fire intelligence processes to serve the enterprise better. The chapter discusses aspects of fire service intelligence processes that work well and need to change or improve. Then, it details the conclusions drawn from the research with answers to the research questions. Finally, the chapter ends with a list of recommendations to improve fire service intelligence processes to inform strategic, operational, and tactical decision-making.

THIS PAGE INTENTIONALLY LEFT BLANK

II. GAPS IN FIRE SERVICE INTELLIGENCE SUPPORT, TECHNIQUES, AND PROCEDURES

Fire service agencies need timely, agency-specific intelligence to prevent adversarial attacks, assist their communities in mitigating the impact of natural and human-made disasters, and respond to and recover from such incidents. Yet many fire service agencies struggle to receive and utilize such intelligence. According to the ISE's annual report, "The U.S. Government's ability to effectively share terrorism-related information and other information related to multiple threat actors, as well as their networks, and then use that information to support a broad array of national security-related missions and activities is essential in protecting the homeland."[81] The fire service should receive such information to bolster its efforts in homeland security missions. This thesis attempts to identify the current state of intelligence and information sharing between the intelligence community and the fire service to inform strategic, operational, and tactical decision-making.

This chapter determines the level of information-sharing gaps in the fire service. The first part of the chapter presents the results of a survey conducted among members of the fire service. It then analyzes the results using a PESTEL analytical framework. Finally, this chapter highlights significant issues learned from the survey.

A. SURVEY OVERVIEW

The participants are members of the IAFC and the Fire Service Section of the National Fire Protection Association. As the goal of this thesis was to establish a practical use guide to inform strategic, operational, and tactical decision-making, no additional participants were necessary. Members of the IAFC come from all fire service ranks and all geographic areas of the United States. The participants responded to a series of demographic, yes/no, and open-ended fire service intelligence–related questions, which are

[81] Office of the Director of National Intelligence, *2018 Information Sharing Environment* (Washington, DC: Office of the Director of National Intelligence, 2018), 19, https://www.dni.gov/files/documents/FOIA/2018_Information_Sharing_Environment_Annual_Report.pdf.

detailed in the following sections. The total number of participants was 340, as determined by the survey system.

This study used LimeSurvey to develop and aggregate survey questions and answers. A brief description of the purpose of the survey and hyperlinks to the survey platform were posted on the IAFC's KnowledgeNet and the National Fire Protection Association's X-Change web portals. The intent of the survey was to identify gaps in fire service intelligence processes. The expected gains from the survey included identifying the perceived ideal state for a fire service intelligence enterprise. In addition, the survey sought to identify barriers to fire departments' receiving, disseminating, and utilizing finished intelligence products. Finally, the survey identified intelligence requirements for fire service agencies.

B. DEMOGRAPHIC QUESTIONS

1. What type of fire department is represented?

Participants in the survey work for a variety of fire service organizations. The overwhelming majority of participants, 67.95 percent, identified their departments as career agencies. In such organizations, firefighters receive compensation and are full-time employees.[82] Another 25.32 percent of the participants identified their agencies as combination fire departments. The *Code of Federal Regulations* defines a combination department as "a fire suppression agency or organization in which at least one active firefighter receives financial compensation for his/her services rendered on behalf of the department, and at least one active firefighter does not receive financial compensation."[83] Additionally, 4.17 percent of participants work for volunteer agencies, which provide no financial compensation. Finally, 0.96 percent of participants identified their departments as "other," which included a paid on-call agency, a state forestry agency, and a state fire academy. See Figure 1 for the fire agency types represented in the survey.

[82] Assistance to Firefighters Grant Program, 44 C.F.R. § 152.2 (2011), https://www.law.cornell.edu/cfr/text/44/152.2.

[83] Assistance to Firefighters Grant Program.

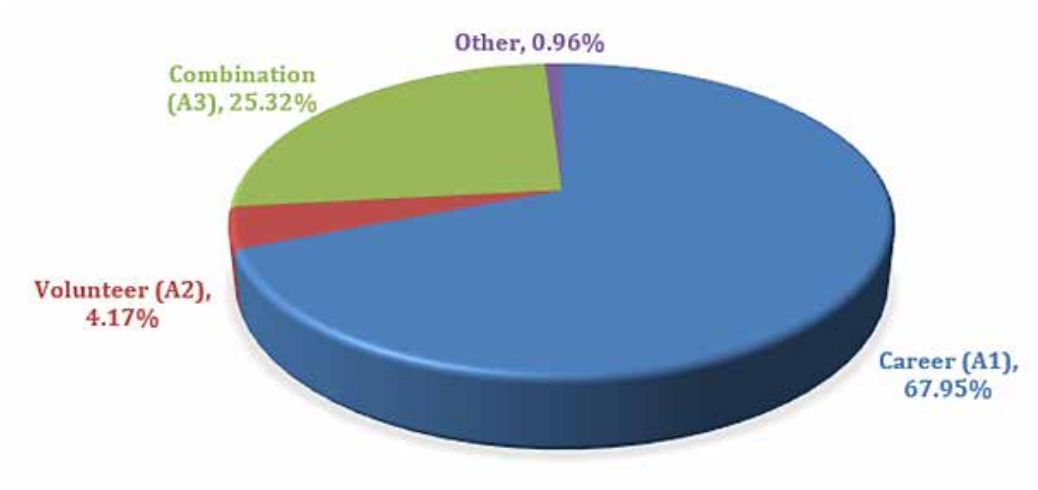


Figure 1. Fire Service Agencies Represented in the Survey

2. How many personnel are there in the department?

The participants in the survey represent agencies that differ greatly in the number of personnel. The most significant sub-section, 56.73 percent, represented agencies with 100 or fewer personnel. Another 18.59 percent represented agencies with more than 400 personnel. Additionally, 15.06 percent of participants represented agencies with 101–200 personnel. Finally, 5.13 percent of participants represented agencies with 201–300 personnel, and 2.88 percent represented agencies with 301–400 personnel. See Figure 2 for the number of personnel in the represented fire agencies.

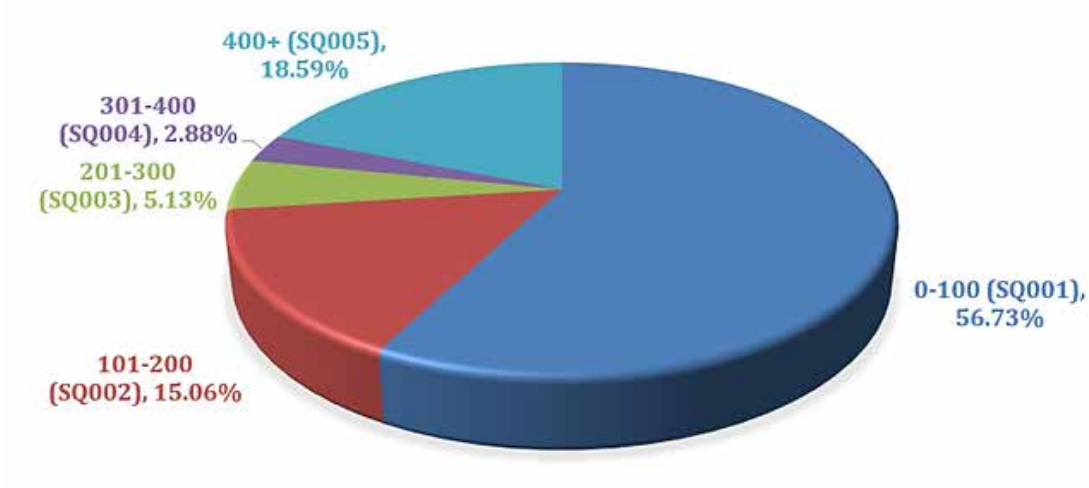


Figure 2. Number of Personnel in the Represented Departments

3. Please specify the geographic location of the department.

Representing 31.41 percent of all fire service agencies, more respondents hailed from the Midwest than from any other region. Another 24.36 percent of the agencies represented the Northeast. Additionally, 18.59 percent of the participants represented departments in the Southeast. The West, Southwest, and Northwest rounded out the list with 9.29 percent, 8.97 percent, and 7.37 percent, respectively. Understanding the demographic makeup of participant agencies is essential because the aim of this thesis is to develop an operational guide for fire service agencies, regardless of geographic location or degree of intelligence integration. See Figure 3 for a breakdown by region.

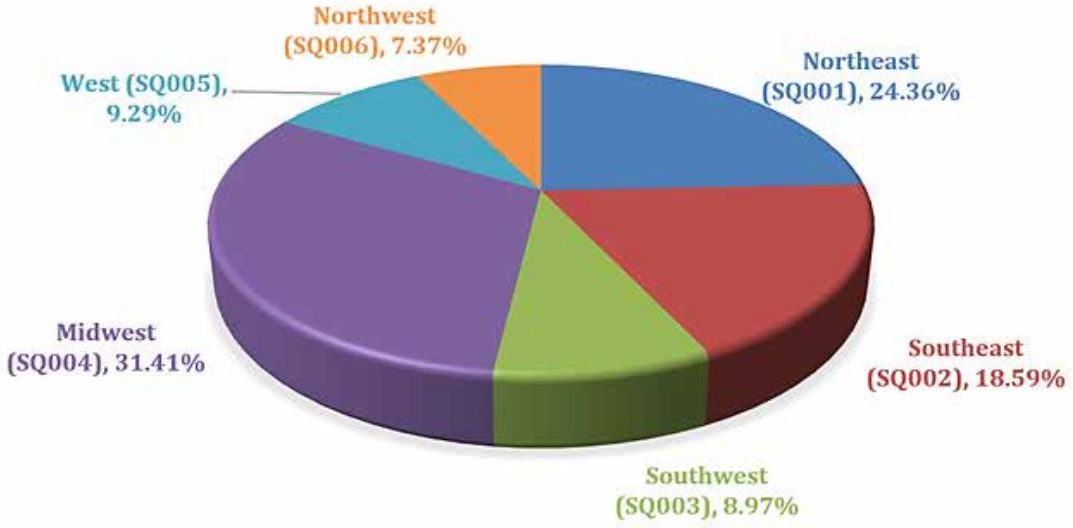


Figure 3. Geographic Regions of the Fire Departments

C. INTELLIGENCE QUESTIONS

1. What would the fire service role in the intelligence community look like?

Establishing the ideal future state of the fire service intelligence enterprise helped to identify the gaps in fire service intelligence policies and practices. The first intelligence-specific question sought to establish that foundation by asking the participants for their input on what role the fire service should have in the overall intelligence enterprise. The open-ended question solicited responses from participants in their own words. The participants identified three vital roles for the fire service in the intelligence enterprise—namely, collaborator, consumer, and collector.

a. Collaborator

For collaboration, participants suggest that fire service agencies should have a seat at the table, similar to that of a unified command. For example, one participant suggested connecting with local, state, and federal partners to build relationships and trust to obtain information that could be disseminated to the members of the department. Alternatively, a different participant submitted that the effort should include fire service representatives researching, analyzing, and sharing fire service–specific information and serving as

subject-matter experts with law enforcement representatives. Another participant advised that fire service agencies should have a seat at the table because they understand how different scenarios will affect fire service operations. Moreover, a different participant supported the assertion by suggesting the need for integrated response planning. Still, others suggested that the fire service should be a collector, analyst, disseminator, and recipient of intelligence.

To further support collaborative efforts, several participants suggested differing forms of integration. In the survey, 11 participants recommended fire service participation in state and local fusion centers and JTTFs. Alternatively, five participants recommended that fire service personnel participate as terrorism liaison officers in their respective jurisdictions. Additionally, participants suggested that the fire service take on the role of subject-matter experts who contribute to the overall homeland security mission. Furthermore, participants envisioned a two-way information-sharing system that provides real-time intelligence sharing and a common operating picture between pertinent partners.

b. Consumer

The participants also offered numerous suggestions for the ideal state of fire service intelligence consumption. While most of the responses were general, others suggested more specific intelligence needs. The intelligence needs centered on personnel safety, operational and situational awareness, preparation, planning, and response. First, several participants pointed to the need for intelligence to provide for the safety of response personnel. For example, one participant suggested the need for information on credible threats or operations that pose a high risk to first responders. Alternatively, a different participant proposed the need for intelligence on atypical threats. Moreover, one participant advised that fire service agencies need warning intelligence, so firefighters may understand how to respond to various incidents. Finally, one participant asserted that the fire service should receive intelligence only for personnel safety, suggesting that too much information would lead to overload.

Second, participants believed the fire service needs intelligence for operational and situational awareness. For instance, one participant emphasized the need for the fire service

to receive intelligence regarding influxes of narcotics, large gatherings, or any threat to public safety. On the other hand, another participant suggested a need for information on pending natural disasters such as storms and reinforced the need for information on large gatherings. Also, participants recounted the need for intelligence regarding target hazards, high-profile visitors, festivals, and high-risk populations. Furthermore, participants maintained that the fire service needs intelligence regarding active violence incidents, pandemics, arson, and bomb threats. Finally, one participant recommended receiving intelligence on high-risk occupancies, including illegal drug manufacturing facilities, and known locations where occupants have a history of threatening first responders.

Also, participants highlighted a need for intelligence to guide preparations in an all-hazards environment. In this case, participants suggested that having an understanding of particular issues is useful in preparing fire service organizations. Also, nine participants suggested that fire service training may benefit from the receipt of intelligence. Furthermore, one participant advised of the intelligence need for ongoing risk-and-needs assessments. Likewise, participants emphasized that understanding threats allow fire departments to match threats with known capabilities and to acquire new capabilities.

For planning purposes, fire service participants believe there is a need for the fire service to work jointly with law enforcement to develop operational plans. As such, four participants argued that firefighters should work in tandem with law enforcement to explore all aspects and impacts when developing plans and to aid in identifying potential targets for better community protection. Other participants supported the claim and suggested the need for both proactive and reactive planning. Moreover, participants advised that the fire service and law enforcement should receive and be privy to the same information concurrently.

Finally, fire service agencies insist on the need to receive all pertinent information that may interfere with responses. One particular threat, fire as a weapon, seems to be particularly important to fire service agencies. As such, some participants acknowledged that fire as a weapon is of paramount concern. Another critical topic involves the receipt of real-time, tactical-level information. Five participants identified the need for real-time

information for deployment decisions, on-scene decision-making, and variations to response routing.

c. Collector

Several participants emphasized the need for collecting and sharing information with law enforcement and other homeland security–related entities. As such, 23 participants suggested that there is value in fire service agencies' documenting and reporting information through suspicious activity reporting or other secure communication means. Alternatively, some participants argued for sharing fire service–specific information, such as inspection information, target hazards, building layouts, risk assessments, and hazardous materials. Still, other participants believe the fire service should offer direct support to law enforcement in intelligence gathering. For example, one participant argued for using fire service aerial ladders and drones for local imaging. Similarly, another participant supported providing the intelligence community with information on fire service capabilities, so it might assess how to utilize fire agencies during incidents.

Alternatively, some participants insisted that the fire service should limit its interaction within the intelligence enterprise to an advisory role. A few others were unsure about where the fire service fits into the intelligence apparatus. For example, one participant suggested that the uncertainty might be the result of a lack of fire service inclusion in intelligence activities. Finally, another participant suggested that the fire service does not have any formal role in intelligence.

2. What are some fire department concerns about receiving intelligence?

Survey participants offered 17 different concerns for the fire service regarding the receipt of intelligence. Approximately 44 percent of participants suggested that security and handling of intelligence are of paramount concern. Another 25 percent reported that the intelligence they receive lacks timeliness and credibility. Additionally, 17.5 percent of participants claimed they do not receive intelligence, or they receive it sporadically. Moreover, 8 percent of participants asserted that the fire service lacks analytical abilities and an understanding of how to use finished intelligence.

Furthermore, participants expressed concerns about receiving too much intelligence. To a minor extent, participants seem concerned over legal issues such as liability against the department, protection of civil liberties, and the questionable statutory authority to engage in intelligence activities. Also, participants expressed concerns about mission overlap and a lack of coordination with law enforcement agencies. Finally, three participants emphasized that engaging in intelligence activities might affect the public perception of firefighters.

3. What type of interaction does the department have with state or local fusion centers?

According to the survey, fire service interaction with state and local fusion centers varies greatly. Of the participants, 34.6 percent claimed they have little to no interactions with state and local fusion centers. However, 31.7 percent of participants suggested they have close relationships with state and local fusion centers. Moreover, 25 percent of the participants stressed they have no formal interaction with fusion centers. Still, others advised that they interact with fusion centers through terrorism liaison officers or on an as-needed basis. Finally, 7 percent of participants stated they were unsure about their departments' interactions with fusion centers.

4. Does the organization supplying intelligence understand the fire department's intelligence needs?

In answering this question, 44.54 percent of the participants answered yes, and 52.1 percent answered no. The remaining 3.36 percent of participants did not offer a response to the question. See Figure 4 for a breakdown of these responses.

Figure 4. Perception That the Organization Supplying Intelligence Understands Fire Service Needs

5. What are the department's preferred ways to receive information/ intelligence?

The results of the question revealed that 75.63 percent of all participants receive their intelligence from state and local fusion centers. The percentage suggests that there is considerable integration of the fire service within fusion centers. Comparatively, 72.27 percent of participants receive intelligence from state or local intelligence units. The information reveals that fire service agencies leverage partnerships with law enforcement to a great extent. Additionally, 61.34 percent of participants use the Homeland Security Information Network (HSIN) for their intelligence needs. The result suggests that a majority of fire service agencies are familiar with the network, and they seek intelligence and information on their own. Alternatively, 46.22 percent of participant agencies receive their intelligence directly from a JTTF, suggesting that the FBI considers the fire service an information-sharing partner. To a lesser extent, 15.97 percent of fire service agencies create their intelligence internally. Finally, the remaining 11.76 percent of participants selected "other," with two participants stating their agencies do not receive intelligence. The remaining agencies receive their intelligence from the following sources:

- Arson Task Force
- Local jurisdictional briefings
- Illinois Mutual Aid Box Alarm System

- Other fire departments
- Technical Resources for Incident Prevention and the Bomb and Arson Tracking System
- Interagency Fire Intelligence Exchange

Figure 5 represents the sources of intelligence for fire departments that participated in the survey. Because this question allowed participants to select all applicable sources, the numbers do not add up to 100 percent. The graph further acknowledges that some agencies receive intelligence from multiple sources.

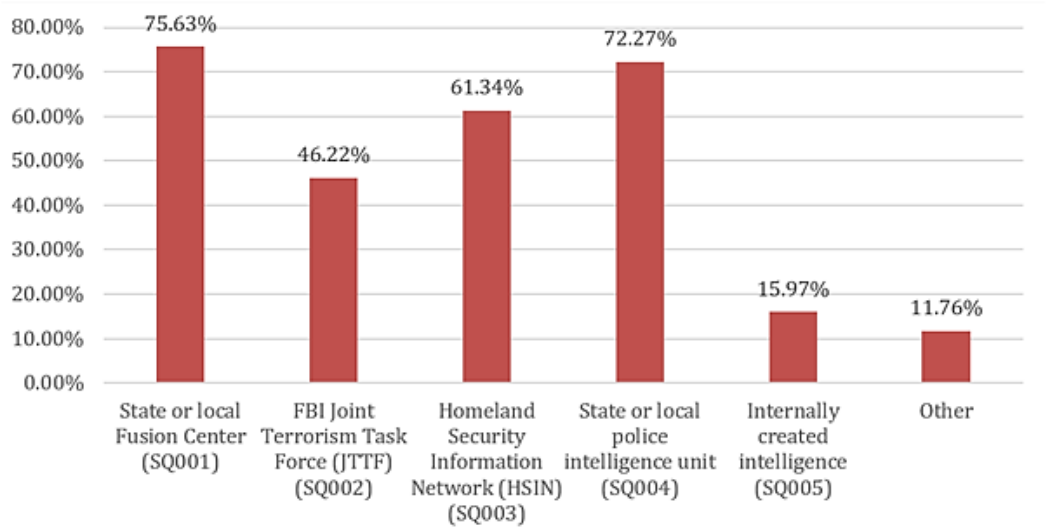


Figure 5. Sources of Intelligence for Survey Participants

6. Is received intelligence of value to the department?

Although 52.1 percent of participants believe that the organizations providing intelligence do not understand fire service intelligence needs, 88.24 percent suggested that the intelligence they receive is of value. In contrast, 8.4 percent of participants believe the intelligence they receive offers little value to their agencies. An additional 3.36 percent of participants declined to provide an answer to the question but were included to ensure the pie chart represented 100 percent of respondents.

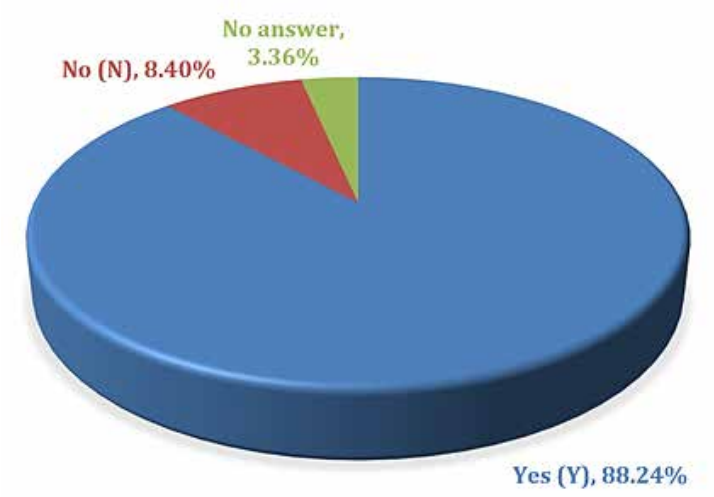


Figure 6. Percentage That Believe Received Intelligence Is of Value

7. How is intelligence disseminated to the rank and file?

In responding to the question on intelligence dissemination to the rank and file, participants offered a medley of answers. Of those surveyed, 35 participant departments disseminate intelligence to the rank and file through departmental email. Another 22 participants acknowledged that their departments spread information during face-to-face briefings. Moreover, eight participants maintained that their departments distribute intelligence information through the chain of command, departmental distribution systems, memoranda, policies, procedures, list serves, and bulletin boards. Other participants mentioned sharing intelligence during training, through terrorism liaison officers, and in caution notes documented in computer-aided dispatch systems.

Additionally, the results of the survey reveal that fire service agencies are creating internal barriers to intelligence and information sharing. At least 18 participants suggested that battalion chiefs and above receive intelligence. In addition, 17 participants emphasized that their departments share intelligence only on a need-to-know basis. Finally, 15 participants stated that their departments do not share intelligence at any level. This author argues that departments should disseminate intelligence under a need-to-share concept. The distinction is important because fire service agencies already struggle to receive intelligence, and employing artificial barriers limits its utility.

8. What type of intelligence or information does the department need for standing information requirements?

This question sought to establish the standing information needs of fire service agencies. A majority of participants, 62 percent, stated that they need specific threat information on known homeland security issues that may affect first responders. Additionally, several respondents indicated they need information for situational awareness to prevent the loss of life and to inform response decisions. Still, others suggested the need for contextual information, so they might understand the entire threat picture. Some of the participants identified specific information they need—such as information on sovereign citizens; national-level concerns; cyber threats; human smuggling; pandemics; threats to critical infrastructure and key resources; threats made via social media; weapons of mass destruction (WMD) threats; theft of first responder uniforms, vehicles, and equipment; civil unrest; school threats; and explosives. Finally, about 10 percent of respondents were unsure about their departments' standing information needs.

9. How does the department use information/intelligence to support daily operations?

About 35 percent of respondents stated their departments use information/intelligence to maintain situational awareness. Another 21 percent indicated that their departments do not currently use information/intelligence to support daily operations. Also, 14 percent specified that their departments use intelligence to inform operational staffing decisions while another 13 percent use intelligence in their planning processes. Additionally, about 8 percent of the participants mentioned they use information/intelligence for training purposes. The remaining participants mentioned that their departments use information/intelligence to share with other agencies, make equipment purchases, identify force protection needs, and make deployment decisions.

10. What type of intelligence is required for strategic decision-making?

Approximately 35 percent of respondents mentioned their departments need intelligence on credible threats to inform their strategic decision-making. About 29 percent

stated their departments need information on terrorist trends. Additionally, 17 percent of respondents indicated their departments need any intelligence or threat information that may affect their responses or resources. Furthermore, 8 percent of respondents did not know what type of intelligence their departments need to guide strategic decision-making. The remaining respondents mentioned the need for predictive intelligence, specific targets, cyber threats, or intelligence that informs strategic equipment purchases and staffing.

11. What type of intelligence is required for operational decision-making?

Regarding the intelligence required for operational decision-making, 38 percent of respondents stated their departments need intelligence on credible threats. Additionally, 22 percent identified that their departments require intelligence on any issues that might hamper their responses or operations. Another 17 percent indicated their departments need specific details regarding potential target locations or threats. Furthermore, 10 percent do not know what type of intelligence their departments need because they do not know what intelligence is available to their departments. Finally, the remaining respondents mentioned that their departments need intelligence that guides their equipment purchases, staffing, data analysis, training, or force protection needs.

12. What type of intelligence is required for tactical decision-making?

For tactical decision-making, 60 percent of respondents indicated that their departments require intelligence on credible, specific threats. Another 12 percent of respondents mentioned needing intelligence on issues that affect their responses. Additionally, 12 percent stated they do not know what type of intelligence their departments need for tactical-level decision-making. The remaining respondents identified the need for intelligence in developing contingency plans and training and ensuring they have available resources to manage the threat.

D. PESTEL ANALYTICAL FRAMEWORK

The PESTEL framework analyzes external forces that affect organizations through multiple overlapping channels. The external forces include political, economic, sociocultural, technological, environmental, and legal categories.

1. Political Issues

Respondents to the survey identified several issues that belong in the political realm. First, respondents indicated that fire service agencies should have an equal seat at the table regarding information and intelligence sharing. Second, they suggested that governments at all levels lack understanding of fire service intelligence needs. In addition, they mentioned that fire service integration into fusion centers and the overall intelligence community is highly sporadic. Still, others highlighted that political mechanisms prevent law enforcement and fusion centers from sharing intelligence information with the fire service. The problem persists despite numerous guidance and strategy documents suggesting that the fire service may play a pivotal role in the ISE.[84] Finally, many participants pointed out that their departments rely on ad hoc relationships with local law enforcement to obtain their intelligence. However, there is some political acceptance of the fire service in the ISE, despite implementation issues. The findings are significant because the fire service must have access to timely, relevant information and intelligence to fulfill its pivotal role in the homeland security domain. Based on these findings, new strategy documents should mandate intelligence and information sharing among all levels of the government and between all first response agencies.

---

[84] Department of Homeland Security, *Fire Service Intelligence Enterprise: Concept Plan* (Washington, DC: Department of Homeland Security, August 2009); Department of Homeland Security, *2013 National Network of Fusion Centers*; Department of Homeland Security, *2015 National Network of Fusion Centers*; Department of Justice, "Fire Service Integration"; Homeland Security Advisory Council, "Intelligence and Information Sharing Initiative: Homeland Security Intelligence & Information Fusion" (Washington, DC: Department of Homeland Security, 2005); Interagency Threat Assessment and Coordination Group, *Intelligence Guide for First Responders*, 2nd ed. (Washington, DC: Office of the Director of National Intelligence, 2011), https://permanent.access.gpo.gov/gpo12126/ITACG_Guide_for_First_Responders_2011.pdf; International Association of Fire Chiefs, *Intelligence Guide for Fire Chiefs*; Joint Counterterrorism Assessment Team, *JCAT Intelligence Guide for First Responders* (Washington, DC: Office of the Director of National Intelligence, 2015), https://www.dni.gov/nctc/jcat/jcat_ctguide/intel_guide.html; Office of Homeland Security, *National Strategy for Homeland Security* (Washington, DC: White House, 2002), ProQuest; National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report*; Executive Office of the President, *National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing* (Washington, DC: White House, 2007), 3, https://apps.dtic.mil/dtic/tr/fulltext/u2/a473664.pdf; Office of the Director of National Intelligence, *Domestic Approach to National Intelligence* (Washington, DC: Office of the Director of National Intelligence, 2016), https://www.dni.gov/files/documents/Newsroom/DomesticApproachtoNationalIntelligence.PDF; Office of the Director of National Intelligence, *2018 Information Sharing Environment*.

2. Economic Issues

In responding to the survey, the participants highlighted the economic issues their departments face regarding information sharing. A significant issue affecting fire service agencies is the lack of training and expertise in the uses of intelligence. Additionally, participants indicated that they lack funding to purchase the necessary information systems to support their information-sharing initiatives. Moreover, some fire service agencies do not have funding available to detail personnel to fusion centers or other intelligence agencies. Finally, participants emphasized that their agencies lack the funding to pay for and obtain security clearances for their personnel. Although this author agrees that fire service agencies struggle with funding, there are grant opportunities available to offset some of the economic burdens.

3. Socio-Cultural Issues

Participants of the survey indicated that several socio-cultural challenges affect fire service intelligence processes. First, participants pointed to trust issues among the fire service, law enforcement, and the greater intelligence community. More specifically, participants stated that the intelligence community often overlooks the fire service because it lacks a law enforcement nexus. Additionally, law enforcement agencies worry about intelligence leaks that might compromise investigations. Another issue is that the fire service believes it might lose community trust if it more closely aligns with law enforcement and begins community surveillance activities. Finally, cultural differences between the fire service and law enforcement add to the mistrust. Participants suggested that the fire service tends to share information more broadly while law enforcement tends to share information on a need-to-know basis.

The cultural differences between fire and law enforcement agencies limit their collaboration on other homeland security projects. For example, survey participants mentioned a lack of integrated response planning and little collaboration on intelligence products. Additionally, participants stated that the lack of collaboration leads to inconsistent receipt of intelligence, and the intelligence they do receive lacks relevance to the fire service mission. Furthermore, the cultural barriers prevent law enforcement

agencies from gaining an awareness of fire service capabilities and limit their use of fire personnel as subject-matter experts. Moreover, as intelligence is mostly in the domain of law enforcement, the fire service lacks analytic capabilities, and often the exchange of information lacks timeliness. What this author takes away from experience with law enforcement is that fire service agencies gain trust through greater collaboration. Moreover, better collaboration and communication between the two disciplines might eliminate most of the cultural barriers to intelligence and information sharing. These findings have important implications for the broader domain of homeland security because the fire service and law enforcement are among the first to respond to incidents, and their daily operations may allow them to identify terrorist plots before they occur.

4. Technological Issues

Technology use in the fire service is increasing dramatically. As such, several participants highlighted some of the technological issues associated with information sharing. First, they highlighted that the fire service and law enforcement do not have a shared intelligence platform. Participants stated that not having a shared system limits the sharing of real-time information, and the fire service does not have a common operating picture with law enforcement. Additionally, participants indicated that their departments do not have an easily accessible reporting platform to submit suspicious activity reports.

Furthermore, participants mentioned that their departments lack secure intelligence interfaces and raised concern about protecting sensitive information. Moreover, departments that use the HSIN find it cumbersome and the periodic password changes frustrating. Finally, participants indicated that their departments are concerned with cyber operations. Understanding the technological challenges is important because first response agencies rely on speed and accuracy of intelligence to maintain situational awareness while responding to incidents.

5. Environmental Issues

The current threat environment is dynamic and ever-changing. As such, survey participants specified several environmental issues that are of concern to their agencies. A primary concern is the use of fire as a weapon, as noted by several participants.

Additionally, fire service agencies have raised concern about the shift from international to domestic terrorism. Several participants cited right-wing movements, sovereign citizens, and homegrown violent extremists as particular areas of concern. As safety is always a priority, several participants highlighted emerging threats and attacks on first responders as essential environmental topics. Additionally, participants indicated that more nascent issues, such as protests, pandemics, natural disasters, and active-shooter incidents, are critical topics for consideration.

6. Legal Issues

In a litigious society like the United States, legal issues are of paramount concern for fire service agencies. Expressly, participants indicated that their agencies have concerns with lawsuits against their personnel for engaging in information sharing and suspicious activity reporting. An additional legal issue of concern to departments is whether fire service agencies have statutory authority to engage in intelligence activities and view law enforcement sensitive information. Finally, participants indicated that their agencies have concerns regarding privacy and civil liberty protections as they relate to intelligence gathering.

E. CONCLUSION

Overall, the participants in the survey offered useful information, which is not found elsewhere, to guide the development of a fire service information-sharing strategy. First, fire service agencies believe they should be equal partners in intelligence activities and engage in joint planning with their law enforcement counterparts. Second, the survey identifies several successful forms of integration for the fire service, eliminating the need for a one-size-fits-all approach. However, some agencies still experience difficulty with intelligence integration. Additionally, the participants identified a lack of understanding of fire service requirements by intelligence-providing agencies. However, an analysis of the survey answers reveals that fire service agencies are unclear of their role in establishing intelligence requirements and forwarding them to their intelligence provider for tasking. Furthermore, participants offered evidence that many in the fire service do not know how to use finished intelligence products. Moreover, the survey suggests that fire service

agencies lack analytical capabilities and have trouble distinguishing between strategic-, operational-, and tactical-level intelligence needs. However, analytical capabilities vary between departments. Some agencies have dedicated intelligence officers who provide analysis and context. Other agencies rely primarily on analysis and interpretations from their intelligence providers. Additionally, participants advised that there are trust issues between the fire service and law enforcement, and they fear losing trust within the community. Finally, some participants are unclear on their statutory authority to engage in intelligence activities. Chapter III explores intelligence policies and practices to identify the current state of the intelligence enterprise for comparison with the gaps identified in this chapter.

THIS PAGE INTENTIONALLY LEFT BLANK

III. CURRENT FIRE SERVICE OPERATIONAL INTELLIGENCE POLICIES AND PRACTICES

Chapter II offered a fresh perspective on the intelligence needs and challenges of the fire service. The current policies and practices that govern intelligence activities in the United States follow logically. A fair assessment of the value and relevance of fire service intelligence activities requires understanding what intelligence is, where it comes from, and how the fire service uses it. This chapter first provides an overview of intelligence, including a working definition, a description of the intelligence cycle, and a description of intelligence types, markings, and handling procedures. Next, it provides an overview of the intelligence community and how it integrates with the fire service. It then focuses on fire service–specific guidelines, policies, and practices. Finally, it concludes with key takeaways from the discussion.

A. INTELLIGENCE OVERVIEW

1. Intelligence Definition

There are several definitions of intelligence. According to Mark Lowenthal, "Intelligence is the process by which specific types of information important to national security are requested, collected, analyzed, and provided to policy makers."[85] Lyman Kilpatrick defines intelligence as "the knowledge—and, ideally, foreknowledge—sought by nations in response to external threats and to protect their vital interests, especially the well-being of their own people."[86] Others define intelligence as the ability to estimate changes in time to adjust to the changes.[87] Lowenthal's characterization serves as the definition for this thesis. This distinction is significant because an apt definition allows for a better understanding of the subject.

---

[85] Lowenthal, *Intelligence*, 10.

[86] Michael Warner, "Wanted: A Definition of 'Intelligence,'" *Studies in Intelligence* 46, no. 3 (2002): 3.

[87] Lowenthal, *Intelligence*, 10.

2. The Intelligence Cycle

The intelligence cycle is the process practitioners use to gather information, process it, and deliver intelligence products to policymakers.[88] The process varies by country and has between five and seven steps. Johnson and Wirtz describe five steps in the cycle: planning and direction, collection, processing, analysis and production, and dissemination.[89] Alternatively, Lowenthal identifies seven steps: identifying requirements, collection, processing and exploitation, analysis and production, dissemination, consumption, and feedback.[90] The following details Lowenthal's seven steps:

1. Identifying Requirements: The process of identifying the policy interests and priorities for gathering intelligence.[91]
2. Collection: The process of identifying methods and gathering information based on the requirements.[92]
3. Processing and Exploitation: The steps necessary to transform collected information into intelligence.[93]
4. Analysis and Production: The process of assigning meaning to intelligence and developing intelligence products.[94]
5. Dissemination: The process of providing consumers with finished intelligence products.[95]
6. Consumption: The process of reviewing and using finished intelligence by policymakers.[96]

---

[88] Loch K. Johnson and James J. Wirtz, eds., *Intelligence: The Secret World of Spies: An Anthology*, 5th ed. (New York: Oxford University Press, 2019), 45.

[89] Johnson and Wirtz, 45.

[90] Lowenthal, *Intelligence*, 73.

[91] Lowenthal, 74.

[92] Lowenthal, 80.

[93] Lowenthal, 81.

[94] Lowenthal, 82–83.

[95] Lowenthal, 84.

[96] Lowenthal, 75.

7. Feedback: A dialogue between producers and consumers to detail how well they met the requirements, make adjustments to finished products, or establish updated requirements.[97]

The intelligence cycle provides consumers with knowledge for decision-making advantage. The distinction is important because many of the survey participants acknowledged that they were unsure of what intelligence is available to inform their decisions. Ultimately, policy- and decision-makers must provide the agencies that process their intelligence with information to establish requirements.

3. Intelligence Levels and Application

Three levels of intelligence guide decision-making at the organizational level: strategic, operational, and tactical.[98] According to the Department of Defense, "The levels provide a doctrinal perspective that clarifies the links between strategic objectives, effects, and tactical actions and assists commanders in visualizing a logical flow of operations, allocating resources, and assigning tasks."[99] Determining whether an action is strategic, operational, or tactical depends on how it contributes to achieving the respective goals.[100]

a. Strategic Intelligence

Strategic intelligence looks at long-term issues that may affect how an organization plans for the future. Intelligence analysts create strategic intelligence for executive-level officials, such as fire chiefs, assistant chiefs, and deputy chiefs in the fire service. Accordingly, executive officials use strategic intelligence to develop strategies and policies, assist with strategic planning activities, identify trends, and support strategic-level operations.[101]

---

[97] Lowenthal, 75.

[98] Joint Chiefs of Staff, *Joint Intelligence*, JP 2-0 (Washington, DC: Joint Chiefs of Staff, 2007), I-21–22.

[99] Joint Chiefs of Staff, I-21.

[100] Joint Chiefs of Staff, I-21.

[101] Joint Chiefs of Staff, I-21.

b. Operational Intelligence

Operational intelligence looks at the information needed for short- to mid-term issues that may affect agency operations. Intelligence analysts create operational intelligence to serve mid-level officials, such as battalion chiefs, division chiefs, or district chiefs in the fire service. As such, mid-level managers use operational intelligence to plan operations; monitor events; match capabilities to threats; provide relevant, timely, and credible assessments; and monitor natural or human-made disasters.[102]

c. Tactical Intelligence

Tactical intelligence is perishable intelligence that supports current tactical operations and keeps personnel out of danger. Intelligence analysts create tactical intelligence for line supervisors and incident commanders, such as lieutenants, captains, and battalion chiefs. Accordingly, line supervisors and incident commanders use tactical intelligence to inform decision-making to achieve tactical objectives. Therefore, tactical intelligence must be accurate, relevant, timely, and precise, with detailed information on who, what, when, where, and how.[103] Additionally, tactical intelligence provides incident commanders with information on imminent threats to response personnel.[104]

4. Intelligence Types

The IC gathers intelligence through numerous methods. The first is open-source intelligence, which is intelligence gathered from public information sources.[105] Next is geospatial intelligence, which is information gathered from various imaging methods, such as spy planes and satellites.[106] Also, there is signals intelligence (SIGINT), which is the gathering of information over electronic media, such as telephones and internet communications.[107] SIGINT also includes communications intelligence, the collection of

---

[102] Joint Counterterrorism Assessment Team, *Intelligence Guide*, I-22.

[103] Joint Counterterrorism Assessment Team, I-22.

[104] Joint Counterterrorism Assessment Team, I-22.

[105] Johnson and Wirtz, *Intelligence*, 48.

[106] Johnson and Wirtz, 48–49.

[107] Johnson and Wirtz, 49–50.

information from telecommunications such as radio waves.[108] Electronic intelligence is also a sub-field of SIGINT, which collects radar signatures and electronic fingerprints.[109] Additionally, there is what the military calls measurements and signatures intelligence, which captures information from the telemetry emissions of missiles, as well as acoustic and seismic information.[110] Finally, there is human intelligence, which agents gather from espionage activities either directly or through proxies.[111] Individually, the sources have distinct advantages and disadvantages and provide only pieces of a larger puzzle; however, such a broad discussion is beyond the scope of this thesis. To leverage the advantages and limit the disadvantages, the IC engages in all-source fusion processes to develop a comprehensive understanding of adversaries.[112] Understanding the various methods available gives policymakers greater insight into how they might frame their intelligence requirements.

5. Intelligence Markings and Handling Requirements

Fire service personnel must be aware of intelligence classifications and handling requirements if they gain access to and use such information. The sensitive nature of intelligence necessitates specific markings and handling. The overarching types of intelligence and information are classified national security information (CNSI) and controlled unclassified information (CUI).[113] Ultimately, understanding the unique markings and handling requirements allows fire service agencies to understand how to disseminate and protect such information from public view.

Fire service personnel with security clearances may be entrusted with receiving CNSI material. The most sensitive national security information is subject to CNSI

---

[108] "INTelligence: Signals Intelligence," Central Intelligence Agency, last updated April 30, 2013, https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/intelligence-signals-intelligence-1.html.

[109] Central Intelligence Agency.

[110] Johnson and Wirtz, *Intelligence*, 50.

[111] Johnson and Wirtz, 50–51.

[112] Johnson and Wirtz, 51.

[113] Center for Development of Security Excellence, *Marking Classified Information Job Aid* (Linthicum, MD: Defense Security Service, 2017), 31.

classification procedures. According to DHS, "Classified information is information that has been determined by a delegated official within the Executive Branch of the Federal Government to require protection because its release or disclosure could cause damage to the national security."[114] Additionally, the organization responsible for the intelligence identifies it by one of three classification levels. The classification levels are top secret, secret, and confidential, and each has differing criteria for such classification. Top secret information is any information with which unauthorized disclosure may cause "exceptionally grave damage to the national security."[115] Alternatively, the system identifies secret information as that which may cause serious damage to national security if an agency releases it without authorization.[116] Finally, the system identifies confidential information as that which may cause damage to national security.[117] The takeaway from this section is that fire service personnel who attain security clearances must understand how to safeguard and store sensitive national security information.

Alternatively, most fire service personnel may be privy to CUI information, through various means, with a need to know in carrying out their roles and responsibilities. CUI information includes For Official Use Only and Law Enforcement Sensitive subsets. Accordingly, the Defense Security Service defines CUI "as unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies."[118] A critical distinction between CNSI and CUI is that a security clearance is unnecessary to receive CUI information, but a person must pass a background examination.[119] Additionally, agencies cannot combine CNSI markings with other classifiers, while CUI information commonly uses additional terms. This terminology includes identifiers such as For Official Use Only (FOUO), Law

---

[114] Department of Homeland Security, *Safeguarding Classified and Sensitive but Unclassified Information: Reference Booklet for State, Local, Tribal and Private Sector Programs* (Washington, DC: Department of Homeland Security, 2005), 6, https://homeport.uscg.mil/Lists/Content/Attachments/2110/SecurityReferenceStateLocalTribalPrivateSector.pdf.

[115] Department of Homeland Security, 6.

[116] Department of Homeland Security, 6.

[117] Department of Homeland Security, 6.

[118] Center for Development of Security Excellence, *Marking Classified Information*, 31.

[119] Department of Homeland Security, *Reference Booklet*, 26.

Enforcement Sensitive (LES), Personally Identifiable Information (PII), and Sensitive Security Information (SSI).[120] Ultimately, fire service agencies and personnel must know how to handle and store CUI information to protect it from unauthorized disclosure.

a. FOUO: For Official Use Only

FOUO is a dissemination control marking, but not a classification.[121] As such, agencies may share FOUO information with other governmental agencies and, to some extent, the private sector.[122] Additionally, FOUO information must have markings to inform the end-user of its sensitive nature and appropriate handling requirements.[123] The marking identifies information that users cannot release to the public without the permission of the originating agency.[124] Additionally, the markers may reference the originating agency, an expiration date, and instructions on how to downgrade the information.[125] Finally, the IC restricts FOUO information to persons with a documented need to know, and the information must be necessary to perform official duties.[126] The restrictions differ from CNSI information, which requires that the requestor have a security clearance at or above the classification level.

b. LES: Law Enforcement Sensitive

At times, fire service agencies may have access to LES information, which may originate from law enforcement agencies at any level of government. Accordingly, the information may contain sensitive information about ongoing investigations or reveal sources and methods, among other operational law enforcement information.[127] A majority of LES documents are available on the HSIN, and vetted fire service members have access

---

[120] Joint Counterterrorism Assessment Team, *Intelligence Guide*, 2.

[121] Joint Counterterrorism Assessment Team, 2.

[122] Department of Homeland Security, *Reference Booklet*, 26.

[123] Department of Homeland Security, 26.

[124] Joint Counterterrorism Assessment Team, *Intelligence Guide*, 2.

[125] Department of Homeland Security, *Reference Booklet*, 26.

[126] Joint Counterterrorism Assessment Team, *Intelligence Guide*, 2.

[127] Joint Counterterrorism Assessment Team, 2.

to the products. Therefore, persons accessing LES information may not disseminate it without permission from the originating agency.[128] In the end, fire service agencies must ensure they follow LES handling requirements to maintain trust and access to intelligence developed by law enforcement agencies.

c. PII: Personally Identifiable Information

Fire service agencies have access to PII as part of their reporting processes through the National Fire Incident Reporting System or health records they generate on emergency medical runs. PII is any information that alone may reveal a person's identity or when used with other personal information may identify an individual.[129] To protect the identity of an individual, PII requires a risk assessment on an individual basis.[130] The Health Insurance Portability and Accountability Act and the Health Information Technology for Economic and Clinical Health Act spell out most PII requirements for fire departments that access such information. Thus, fire service agencies are already aware of such handling requirements and protections.

d. SSI: Sensitive Security Information

As part of their coordination with transit agencies and other critical infrastructure, fire service agencies may gain access to SSI. Federal law governs SSI as it contains sensitive but unclassified information that may be harmful to transportation security.[131] As such, the federal government may impose enforcement actions or civil penalties on agencies who disclose such information without authorization.[132] SSI is subject to the handling requirements outlined in 49 C.F.R. § 1520.[133] The regulation states, "No part of this record may be disclosed to persons without a 'need to know,' as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the

[128] Joint Counterterrorism Assessment Team, 2.

[129] Joint Counterterrorism Assessment Team, 3.

[130] Joint Counterterrorism Assessment Team, 3.

[131] Joint Counterterrorism Assessment Team, 3.

[132] Joint Counterterrorism Assessment Team, 3.

[133] Joint Counterterrorism Assessment Team, 3.

Transportation Security Administration or the Secretary of Transportation."[134] Accordingly, fire service agencies must protect SSI, or they may face severe government sanctions.

B. INTELLIGENCE COMMUNITY

In the United States, the IC is a loose federation of 17 agencies. Each of the agencies has a separate mission for gathering national intelligence, which includes domestic, foreign, and homeland security intelligence.[135] According to Lowenthal, "The community is made up of agencies and offices whose work is often related and sometimes combined, but they serve different needs or different policy makers."[136] Consequently, management and execution represent the two functional areas of the IC.[137] The management aspect refers to establishing requirements, gathering resources, establishing a collection plan, and determining production products.[138] Alternatively, execution refers to developing systems for collection, collecting and producing intelligence, and maintaining intelligence infrastructure.[139] Ultimately, the fire service needs to understand the makeup of the IC, so it is better informed regarding how the IC produces and disseminates intelligence. For a depiction of the IC, see Figure 7.

---

[134] Protection of Sensitive Security Information, 49 C.F.R. § 1520.13 (2004), https://www.law.cornell.edu/cfr/text/49/1520.13.

[135] Lowenthal, *Intelligence*, 40.

[136] Lowenthal, 13.

[137] Lowenthal, 44.

[138] Lowenthal, 44.

[139] Lowenthal, 44.

Figure 7. Agencies of the Intelligence Community[140]

Policymakers at all levels of government need intelligence and information to inform their homeland security policy development. According to the ISE annual report, "The U.S. Government's ability to effectively share terrorism-related information and other information related to multiple threat actors, as well as their networks, and then use that information to support a broad array of national security–related missions and activities is essential in protecting the homeland."[141] As such, the Office of the Director of National Intelligence proposes that federal, state, and local partners are essential in meeting homeland security mission objectives.[142] Accordingly, state, local, tribal, and territorial agencies primarily receive information from DHS and the FBI.[143] Additionally, the 2007

[140] Source: "What We Do," Office of the Director of National Intelligence, accessed April 17, 2020, https://www.dni.gov/index.php/what-we-do.

[141] Office of the Director of National Intelligence, *2018 Information Sharing Environment*, 19.

[142] Office of the Director of National Intelligence, *Domestic Approach*, 7.

[143] Office of the Director of National Intelligence, 15.

National Strategy for Information Sharing suggests that sharing information should be the rule, not the exception, and federal, state, local, and tribal governments may use such information for budgeting, developing resilience plans, preventing terrorism, developing training plans, and prioritizing response and recovery efforts.[144] Because terrorism and other disasters are local events, and local agencies are first on the scene and the last personnel to leave, information sharing is paramount.[145] Ultimately, to better inform fire service strategies, operations, and tactics, the fire service needs access to timely and relevant intelligence.

Notwithstanding, the fragmented nature and the redundant mechanisms of the IC emphasize several problems, which have been the subjects of government reports. *The 9/11 Commission Report* pushed for the reorganization of the IC and the development of the ISE to prevent surprise attacks by aligning all IC agencies. The 9/11 Commission offered several recommendations, including unifying strategic intelligence and operational planning under a National Counterterrorism Center, coalescing the IC under a national intelligence director, and developing a network-based information-sharing system.[146] The IC applied these recommendations as activities under the IRTPA of 2004.[147] However, as Amy Zegart points out, the IC remains disjointed despite the IRTPA and the creation of a director of national intelligence.[148] Additionally, the *Domestic Approach* suggests that absent unity of effort, unreliable practices, and the lack of doctrine still typify the domestic intelligence environment.[149] Other challenges include the FBI and DHS counterterrorism mission overlap, large geographic regions, a lack of clear vision, and a focus on sustainment over enhancement.[150] This issue is important because the fire service, along with many other agencies, relies on the IC for its intelligence needs. Therefore,

---

[144] Executive Office of the President, *National Strategy for Information Sharing*, 1.

[145] Office of Homeland Security, *National Strategy for Homeland Security*, 1.

[146] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report*, 399–400.

[147] Intelligence Reform and Terrorism Prevention Act of 2004.

[148] Zegart, *Spying Blind*, 183.

[149] Office of the Director of National Intelligence, *Domestic Approach*, 9.

[150] Offices of the Inspectors General, *Review of Domestic Sharing*, 8–9.

understanding the insular issues arms the fire service with the information it needs to take steps to resolve problems early in the intelligence integration process.

Ultimately, the obstacles faced at federal, state, and local levels produce significant challenges for fire service agencies. First, there is the issue of finding linkages to the overall IC, considering the involvement of numerous agencies. Second, there is the challenge for the fire service in receiving relevant and timely information to inform strategic, operational, and tactical decision-making. Additionally, the documents lack detailed guidance on how fire service agencies may use intelligence to inform decision-making. Finally, the fire service must find ways to counter parochialism to ensure it receives a steady flow of intelligence to protect its communities.

C. FIRE SERVICE INTELLIGENCE ENTERPRISE CONCEPT PLAN

To reduce the challenges associated with establishing fire service intelligence requirements and usage, in 2009, DHS developed the Fire Service Intelligence Enterprise (FSIE)'s *Concept Plan*. The FSIE was one of the earliest efforts undertaken to integrate the fire service into the greater intelligence community, under the assumption that the fire service would provide a value-added capacity in DHS efforts to prevent, protect, respond to, and recover from terrorist activities.[151] To guide the development process, DHS and other partners ensured the activities aligned with relevant federal policies, directives, strategies, and legislation. See Table 1 for a list of relevant policies.

[151] Department of Homeland Security, *Concept Plan*, 4.

Table 1. List of FSIE-Related Directives, Policies, Strategies, and Legislation

Year	Policy, Directive, Strategy, or Law	Organization
2002	Homeland Security Act of 2002	Public Law 107–296
2003	*National Criminal Intelligence Sharing Plan*	Department of Justice
2004	Executive Order 13356: "Strengthening the Sharing of Terrorism Information to Protect Americans"	White House
2004	Intelligence Reform and Terrorism Prevention Act of 2004	Public Law 108–458
2005	*Intelligence-Led Policing: The New Intelligence Architecture*	Bureau of Justice Assistance
2005	Executive Order 13388: "Further Strengthening the Sharing of Terrorism Information to Protect Americans"	White House
2005	Memorandum for the Heads of Executive Departments and Agencies: "Guidelines and Requirements in Support of the Information Sharing Environment"	White House
2006	*Information Sharing Environment Implementation Plan*	Information Sharing Environment
2006	*Fusion Center Guidelines*	Department of Justice; Department of Homeland Security
2007	Implementing the Recommendations of the 9/11 Commission Act of 2007	Public Law 110–53
2007	*National Strategy for Homeland Security*	White House
2007	*National Strategy for Information Sharing*	White House
2008	*DHS Information Sharing Strategy*	Department of Homeland Security
2008	*Vision 2015: A Globally Networked and Integrated Intelligence Enterprise*	Office of the Director of National Intelligence
2008	Executive Order 12333: "United States Intelligence Activities" (as amended)	White House
2008	*Baseline Capabilities for State and Major Urban Area Fusion Centers*	Department of Justice
2008	*DHS Intelligence Enterprise Strategic Plan*	Department of Homeland Security

The FSIE's *Concept Plan* establishes the legal basis for domestic information and intelligence collection and sharing. Additionally, the plan recognizes that the fire service plays an integral role in every homeland security mission. Accordingly, the plan identifies agencies from which the fire service may receive intelligence and mechanisms by which to satisfy fire service intelligence needs. Finally, the most significant outcome of the FSIE initiative is a set of guidelines for integrating the fire service into state and local fusion centers. Integration into fusion centers is vital to the fire service because they enable a two-way flow of intelligence, and fusion centers act as a hub for intelligence that comes from the IC.

Unfortunately, the FSIE *Concept Plan* no longer exists in its original form. Robert Covert has suggested that the FSIE plan dissolved in 2010.[152] However, most of the tenets set out in the FSIE *Concept Plan* have been placed in the "Fire Service Integration for Fusion Centers" appendix, which appears in the next section of this chapter. Additionally, interested individuals have taken on remnants of the program. Currently, DHS maintains a fire service intelligence liaison position that maintains the HSIN's emergency services site, with sub-linkages to fire service intelligence. There are more than 27,000 members of the fire service vetted for site access. Additionally, as Keith Henke details,

> The FSIE is a management initiative between the Department of Homeland Security Office of Intelligence and Analysis (I&A), the Federal Emergency Management Agency (FEMA), and the U.S. Fire Administration, and was created to provide organized Federal support incorporation [for] the Fire Service in gathering, analyzing, and disseminating homeland security related information and intelligence. The goals of the FSIE initiative include supporting fire service collaboration within state and major urban area fusion centers and facilitating the identification and development of information and intelligence sharing requirements, mechanisms, technical assistance, and training for fire service personnel.[153]

[152] Robert M. Covert II, "Evolving the Local Fire Service Intelligence Enterprise in New York State: Implementing a Threat Liaison Officer Program" (master's thesis, Naval Postgraduate School, 2012), 34, http://hdl.handle.net/10945/27813.

[153] Keith Henke, "Fire Service Intel and Info Resources" (presentation, Department of Homeland Security, November 2019).

The observation that there is still a great deal of interest in the fire service intelligence process—given that there are 27,000 members—is important because it shows how the fire service views intelligence as an integral part of its planning and operations.

D. FIRE SERVICE INTEGRATION FOR FUSION CENTERS

In 2010, the Department of Justice (DOJ) issued a guide titled "Fire Service Integration for Fusion Centers" as an appendix to *Baseline Capabilities for State and Major Urban Area Fusion Centers*. The guide recognizes the fire service as a valuable partner in the overall intelligence enterprise. Accordingly, the DOJ states, "The integration of fire service organizations and personnel into the fusion process enhances the efforts of all homeland security partners across all mission areas."[154] The guide further acknowledges that the fire service may serve as a consumer, collaborator, or contributor vis-à-vis fusion centers.[155] The guide is important to the fire service because it highlights various ways it may integrate into the IC through fusion centers.

Beyond confirming the value-added benefits of integrating fire services, the guide highlights the critical elements necessary to inform fire service intelligence usage. More specifically, the guide aids the fire service in developing intelligence requirements, reporting suspicious activity, conducting risk assessments, outlining procedures to receive alerts and warnings, and maintaining situational awareness.[156] Additionally, the guide helps fire service agencies develop feedback mechanisms to ensure received intelligence is of value.

E. INTELLIGENCE GUIDE FOR FIRE CHIEFS

Sensing the need for fire service intelligence practices, the IAFC provided the necessary leadership. Accordingly, the IAFC developed the *Intelligence Guide for Fire Chiefs* to serve as a reference for collaboration with DHS.[157] The IAFC developed the guide

---

[154] Department of Justice, "Fire Service Integration," 2.

[155] Department of Justice, 3.

[156] Department of Justice, 5–6.

[157] International Association of Fire Chiefs, *Intelligence Guide for Fire Chiefs*.

because fire service agencies have struggled to obtain relevant intelligence information. The intelligence guide highlights various resources available to the fire service for its intelligence needs. More specifically, the guide suggests developing partnerships with fusion centers, JTTFs, and local law enforcement agencies.[158] Additionally, the guide recommends engaging in information-sharing portals such as the HSIN, Law Enforcement Online, Technical Resources for Incident Prevention (TRIPwire), and the National Terrorism Advisory System.[159] The guide has important implications for the broader domain of information sharing as the fire service has realized it must lead the effort for improved information-sharing practices.

Subsequently, the IAFC realized that the fire service has unique capabilities that are beneficial to the IC. To add value to the IC, the guide recommends involvement in reporting activities. For such reporting, the guide suggests submitting suspicious activity reports (SARs), involving line-level personnel in the Nationwide SAR Initiative, and promoting the "If You See Something, Say Something" campaign.[160] Furthermore, the guide advises identifying personnel to apply for security clearances to gain access to more privileged intelligence information.[161] Finally, the guide proposes developing a dissemination process to distribute intelligence to other members of the agency. The report recommends developing an intelligence liaison officer program with state and local fusion centers to accomplish dissemination goals.[162] Ultimately, the IAFC has recognized that the fire service might serve as a contributor and collaborator—instead of relegating itself to consumer.

F. INTELLIGENCE GUIDE FOR FIRST RESPONDERS

Local responders working on the Joint Counterterrorism Assessment Team (JCAT) at the National Counterterrorism Center acknowledged a need for more comprehensive

[158] International Association of Fire Chiefs, 7–10.

[159] International Association of Fire Chiefs, 11–15.

[160] International Association of Fire Chiefs, 17–20.

[161] International Association of Fire Chiefs, 20–23.

[162] International Association of Fire Chiefs, 23–24.

information sharing among response personnel. The JCAT developed the *Intelligence Guide for First Responders* to increase information sharing among all levels of government.[163] The guide provides a high-level overview of how to gain access to information, understand estimative language, and report suspicious activity, among other things.[164] The addition of the guide gave first responders insight into intelligence processes and the intelligence community.

1. Gaining Access to Sensitive Information

Agencies performing homeland security or law enforcement–related duties may access unclassified information through several online portals.[165] The portals include previously mentioned sites such as the HSIN, Law Enforcement Online, and TRIPwire. Likewise, agencies may access information through the National Situation Awareness Room (SitAware), Intelink-U, the Law Enforcement Enterprise Portal, and the Regional Information Sharing Systems Network, all of which have different vetting practices.[166]

2. Estimative Language

The IC uses estimative language to judge the likelihood or probability of an event.[167] Typically, there are three degrees of likelihood: high confidence, moderate confidence, and low confidence. High confidence is a solid judgment based on high-quality information.[168] Alternatively, moderate confidence indicates the information is not corroborated but credible.[169] Finally, low confidence indicates that there may be concerns with the sources, making it difficult to arrive at firm conclusions.[170] The high, moderate, and low confidence judgments identify the scope and quality of the intelligence

---

[163] Joint Counterterrorism Assessment Team, *Intelligence Guide*, v.

[164] Joint Counterterrorism Assessment Team, 2–15.

[165] Joint Counterterrorism Assessment Team, 6.

[166] Joint Counterterrorism Assessment Team, 7–8.

[167] Joint Counterterrorism Assessment Team, 12.

[168] Joint Counterterrorism Assessment Team, 12.

[169] Joint Counterterrorism Assessment Team, 12.

[170] Joint Counterterrorism Assessment Team, 12.

provided.[171] Understanding estimative language is essential for the fire service because it helps personnel grasp the likelihood of an incident occurring.

3. Suspicious Activity Reporting

During the ordinary course of business, firefighters can identify suspicious behaviors in their communities. In some instances, reported suspicious activities have led to arrests, corroborated intelligence, or disrupted terrorist attacks.[172] Consequently, firefighters should engage in SAR activities. To enable firefighters to submit SARs, DHS and the FBI developed the Nationwide Suspicious Activity Reporting Initiative.[173] This program promotes reporting observations for vetting and sharing of information. Additionally, the program offers online training to highlight the SAR process and ensure that firefighters protect the civil liberties of ordinary citizens. The JCAT guide offers 10 ways for firefighters to incorporate SARs into agency operations.

G. CONCLUSION

After the events of 9/11, DHS and the FBI created several guidance documents that govern domestic intelligence processes and programs. Although the current policies identify mechanisms for the fire service to consume, collect, and collaborate in intelligence processes, they all have fallen short. First, the processes fail to establish the requirements necessary for intelligence agencies to understand fire service intelligence needs. Second, the processes do not elaborate on how a fire chief or fire service agency may use intelligence to inform strategic, operational, and tactical decision-making. Ultimately, a gap persists between policy and practice regarding fire service access and the use of intelligence products.

To ensure the fire service has access to the intelligence it needs, fire service agencies and leaders have developed policies and practices aimed at collecting, analyzing, and disseminating intelligence to support their decision-making. Unfortunately, most in the

---

[171] Joint Counterterrorism Assessment Team, 12.

[172] Joint Counterterrorism Assessment Team, 14.

[173] Joint Counterterrorism Assessment Team, 14.

fire service do not recognize or benefit from the use of the publications. The next chapter analyzes the intelligence products for three different fire service agencies. The purpose of the analysis is to gain insight into best practices in separate fire service intelligence programs.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CASE STUDIES OF EFFECTIVE FIRE INTELLIGENCE USE, POLICIES, AND PRACTICES

After the initial FSIE program, several fire departments developed their own intelligence programs. These include the Chicago Fire Department's Tactical Operations Intelligence Center, the FDNY, and the National Capital Region Threat Intelligence Consortium, staffed by the District of Columbia Fire and Emergency Medical Services Department (DCFEMS) and other local agencies. This chapter uses case studies to evaluate the specific fire service intelligence products the agencies produce. The case studies evaluate how well agency product lines meet the criteria for intelligence at the strategic, operational, and tactical levels.

For additional analysis, this chapter uses Lowenthal's framework for identifying good intelligence. The framework analyzes intelligence products on whether they are timely, tailored, digestible, and clear regarding knowns and unknowns.[174] As Lowenthal suggests, "Getting the intelligence to the policymaker on time is more important than waiting for every last shred of collection."[175] Under the tailored criterion, Lowenthal recognizes the importance of focusing on specific needs while remaining objective.[176] The digestible aspect advises that the length must allow for a decision-maker to identify the most important aspects of the intelligence quickly.[177] Finally, clear intelligence identifies a degree of confidence regarding knowns and unknowns, and what insight comes from the analysis.[178] Ultimately, understanding finished intelligence products and what constitutes good intelligence may inform other fire service agencies in how to develop and consume intelligence products to serve their planning and decision-making needs.

---

[174] Lowenthal, *Intelligence*, 214–15.

[175] Lowenthal, 214.

[176] Lowenthal, 214.

[177] Lowenthal, 214.

[178] Lowenthal, 215.

A. CHICAGO FIRE DEPARTMENT TOIC

1. Structure

Recognizing a need to provide critical information to response personnel, the Chicago Fire Department established the Tactical Operations Intelligence Center (TOIC) in 2006.[179] TOIC develops a bulletin to support internal departmental briefings on significant local, national, and international events.[180] TOIC publishes the bulletin weekly as a sensitive but unclassified document for internal use only, and it averages 12 pages in length. Also, the bulletin aggregates information from various fusion center and DHS publications. Furthermore, TOIC structures the bulletins into four sections, which include significant incidents, national and international intelligence, special events, and significant dates.[181] Moreover, TOIC supports the information with photos and attributes the sources with uniform resource locators. Finally, the Chicago Fire Department coordinates intelligence production and dissemination with the Chicago Police Department's Crime Prevention and Information Center (CPIC).[182] Its collaboration with CPIC gives Chicago Fire access to the Chicago Police Department's district intelligence bulletins (DIBs), bus and rail update reports, intelligence notes, and suspicious activity report intelligence analysis. The most useful product for the fire service is the DIBs, intranet-based products available from onboard computers that identify problem areas within response districts.[183] Additionally, the system provides real-time intelligence products that are customizable for each district.[184]

---

[179] Department of Homeland Security and Department of Justice, "Fire Service Information Sharing Workshop: Fusion Center Resource" (Washington, DC: National Criminal Intelligence Resource Center, September 2010), 1.

[180] Department of Homeland Security and Department of Justice, 1.

[181] Department of Homeland Security and Department of Justice, 1.

[182] Department of Homeland Security and Department of Justice, 2.

[183] Department of Homeland Security and Department of Justice, "Case Study: Crime Prevention and Information Center" (Washington, DC: National Criminal Intelligence Resource Center, November 2007), 6.

[184] Department of Homeland Security and Department of Justice, "Fire Service Information Sharing Workshop," 2.

2. Strategic-Level Intelligence

For the strategic level, TOIC's bulletin offers articles from national and international sources. A brief analysis of five TOIC bulletins reveals several strategic-level considerations. At the national level, the bulletin covers a broad spectrum of potential homeland security issues, such as vaccinations, new diseases, inclement weather conditions, violence against first responders, and U.S. travel advisories for foreign countries. The articles are all open-source summaries, and TOIC does not offer a perspective on the strategic implications for fire service agencies. At the international level, the bulletin details wide-ranging international security issues that might eventually have a domestic nexus. The international topics include information on terrorist tactics, such as the use of explosives. Additionally, the bulletin details information on critical infrastructure problems abroad and documents the movements and rhetoric of foreign terrorist organizations. Moreover, the articles discuss natural disasters in foreign countries.

Although the articles touch on broad homeland security topics, a user would need some analytical skills to determine potential long-term impacts for the department. Consequently, fire departments that use such information must train other personnel to analyze the articles to make the information more relevant because TOIC does not provide the necessary analysis and assessment. Furthermore, the information appears to be little more than the news civilians read or aggregate online. TOIC's bulletin is not very helpful for strategic planning and preparation as it fails to offer analysis on the subjects of the articles.

3. Operational-Level Intelligence

The information in TOIC's bulletins offers several opportunities to support operational intelligence activities. Unfortunately, TOIC does not provide analysis of the articles in the bulletins, which is a necessary component for an intelligence product. Therefore, a user of the intelligence product must read the articles intently to identify specific issues that might affect the organization. Nevertheless, a brief analysis of five such bulletins highlights several operational-level considerations. First, the bulletin routinely offers information regarding attacks on first responders. Understanding the tactics,

techniques, and procedures used by attackers allows for first response agencies to make operational adjustments to counter the issues. Second, TOIC's bulletin highlights incidents where adversaries have used fire as a weapon, which may challenge standard response models and on-scene operations. Additionally, the bulletin offers information on attacks where terrorists have used improvised explosive devices. Finally, the bulletin aggregates stories concerning terrorist ideology, terrorism funding, actual targets of terrorist attacks, public health issues, and homegrown violent extremism. The information in the articles, however, fails to rise to the level of intelligence without additional exploitation and processing. TOIC provides no analytical input, leaving the information up to broad interpretation.

4. Tactical-Level Intelligence

The tactical-level information in TOIC's bulletin highlights upcoming special events and necessary situational awareness. The product employs sub-labels, such as assembly, rally, parade, or protest, and details the dates, times, locations, and descriptions of the actual events. Unfortunately, the information does not provide additional tactical-level insight, such as the number of participants, or any known information regarding protest groups. However, the information is valuable for situational awareness of companies that may respond to the area. Because TOIC does not perform analysis, the information lacks substance and does not provide any tactical-level decision-making advantage. The information on special events and situational awareness, absent analysis, is not intelligence and has limited utility for informing tactics.

However, DIBs may be of great value at the tactical level because they provide real-time intelligence directly to personnel operating in the field. CPIC permitted the Chicago Fire Department's access to DIBs after a shooting incident involving a firefighter.[185] DIBs provide alerts regarding numerous problems, including gang activity, illicit drug sales, shots fired in an area, a most-wanted list, and other intelligence as it becomes available.[186] Ultimately, access to DIBs provides Chicago fire personnel with

[185] Department of Homeland Security and Department of Justice, 2.

[186] Department of Homeland Security and Department of Justice, "Case Study," 6.

real-time information within their response areas, improving personnel safety and situational awareness.[187]

5. Analytical Value

TOIC's bulletin is a compilation of news stories that may have a nexus to terrorism or the fire service in general. The news stories provide only general information that does not rise to the level of intelligence. Additionally, TOIC does not perform analysis on the implications of the information in the articles to inform strategic, operational, and tactical decision-making and planning. The lack of analysis leaves the information open to broad, independent interpretations, which may pose challenges for response personnel when developing plans. The lack of analysis severely limits the utility of TOIC's bulletin, regardless of the subject of the articles.

6. Lowenthal's Intelligence Framework

In using Lowenthal's framework, the two primary products offer differing intelligence value. TOIC develops the bulletin weekly, which is timely for strategic and operational levels, but less timely for tactical decision-making. However, TOIC tailors the bulletin for internal distribution, so it meets the second criteria under Lowenthal's frame. On the other hand, TOIC's bulletin is not digestible because the length is generally 12 pages. Finally, the product is unclear regarding knowns and unknowns because the authors do not provide independent analysis.

Alternatively, CPIC's DIBs are real-time products, with personnel having access to the information through onboard computers. The real-time aspect and ease of access allow DIBs to meet the timely metric under Lowenthal's framework. Although the product is timely, CPIC writes the information for district law enforcement personnel, which lacks tailoring for the fire service. However, the information in the DIBs is digestible, as it encompasses no more than two pages. Finally, DIBs are clear regarding knowns but may lack the clarity necessary to provide information on unknowns.

---

[187] Department of Homeland Security and Department of Justice, "Fire Service Information Sharing Workshop," 2.

B. FDNY INTELLIGENCE

1. Structure

The FDNY produces three intelligence publications to support its strategic, operational, and tactical decision-making. The publications are *Watchline*, *Fireguard*, and the FDNY's Monograph Series. *Watchline* is a weekly intelligence product that was born in the early days of homeland security intelligence processes because law enforcement and the intelligence community did not believe the fire service had a place in the intelligence discipline. The FDNY still manages its intelligence process despite the move to more fire service integration into the intelligence community.

The structure of *Watchline* has several significant characteristics that make it highly readable while maintaining its importance to fire service personnel. First, the FDNY's Center for Terrorism and Disaster Preparedness (CTDP) keeps the periodical to one page, so a user may browse through and glean all the critical information in a few minutes.[188] Keeping the information brief is essential, especially at the operational and tactical levels. Second, the publication is easy to read, with the first sentence of each story capturing the essence of the issue at hand.[189] Additionally, it provides analysis for each story, so the reader gains an understanding of how the issue may affect operations.[190] Also, the information is timely, reliable, and relevant to emergency services as the product has readership outside the fire service.[191] The current readership extends to over 150 agencies in the United States and 20 countries abroad, equating to over 100,000 consumers.[192] *Watchline* has influenced several other fire service intelligence products, with most providing some form of analysis to add relevancy to the selected news stories. Notably, the CTDP develops *Watchline* using the intelligence cycle, including intelligence requirements, collection, processing, analysis, and dissemination. Finally, *Watchline*

---

[188] New York City Fire Department, Center for Terrorism and Disaster Preparedness, "*Watchline*: FDNY's Flagship Intelligence Product" (presentation, New York City Fire Department, February 8, 2018), 3.

[189] New York City Fire Department, 3.

[190] New York City Fire Department, 4.

[191] New York City Fire Department, 1.

[192] New York City Fire Department, 6.

touches on several homeland security issues, including terrorism-related tactics, techniques and procedures, historical events, first responder–specific concerns, and advances in science.[193]

The FDNY's *Fireguard* is a PowerPoint presentation series that provides an expansive overview of a particular topic.[194] The CTDP creates *Fireguard* for internal dissemination to field-level units, but the reports are relevant for broader audiences such as law enforcement and public health entities.[195] Since it's the presentation's inception, the CTDP has expanded the offerings of *Fireguard* to include information that is relevant to a broader audience than the fire service.[196] An examination of two *Fireguard* products reveals that the structure includes background information on the issue; the availability of the product; the number of attacks; case studies of relevant incidents, including motivations for such attacks; and response considerations. The product provides a great deal of information on specific tactics, which may inform strategic, operational, and tactical decision-making.

The Monograph Series is another extension of the intelligence products offered by the FDNY's CDTP. As a monograph studies a topic in great detail, the purpose of this intelligence product is solely to provide updates on emergent or critical events to the first responder community.[197] However, the design and tone of the Monograph Series may allow for broader distribution beyond department members. While the product lacks the strict standard of writing seen in *Watchline* in favor of paraphrasing topics and does not adhere to a designated length, the CTDP uses it to push out the latest information on a subject.[198] Although the product is new, it provides significant information regarding the

---

[193] New York City Fire Department, 12–14.

[194] Joseph W. Pfeifer et al., *FDNY Counterterrorism and Risk Management Strategy*, ed. Janet Kimmerly (New York: New York City Fire Department, 2011), 10, https://www1.nyc.gov/assets/fdny/downloads/pdf/FDNY_ct_strategy_2011_12.pdf.

[195] Pfeifer et al., 10.

[196] Pfeifer et al., 10.

[197] New York City Fire Department, "FDNY's Flagship Intelligence Product," 1.

[198] New York City Fire Department, 1.

subject area, and the information may find utility at the strategic, operational, and tactical levels.

2. Strategic-Level Intelligence

At the strategic level, all three FDNY intelligence products offer tremendous utility. First, *Watchline* identifies terrorist tactics, techniques, and procedures that may eventually make their way to the United States. An analysis of several *Watchline* products reveals information on numerous foreign and domestic attack trends. Alternatively, the FDNY's *Fireguard* offers information on both the domestic and international fronts. Domestically, *Fireguard* highlights issues that may pose a danger to first responders or the community. Internationally, *Fireguard* details information on international incidents that may have national relevance. Finally, the Monograph Series provides a detailed study of specific topics. As the publication is new, it has covered only a few incidents. However, the content offers an extensive look at the pandemic and its implications. The three products offer executive-level personnel remarkable insight into various trends, tactics, techniques, and procedures. The insight may inform policy formulation, planning for equipment and supply acquisitions, and development of procedures to counter such issues.

3. Operational-Level Intelligence

At the operational level, *Watchline* and *Fireguard* offer the most value for mid-level management. Regarding *Watchline* the assessment section of each article lends insight to inform operational decision-making. For instance, the assessment may detail necessary training, communication plans, standard operating guidelines, pre-incident planning, personnel safety, and operational coordination. Alternatively, *Fireguard* offers much more in-depth information on specific threats. Accordingly, the products describe the specific issue in great detail while following up with implications for operational decision-making to ensure effective outcomes. Additionally, *Fireguard* highlights case studies of similar occurrences domestically and internationally. The high level of detail in *Fireguard* allows operational commanders to weigh several considerations before deciding on a particular action plan.

4. Tactical-Level Intelligence

At the tactical level, *Watchline* and *Fireguard* hold the most promise. The assessment section of *Watchline* identifies numerous tactical considerations related to the article. According to Brian Heirston, "*Watchline* is unique from a fire service perspective because the recommendations are tactically oriented, directed to the frontline firefighter, concise, and practical."[199] On the other hand, *Fireguard* offers more detailed response considerations to guide tactical decision-making. *Watchline* and *Fireguard* support on-scene tactical decision-making by company commanders and other field response personnel. However, *Fireguard* offers more comprehensive information for informed decisions.

5. Analytical Value

Regarding analytical value, *Watchline* and *Fireguard* offer considerable insight. The assessment section of *Watchline* succinctly describes the critical issues involved in the article. The section is usually no more than three sentences and contains crucial considerations for strategic, operational, and tactical decisions. Alternatively, *Fireguard* offers more detailed information, but the authors scatter the information throughout the presentation. Although *Fireguard* is more informative, it is less practical than *Watchline.* The Monograph Series, in contrast, offers no analysis and leaves the sense-making up to individual readers. Overall, *Watchline* and *Fireguard* are excellent sources of analytical sense-making for personnel at all levels of the organization.

6. Lowenthal's Intelligence Framework

In using Lowenthal's framework, the three primary products for the FDNY offer different values of intelligence. The FDNY develops the *Watchline* bulletin weekly, which is timely for strategic and operational levels, but much less timely for tactical decision-making. However, the FDNY tailors the bulletin for internal distribution and limits the document to a single page. Therefore, *Watchline* meets Lowenthal's criteria for tailoring

[199] Heirston, "Terrorism Prevention and Firefighters," 49.

and digestibility. Additionally, *Watchline* meets Lowenthal's concept of clarity as the FDNY provides an analysis of knowns and unknowns at the end of each story.

Alternatively, the FDNY creates *Fireguard* and the monographs on an as-needed basis. The nature of these products may hold strategic and operational intelligence value, as they provide information in greater detail. However, they are less timely for the tactical level, and the information they provide typically comes from past encounters and incidents. The FDNY's *Fireguard* and Monograph Series meet Lowenthal's tailored criterion because the FDNY creates the publications for internal dissemination. Although the products meet the tailored requirement, they lack digestibility because of their length and added detail. Finally, the two publications meet the clarity concept as they both provide comprehensive information on particular subjects.

C. NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM

1. Structure

The National Capital Region Threat Intelligence Consortium (NTIC), formerly the Washington Regional Threat and Analysis Center, is the region's civilian-led fusion center, based in the District of Columbia's Homeland Security and Emergency Management Agency.[200] Created in 2019, NTIC supports situational awareness and decision-making by producing analytical intelligence products that serve several disciplines.[201] Additionally, NTIC sub-divides its missions into four fields: the public, executive leadership, critical infrastructure partners, and first responders.[202] The list of products include the following:

- Impact assessments
- Threat assessments

[200] District of Columbia Homeland Security and Emergency Management Agency and National Capital Region Threat Intelligence Consortium, *Emerging Incident Playbook* (Shawnee, KS: Guest Communications Corporation, 2019), 5.

[201] District of Columbia Homeland Security and Emergency Management Agency and National Capital Region Threat Intelligence Consortium, 5.

[202] District of Columbia Homeland Security and Emergency Management Agency and National Capital Region Threat Intelligence Consortium, 5.

- Intelligence bulletins
- Intelligence assessments
- Cyber advisories
- Officer safety bulletins
- First responder awareness bulletins

Notably, while the Washington Regional Threat Analysis Center previously authored a publication called *Fire Watch*, similar information now appears in first responder awareness bulletins. Moreover, all of the publications listed are available to the fire service.

2. Strategic-Level Intelligence

At the strategic level, the vast array of NTIC's products makes them suitable for executive-level decision-makers. In 2020, NTIC developed a comprehensive threat assessment that covers a wide spectrum of threats to the homeland. The document identifies numerous threats and hazards as well as highlights the risk attributes thereof. Additionally, the document qualifies the threats based on a risk scale of high, medium, or low and offers critical judgments to guide strategic-level thinking and policymaking. Finally, NTIC has created a standing information-needs product, which highlights various topics that executive personnel may require for planning purposes. Having such information allows policymakers to analyze the inspirational materials to identify other potential risks or request additional intelligence to make better judgments. Ultimately, NTIC's product line has a tremendous amount of information to guide strategic thought at the highest levels of the agency.

3. Operational-Level Intelligence

Intelligence products developed by NTIC offer insight for middle managers and their operational outlook. An example of this is manifest in the intelligence assessment products, which offer perspectives regarding the issue at hand and further delineate an outlook based on what operational decision-makers may expect. Alternatively, NTIC's intelligence bulletins highlight emerging issues in homeland security with actions that operational personnel may take to mitigate such threats. Additionally, the intelligence

bulletin identifies recent incidents associated with the issue to give decision-makers a better perspective. Finally, NTIC's impact assessments detail findings involving specific events in the National Capital Region and identify key findings, previously known incidents surrounding similar events, and an operational outlook with several indicators to guide supervisory and management personnel in managing such events. Overall, NTIC intelligence products are a noteworthy source for operational-level intelligence.

4. Tactical-Level Intelligence

At the tactical level, NTIC produces various advisories and safety bulletins for response-level personnel. For instance, NTIC produces situational awareness bulletins on trending topics in homeland security, as they may eventually make their way into the jurisdiction. NTIC analyzes DHS reports to identify developing threats and potential targets for such dangers. Additionally, NTIC creates officer safety bulletins to warn law enforcement officers of the tactics, techniques, and procedures used by adversaries to harm uniformed personnel. Furthermore, the tactical-level reports identify intelligence gaps where line personnel may assist with gathering field-level intelligence. Moreover, NTIC offers a product called a sunrise brief, which details tactical-level information to guide day-to-day decisions. Finally, NTIC offers cyber advisories to inform personnel on how to protect their privacy and information systems from cyber-attackers. Generally, NTIC products offer a good level of detail to inform the decision-making of tactical, line-level supervisors and managers.

5. Analytical Value

Intelligence products from NTIC offer an abundance of analytical value at multiple levels. First, there are key findings and judgments, which highlight important aspects of homeland security issues along with the associated risk level. Second, the products identify intelligence gaps, so policymakers understand that the provided intelligence remains incomplete for the most accurate policy determinations. Also, some intelligence products give issues context and an outlook on how they may affect operations. Moreover, some products detail specific safety concerns, access and egress points, and incident command structure and coordination. Furthermore, many of the bulletins contain direct comments

from analysts who provide more detailed analysis to improve sense-making for practitioners. Finally, NTIC develops security and preparedness packets on emerging threats and trends for issues such as school safety, campus safety, and human trafficking. The preparedness packets offer a broader view of a topic, as well as detailed steps an organization may take to mitigate, respond to, and recover from such instances. Despite the numerous publications, NTIC products offer a wealth of analysis, which serves to inform operational and policy decisions.

6. Lowenthal's Intelligence Framework

The products available to DCFEMS through NTIC meet Lowenthal's framework with varying degrees. The impact, threat, and intelligence assessments are timely at the strategic level. Likewise, the cyber advisories are timely at the operational level. Also, the intelligence bulletins, officer safety bulletins, and first responder safety bulletins are timely at the tactical level. The only fire service–tailored product offered by NTIC is the first responder awareness bulletin, with the rest of the product line being general or law enforcement in nature. The tactical-level bulletins are all digestible, with many limited to one or two pages. Finally, the entire product line provides clarity on knowns and unknowns, as NTIC provides a high level of analysis.

D. CONCLUSION

The Chicago Fire Department, the New York City Fire Department, and the District of Columbia Fire and Emergency Medical Services Department were three of the earliest proponents of the fire service's integration and engagement in the intelligence enterprise. Accordingly, the three case studies offer insight into the value that fire service agencies bring to the intelligence community generally and state and local intelligence efforts more specifically. Although their intelligence practices began internally, their proficiency and dedication have led to partnerships with fusion centers, law enforcement, DHS, and a host of other intelligence agencies. The intelligence products circulated by the three departments are unique and serve a larger audience than the fire service.

Structurally, the FDNY's CDTP remains an anomaly by maintaining a separate intelligence function within the department. Conversely, Chicago Fire and DCFEMS both

integrate, to some extent, with local fusion centers. The Chicago Fire Department's TOIC integrates and coordinates with the Chicago Police Department's Crime Prevention and Information Center while DCFEMS integrates and collaborates with the National Capital Region Threat Intelligence Consortium. The differing levels of integration show that fire service intelligence processes can work in different configurations. Strategically, operationally, and tactically, all three organizations produce quality intelligence products. Still, the lack of analytical input by TOIC makes it a less valuable source than the FDNY or DCFEMS. Analytically, the intelligence products developed by the FDNY and DCFEMS through NTIC are of high quality, depending on the particular intelligence product.

The case studies offered in this chapter bring to light several significant outcomes for consideration. First, despite the lack of trust in fire service intelligence capabilities after 9/11, several agencies have shown the value of including the fire service in intelligence processes. Second, fire service agencies have proven they are capable of developing intelligence products to inform strategic, operational, and tactical decision-making. Also, the fire service continues to improve its intelligence analysis, which may broaden the perspective of intelligence products. Additionally, the case studies demonstrate that fire service integration into the intelligence community is possible and practical. Finally, the varying styles and lengths of fire service intelligence products may serve as templates for other IC agencies in developing products tailored to meet the needs of the fire service.

V. DISCUSSION, CONCLUSIONS, AND RECOMMENDATIONS

Chapter I offered a problem statement, a review of relevant literature, and identified two related research questions. Chapter II discussed gaps in fire service intelligence support, techniques, and procedures by conducting a gap analysis through a survey instrument. Chapter III identified current intelligence processes, including policies and practices specific to the fire service. Chapter IV analyzed available fire service intelligence products to identify best practices in product design. This chapter serves to tie the information from the previous chapters together. It first discusses successful aspects of fire service intelligence processes. Next, it treats aspects requiring change or improvement. Then, it answers the research questions and draws conclusions from the research. Finally, the chapter ends with a list of recommendations to improve fire service intelligence processes to inform strategic, operational, and tactical decision-making.

A. DISCUSSION

This thesis examined the state of current fire service intelligence practices to identify the gaps that limit the use of intelligence for direct strategic, operational, and tactical support. This thesis used a survey instrument that asked current fire service members about intelligence in the fire service to identify strengths and weaknesses in intelligence practices. The survey consisted of three demographic questions, followed by 12 intelligence-specific questions. The results of the survey indicate that some intelligence practices work well while others need considerable work.

1. Demographics

Respondents represented career, volunteer, and combination departments, as well as a state fire academy, a paid on-call agency, and a state forestry agency. Additionally, respondents represented various sized fire departments from every geographic region in the United States. Because this thesis has attempted to identify shortcomings in fire service intelligence practices as a whole, representation from different types, sizes, and geographic regions best supports the development of solutions that a majority of departments can use.

2. Intelligence Practices: Successful Aspects

The survey data reveal that several intelligence practices are going well. First, a significant majority of participants reported receiving intelligence from at least one source, with several receiving intelligence from multiple sources. The most highly recognized sources were state or local fusion centers, police intelligence units, the Homeland Security Information Network, and JTTFs. To a lesser extent, others noted that their agencies use internally created intelligence, arson task forces, TRIPwire, the Bomb and Arson Tracking System, and the Interagency Fire Intelligence Exchange. These findings challenge the work of earlier researchers who suggested that the fire service lacks access to intelligence products because of a lack of security clearances or other reasons.[203] The findings matter because fire service agencies need access to intelligence to inform decision-making at all levels of their organizations.

Second, several participants highlighted successful integration by their agencies with their state or local fusion centers, with some having a fire service representative or terrorism liaison officer assigned as well. Accordingly, some participants stated that their integration is robust, and their agencies receive frequent updates. Although integration remains fragmented, the numbers are promising for further improvements. Pinpointing instances of successful integration challenges the assumption that the fire service does not have a place in the overall intelligence enterprise. Additionally, 88.24 percent of participants found that the intelligence received is of some value, despite survey data that reveal 52 percent of fire agencies perceive that intelligence providers are unaware of fire service intelligence needs. The finding reinforces the importance of the intelligence cycle and that consumers must identify their intelligence requirements. Otherwise, intelligence providers base their assessments on guesses and prior production history.

3. Intelligence Practices: Areas for Improvement

On the other hand, barriers to information sharing persist within fire service agencies and between their law enforcement counterparts. Internally, fire service agencies

[203] Robson, "Burning Need to Know," 2.

tend to withhold information from the rank and file, disseminating it only to high-ranking personnel. Similarly, some suggest that intelligence dissemination occurs on a need-to-know basis, instead of using the need-to-share doctrine. Still, others mention a lack of dissemination of intelligence within their departments. Regarding law enforcement, many survey participants note the lack of trust between the fire service and law enforcement as an important information-sharing barrier. The problem endures despite several guidance documents recognizing the fire service as an equal and fully trusted partner.[204] Additionally, fire service agencies advise that they do not receive the same type of intelligence as law enforcement, suggesting its lower value to decision-makers. Ultimately, the lack of information sharing within fire service agencies and between law enforcement severely limits fire service activities regarding homeland security issues.

An additional weakness is that fire service interaction with fusion centers remains fragmented. Over 34 percent of the participants in the survey reported little to no interaction or integration with their state or local fusion centers. In particular, participants from Washington State and New York acknowledged that the fire service is left out of the information-sharing loop altogether. Still, others stated that their fusion centers deal mainly with criminal issues such as drug trafficking. Moreover, some participants concluded that a lack of interest among fire chiefs and trouble staffing representatives in fusion centers limit sharing. Furthermore, the PESTEL analysis reveals that legal frameworks in some states prohibit information sharing with the fire service. This is despite the high interest of the fire service to engage in intelligence activities and the proliferation of numerous guidance documents by DHS and the DOJ. These findings have important implications for the broader domain of information sharing because fusion centers are the conduit between the intelligence community and state and local first response agencies.

4. Intelligence Practices: Critical Improvement Areas

The most critical issues for information sharing are law enforcement collaboration, intelligence requirements, handling of sensitive information, and finished intelligence. As a result of the study, the fire service overwhelmingly suggests that intelligence and

[204] Executive Office of the President, *National Strategy for Information Sharing*, 3.

operational planning must be a collaborative effort. Numerous participants proposed reserving a seat at the table for fire service agencies to engage in intelligence and information-sharing initiatives. Furthermore, participants suggested tying in intelligence activities with integrated response planning for events that may affect the jurisdiction. Additionally, participants recommended establishing joint information-sharing portals, so law enforcement, fire, and EMS might have a common operating picture when planning for and responding to incidents involving joint operations. Still, others advised that the fire service offers a unique perspective that may be beneficial in developing a clearer threat picture and a better-informed operational plan.

The issue of fire service intelligence requirements has several interrelated concerns. First, fire service agencies have argued that the intelligence they receive lacks relevance, timeliness, and coordination between fire and law enforcement agencies. Second, participants claimed that intelligence agencies are not aware of fire service intelligence needs. These claims are of some concern because they shed light on misperceptions within the fire service regarding intelligence requirements. The fire service must establish and submit its requirements to intelligence agencies for the information to be relevant to the fire service. Additionally, the survey reveals some confusion concerning the intelligence requirements for standing information needs and the strategic, operational, and tactical levels. When responding to four survey questions regarding standing information needs, strategic intelligence, operational intelligence, and tactical intelligence, respondents offered similar answers for each. Given some overlap, agencies should expect some duplication, yet distinctions at each level seem to be confusing to the participants. Despite the confusion, participants identified several intelligence requirements related to the fire service. The following section identifies the specific requirements suggested by the participants.

Another concern is the lack of understanding handling requirements for sensitive information, as many agencies do not have an information security officer position. Several participants highlighted security concerns over the leaking of sensitive information to the general public. One participant pointed out that from practical experience, firefighters lack an understanding of handling requirements and fail to protect sensitive information. Other

participants suggested a need for training on the meanings of control markings and the development of policies for handling sensitive information. Ultimately, improving the understanding and enforcement of handling requirements may improve the level of trust between the fire service and law enforcement agencies.

Regarding the use of finished intelligence, participants identified several shortcomings in the survey. First, participants acknowledged that fire service members need additional training in how to understand, interpret, and act on intelligence. Second, participants suggested that often there is an overabundance of information given that drowns out the more pertinent details. Additionally, participants pointed out a need to practice utilizing intelligence in training scenarios to improve understanding. Furthermore, participants recognized that without knowing how to use intelligence, fire personnel may respond blindly to incidents that have grave consequences. Notably, these findings suggest that not knowing how to use intelligence is just as bad as not receiving any.

B. CONCLUSIONS

This thesis aimed to answer two specific fire service intelligence questions. First, this thesis sought to determine fire service intelligence requirements to provide direct support to inform strategies, operations, and tactics. Second, this thesis used a survey instrument, completed by members of the fire service, to identify standing information needs and strategic-, operational-, and tactical-level intelligence requirements. The results of the survey follow.

1. Standing Information Needs/Requirements

Participants in the survey identified several standing information needs for efficient, effective, and safe operations of the fire service daily. According to the Department of Justice, "SINs [standing information needs] help focus intelligence gathering, analysis, and reporting on those topics or issues of most concern to the entity that defines them."[205] Additionally, the Department of Justice suggests, "SINs are the

[205] Department of Homeland Security, *2013 National Network of Fusion Centers*, 21.

enduring subjects of intelligence or operational interest for an entity or jurisdiction."[206] The following is a compilation of standing information needs highlighted in the survey.

- Specific and credible threats against first responders
- Suspicious activity in a given area
- Sovereign Citizen movements
- Prior law enforcement interaction with bomb-making materials
- Information of issues or events that may alter response routing
- Known cyber activity that may target fire department information systems
- Human smuggling operations within the jurisdiction
- Information on the spread of pandemics and necessary precautions
- Specific, credible threats to businesses and critical infrastructure
- Arson-related activity, trends, and tactics
- Social media references to terrorist or dangerous criminal activity
- Large-scale events within the jurisdiction
- Chemical, biological, radiological, nuclear, and explosive hazards or threats within the jurisdiction
- Theft of fire service equipment, vehicles, and uniforms
- Extremist groups that may be traveling to the area
- Information on known illicit drug laboratories
- Civil unrest, protests, rioting, protest devices, barricaded/blocked streets
- Extreme weather events and other potential natural disasters
- School and active-shooter threats or indicators
- Indicators of pre-attack operational surveillance
- Locations of properties storing hazardous materials
- Gang activity that may pose a threat to first responders

[206] Department of Homeland Security, 21.

2. Strategic Intelligence Requirements

Strategic intelligence looks at long-term issues that may affect how an organization plans for the future. Participants in the survey identified numerous requirements to support strategic planning and decision-making. The following is a compilation of strategic intelligence requirements participants emphasized in the survey.

- Emergent groups that may pose a threat to first responders
- Identification of known and potential targets in the jurisdiction
- Threats or issues that may affect ongoing resource allocations
- Critical infrastructure and key resource threat assessments
- Cyber events such as swatting, doxing, and denial of service attacks that target response agencies
- Emergent threats, along with potential actions to counter the threats and guide strategic planning
- Trends on tactics, techniques, procedures, and the context for which they are in use overseas that may eventually threaten the homeland
- Criminal and terrorist modus operandi that may drive decisions for equipment purchases, training, and long-range planning
- High-level briefings on world political events and how they may affect the homeland
- Evaluation of potential threats versus response capabilities

3. Operational Intelligence Requirements

Operational intelligence looks at the information needed for short- to mid-term issues that may affect agency operations. Fire service agencies utilize operational intelligence to plan operations; monitor events; match capabilities to the threat; provide relevant, timely, and credible assessments; and monitor natural or human-made disasters.[207] Participants in the survey identified numerous requirements to support

[207] Joint Counterterrorism Assessment Team, *Intelligence Guide*, I-22.

operational planning and decision-making. The following is a compilation of operational intelligence requirements participants emphasized in the survey.

- Threats to first responders
- Threats to target hazards, critical infrastructure, and key resources
- Pre-incident information that may guide unified command operations
- Geographic information system mapping and plume data
- Specific risks, threats, and methods
- Intelligence that informs short-term planning objectives, training activities, and equipment purchases
- Current issues that may warrant the alteration of response plans and routes
- Known threats and hazards for pre-planning mitigation and response
- Availability of special resources
- Special event threat assessments
- Information on extremist groups in the jurisdiction, along with their plans

4. Tactical Intelligence Requirements

Tactical intelligence is perishable intelligence that supports current tactical operations and keeps personnel out of danger. Tactical intelligence must be accurate, relevant, timely, and precise, with detailed information on who, what, when, where, and how.[208] Participants in the survey identified numerous requirements to support tactical decision-making. The following is a compilation of tactical intelligence requirements participants emphasized in the survey.

- Information on known, credible threats for incidents to which first responders will respond
- Immediate known threats to personnel safety, such as civil unrest, known chemical agents, and bomb-making materials
- Information on active-shooter or bomb threat incidents

[208] Joint Counterterrorism Assessment Team, I-22.

- Real-time threat-related information, safe response routes, and secured staging areas
- Intelligence based on incident indicators such as plumes, fumes, or odors that may indicate WMD materials
- Cyber threats
- Real-time information on complex-coordinated attacks
- Public health issues and force protection methods
- Impending severe weather and other natural disasters
- Pre-attack indicators, materials involved, actions to take
- Daily intelligence briefs

5. Using Finished Intelligence

Additionally, this thesis sought to determine how the fire service can use intelligence to guide strategic policy development, operational planning, and tactical decision-making. Second, this thesis used a survey instrument, completed by members of the fire service, to identify current fire service uses of intelligence to support daily operations. Furthermore, this thesis compared intelligence products from three agencies that develop fire-based intelligence products. The results of the survey and comparative analysis follow.

a. Strategic Level

At the strategic level, fire service agencies use intelligence for long-term strategic planning. Using the intelligence to inform strategic planning allows for adjustments to staffing models, standards of cover, and standard operating guidelines. Additionally, strategic intelligence drives equipment purchases, so fire agencies can match their capabilities to acknowledged threats. Moreover, strategic intelligence allows fire agencies to develop training plans to ensure personnel receive the training necessary to counter emergent threats. Finally, strategic intelligence aids fire agencies in developing prevention, mitigation, and long-term recovery strategies. Ultimately, strategic intelligence looks at

long-range issues that may affect how an organization plans or operates based on future-oriented events.

b. Operational Level

At the operational level, fire service agencies use intelligence in various ways. First, fire agencies use operational intelligence to develop operational plans for special events and large-scale incidents. Second, agencies use operational intelligence to advise and report on suspicious activities. Additionally, operational intelligence aids in identifying threat-based staffing needs and recalling personnel with specialized knowledge. Finally, agencies use operational intelligence to inform personnel about novel issues, such as new street drugs and their attendant effects or pandemic information for COVID-19 and the associated personal protective equipment requirements. In the end, operational intelligence looks at the information needed for short- to mid-term issues that may affect agency operations.

c. Tactical Level

At the tactical level, fire service agencies use intelligence for force protection activities. Force protection takes several forms, such as providing general situational awareness, changing response routing, or responding to a staging area until dispatchers declare the scene safe for entry. Additionally, tactical intelligence can inform response personnel to remain observant of threatening individuals or groups. Also, the intelligence may prompt response personnel to remain vigilant in identifying anomalies in their response districts for SARs. Furthermore, tactical intelligence may inform of the need to increase station security levels due to a known threat or in times of civil unrest. Finally, tactical intelligence can notify personnel of real-time issues such as addresses with known hazards or threats, or real-time movements of protest groups, so companies can avoid ambushes and identify alternate response routes. Ultimately, tactical intelligence is perishable and supports current tactical deployments to resolve incidents while effectively keeping response personnel out of danger.

C. RECOMMENDATIONS

According to Thomas Robson, "The ability of the fire service to execute its sworn duty to protect life and property in the local community, as well as, to the extent possible, protect the firefighters who serve there from the consequences of terrorism, is dependent on the efficient usage of intelligence."[209] As such, the fire service has intelligence to support mission-critical decisions at all levels of the organizations. More specifically, intelligence aims to inform long-range strategic planning, gain an understanding of threats and their implications for the organization, and protect the lives of personnel operating on the ground. Given the importance of intelligence, this thesis outlines recommendations for the three most critical issues identified in the survey and analysis of professed intelligence problems: intelligence requirements, handling of sensitive information, and more effective law enforcement collaboration in developing intelligence products.

1. Identify and distribute a list of baseline fire service intelligence requirements.

The International Association of Fire Chiefs should identify and distribute a list of baseline fire service intelligence requirements to all fire service organizations for submission to their intelligence producers. Intelligence producers in the intelligence community acknowledge that intelligence consumers have diverse intelligence needs, and the fire service is no different. Accordingly, fire service leaders require personalized, well-timed intelligence that identifies threat-based risks, background and contextual analysis, and warnings to perform their duties and protect their personnel effectively. However, the results of the survey suggest there is confusion in the fire service regarding who sets and communicates the requirements to intelligence producers. In short, fire service leaders and policymakers should identify and establish their own requirements and send them to their intelligence producers. If fire service leaders do not convey requirements to their producers, the producers will set priorities based on their knowledge, and the intelligence may lack relevance to the fire service.

[209] Robson, "Burning Need to Know," 14.

2. Develop a training brief and policy guidance on intelligence handling requirements and operational security.

DHS and the Department of Justice should develop a training brief and policy guidance on intelligence handling requirements and operational security. According to the Defense Security Service, "Marking is the principal way of letting holders of information know the specific protection requirements for that information."[210] Additionally, the agency suggests there are several purposes for understanding intelligence markings and handling requirements. More specifically, intelligence markings alert the holder to potentially sensitive information, indicate how to protect it, and offer guidance on how to safely share it. Accordingly, numerous participants suggested that the handling of sensitive information is an area of concern for the fire service. Many of the participants advised that they were unfamiliar with terms such as For Official Use Only and the associated requirements for safeguarding the information.

Additionally, participants mentioned that fire service agencies tend to share information more broadly as opposed to the closely guarded treatment by law enforcement. Furthermore, participants mentioned that the differences in sharing and safeguarding are a point of contention for improved information sharing between the two disciplines. Therefore, a detailed training plan and policy guidance document are necessary to educate fire service members on intelligence restrictions, and doing so may improve information sharing between fire and their law enforcement counterparts. Also, fire service agencies would benefit from establishing an information security officer, similar to a Health Insurance Portability and Accountability Act compliance officer, to ensure the agency meets intelligence-handling guidelines.

3. Develop a joint intelligence guide for use by fire, law enforcement, EMS, and other first response agencies.

DHS, the Department of Justice, the International Association of Fire Chiefs, and the International Association of Chiefs of Police should develop a joint intelligence guide for use by fire, law enforcement, EMS, and other first response agencies. Many of the

[210] Center for Development of Security Excellence, *Marking Classified Information*, 3.

participants in the survey suggested that there is a need for more collaboration with law enforcement for intelligence processes and planning. As such, a joint intelligence doctrine may prove beneficial. The Department of Defense suggests that accomplishing missions relies on joint intelligence.[211] More specifically, the purpose of joint intelligence is to "inform the commanders; identify, define, and nominate objectives; support the planning and execution of operations; counter adversary deception and surprise; support friendly deception efforts; and assess the effects of operations on the adversary."[212] Additionally, intelligence informs decision-making by highlighting paths of action and allows for prediction and anticipation of future events.[213] Ultimately, the joint intelligence doctrine has proven beneficial to the military, and adoption by fire and law enforcement agencies may be as valuable. this research points to the need for such a guide. Although the guide itself is beyond the scope of this thesis due to CUI restrictions, a proposed outline is provided in Appendix B, and the author intends to develop the guide as a separate project.

In sum, identifying and distributing baseline intelligence requirements to fire service agencies will ensure the timeliness and relevance of intelligence in supporting decision-making at all levels of fire service organizations. Also, training on handling sensitive information and the development of internal security policies may eliminate barriers to information sharing between the fire service and law enforcement. Finally, developing a joint planning doctrine and guide will allow for more effective coordination and collaboration at the local level to ensure the completion of homeland security missions in the most effective and efficient ways possible. As a follow-on to this thesis, I intend to develop a detailed requirements list and draft a joint intelligence guide for dissemination to intelligence agencies for further development and distribution to associated agencies.

---

[211] Joint Chiefs of Staff, *Joint Intelligence*, I-3.

[212] Joint Counterterrorism Assessment Team, *Intelligence Guide*, ix.

[213] Joint Chiefs of Staff, *Joint Intelligence*, ix.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. FIRE SERVICE INTELLIGENCE REQUIREMENTS

The fire service has a wide range of intelligence needs to support strategic, operational, and tactical decision-making. Establishing intelligence requirements is the first step in the intelligence cycle. The fire service must establish and submit its requirements to intelligence agencies for the information to bear relevance. Given that intelligence needs vary based on jurisdiction, this list is not meant to be exhaustive. However, the list sets itself apart from others as it highlights intelligence requirements at four levels: standing information needs, strategic requirements, operational requirements, and tactical requirements. For a more comprehensive list of fire service or homeland security–related intelligence requirements, DHS and the FSIE offer guides on key intelligence questions that may serve the basis for establishing requirements.

A. STANDING INFORMATION NEEDS/REQUIREMENTS

Standing information needs are a key component for efficient, effective, and safe operations of the fire service daily. According to the Department of Justice, "SINs help focus intelligence gathering, analysis, and reporting on those topics or issues of most concern to the entity that defines them."[214] Additionally, the Department of Justice suggests, "SINs are the enduring subjects of intelligence or operational interest for an entity or jurisdiction."[215] The following is a compilation of standing information needs highlighted by fire service members in this thesis.

- Specific and credible threats against first responders
- Suspicious activity in a given area
- Sovereign Citizen movements
- Prior law enforcement interaction with bomb-making materials
- Information of issues or events that may alter response routing
- Known cyber activity that may target fire department information systems

[214] Department of Homeland Security, *2013 National Network of Fusion Centers*, 21.

[215] Department of Homeland Security, 21.

- Human smuggling operations within the jurisdiction
- Information on the spread of pandemics and necessary precautions
- Specific, credible threats to businesses and critical infrastructure
- Arson-related activity, trends, and tactics
- Social media references to terrorist or dangerous criminal activity
- Large-scale events within the jurisdiction
- Chemical, biological, radiological, nuclear, and explosive hazards or threats within the jurisdiction
- Theft of fire service equipment, vehicles, and uniforms
- Extremist groups that may be traveling to the area
- Information on known, illicit drug laboratories
- Civil unrest, protests, rioting, protest devices, barricaded/blocked streets
- Extreme weather events and other potential natural disasters
- School and active-shooter threats or indicators
- Indicators of pre-attack operational surveillance
- Locations of properties storing hazardous materials
- Gang activity that may pose a threat to first responders

B. STRATEGIC INTELLIGENCE REQUIREMENTS

Strategic intelligence looks at long-range issues that may affect how an organization plans for the future. Participants in the survey identified numerous requirements to support strategic planning and decision-making. The following is a compilation of strategic intelligence requirements participants emphasized in the survey.

- Emergent groups that may pose a threat to first responders
- Identification of known and potential targets in the jurisdiction
- Threats or issues that may affect ongoing resource allocations
- Critical infrastructure and key resources threat assessments
- Cyber events such as swatting, doxing, and denial of service attacks that target response agencies

- Emergent threats, along with potential actions to counter the threats and guide strategic planning
- Trends on tactics, techniques, procedures, and the context for which they are in use overseas that may eventually threaten the homeland
- Criminal and terrorist modus operandi that may drive decisions for equipment purchases, training, and long-range planning
- High-level briefings on world political events and how they may affect the homeland
- Evaluation of potential threats versus response capabilities

C. OPERATIONAL INTELLIGENCE REQUIREMENTS

Operational intelligence looks at the information needed for short- to mid-term issues that may affect agency operations. Fire service agencies utilize intelligence to plan operations; monitor events; match capabilities to the threat; provide relevant, timely, and credible assessments; and monitor natural or human-made disasters.[216] Participants in the survey identified numerous requirements to support operational planning and decision-making. The following is a compilation of operational intelligence requirements participants emphasized in the survey.

- Threats to first responders
- Threats to target hazards, critical infrastructure, and key resources
- Pre-incident information that may guide unified command operations
- Geographic information system mapping and plume data
- Specific risks, threats, and methods
- Intelligence that informs short-term planning objectives, training activities, and equipment purchases
- Current issues that may warrant the alteration of response plans and routes
- Known threats and hazards for pre-planning mitigation and response
- Availability of special resources

[216] Joint Counterterrorism Assessment Team, *Intelligence Guide*, I-22.

- Special event threat assessments
- Information on extremist groups in the jurisdiction, along with their plans

D. TACTICAL INTELLIGENCE REQUIREMENTS

Tactical intelligence is perishable intelligence that supports current tactical operations and keeps personnel out of danger. Tactical intelligence must be accurate, relevant, timely, and precise, with detailed information on who, what, when, where, and how.[217] Participants in the survey identified numerous requirements to support tactical decision-making. The following is a compilation of tactical intelligence requirements participants emphasized in the survey.

- Information on known, credible threats for incidents to which first responders will respond.
- Immediate known threats to personnel safety, such as civil unrest, known chemical agents, and bomb-making materials
- Information on active-shooter or bomb threat incidents
- Real-time threat-related information, safe response routes, and secured staging areas
- Intelligence based on incident indicators such as plumes, fumes, or odors that may indicate WMD materials
- Cyber threats
- Real-time information on complex-coordinated attacks
- Public health issues and force protection methods
- Impending severe weather and other natural disasters
- Pre-attack indicators, materials involved, actions to take
- Daily intelligence briefs

[217] Joint Counterterrorism Assessment Team, I-22.

APPENDIX B. JOINT INTELLIGENCE GUIDE OUTLINE

In the fire service, there is a need for more collaboration with law enforcement for intelligence processes and planning. As such, a joint intelligence doctrine may prove beneficial. The Department of Defense suggests that accomplishing missions relies on joint intelligence.[218] More specifically, the purpose of joint intelligence is to "inform the commanders; identify, define, and nominate objectives; support the planning and execution of operations; counter adversary deception and surprise; support friendly deception efforts; and assess the effects of operations on the adversary."[219] Additionally, intelligence informs decision-making by highlighting paths of action and allows for prediction and anticipation of future events.[220] Ultimately, the joint intelligence doctrine has proven beneficial to the military, and adoption by fire and law enforcement agencies may be as valuable. Accordingly, the attached outline represents the vision of this thesis for a joint intelligence guide for use by first response agencies.

[218] Joint Chiefs of Staff, *Joint Intelligence*, I-3.

[219] Joint Counterterrorism Assessment Team, *Intelligence Guide*, ix.

[220] Joint Chiefs of Staff, *Joint Intelligence*, ix.

First Responder Joint-Intelligence Guide

Executive Summary

I. What Is Intelligence?

- A. Definition
- B. Principle of Joint Intelligence
- C. Intelligence Types
  - 1. Open-Source Intelligence
  - 2. Geospatial Intelligence
  - 3. Measurements and Signatures Intelligence
  - 4. Electronic Intelligence
  - 5. Human Intelligence
  - 6. Signals Intelligence
  - 7. Communications Intelligence
  - 8. Intelligence Cycle
    - a) Requirements
    - b) Collection
    - c) Processing and Exploitation
    - d) Analysis and Production
    - e) Dissemination
    - f) Consumption
    - g) Feedback
  - 9. Intelligence Levels
    - a) Strategic

b) Operational

c) Tactical

10. Intelligence Markings

a) CNSI: Controlled National Security Information

b) CUI: Controlled, Unclassified Information

(1) LES: Law Enforcement Sensitive

(2) FOUO: For Official Use Only

c) PII: Personally Identifiable Information

d) SSI: Sensitive Security Information

11. Estimative Language

12. Intelligence Products

II. Access and Use

A. Gaining Access to Sensitive Information

1. Homeland Security Information Network

2. Technical Resources for Incident Prevention

3. Regional Information Sharing Systems Network

4. Law Enforcement Enterprise Portal

5. Law Enforcement Online

6. Fire Service Intelligence Enterprise

7. Interagency Fire Intelligence Exchange

B. Security Clearances

1. Levels

2. Clearance Process

C. Handling Requirements

1. Storage

2. Dissemination Controls

3. Information Security Officers

III. Intelligence Support to First Response Organizations

A. Joint Intelligence Sharing Environment

1. Memoranda of Understanding

2. Information-Sharing Architecture

3. Joint Information-Sharing Systems

4. Unity of Effort

5. Concurrent Planning

6. Need to Share Doctrine

7. Joint Training and Exercises

B. Systems Perspective: Strategic, Operational, Tactical

C. Planning

1. Strategic

2. Operational

D. Tactical Execution

1. Initial Phase

2. Ongoing Phase

3. Post-Incident Phase

IV. Appendices

APPENDIX C. SURVEY RESULTS

Quick statistics
Survey 994998 'Fire Service Intelligence: Informed Strategies, Operations, and Tactics'

Results

Survey 994998

Number of records in this query:	323
Total records in survey:	323
Percentage of total:	100.00%

Field summary for Q1

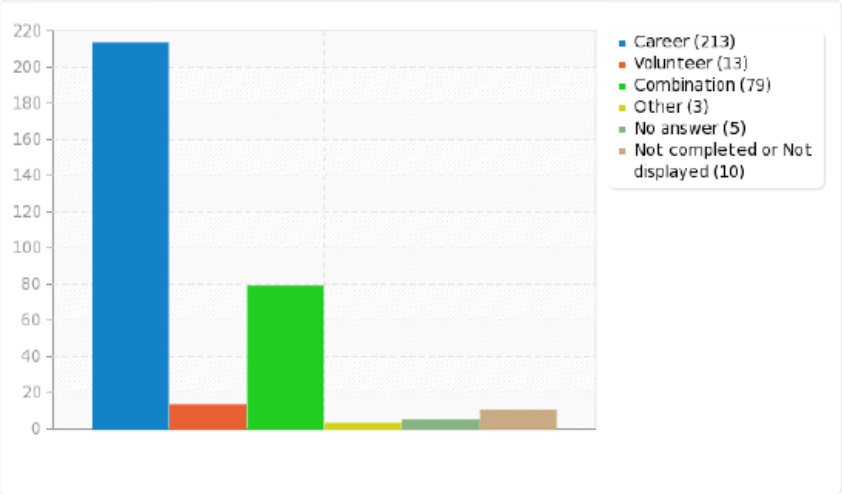
What type of fire department is represented?

Answer	Count	Percentage
Career (A1)	213	65.94%
Volunteer (A2)	13	4.02%
Combination (A3)	79	24.46%
Other	3	0.93%
No answer	5	1.55%
Not completed or Not displayed	10	3.10%

ID	Response
16	State Fire Academy
71	call
250	State Forestry Agency

Field summary for Q1

What type of fire department is represented?



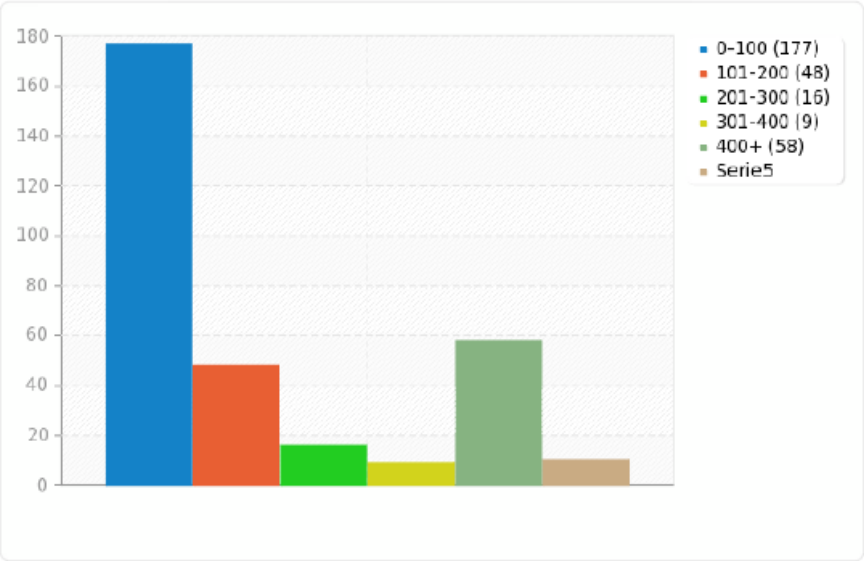
Field summary for Q2

How many personnel are there in the department?

Answer	Count	Percentage
0-100 (SQ001)	177	54.80%
101-200 (SQ002)	48	14.86%
201-300 (SQ003)	16	4.95%
301-400 (SQ004)	9	2.79%
400+ (SQ005)	58	17.96%
Not completed or Not displayed	10	3.10%

Field summary for Q2

How many personnel are there in the department?



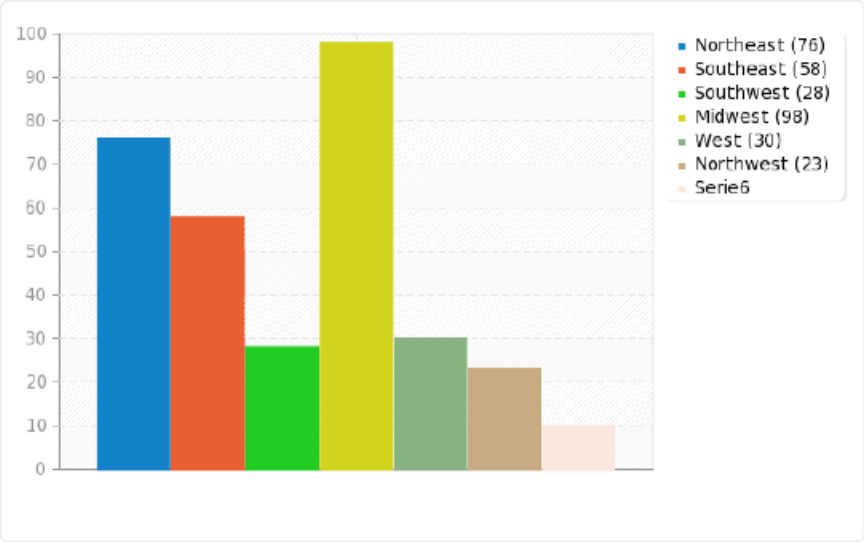
Field summary for Q3

Please specify the geographic location of the department.

Answer	Count	Percentage
Northeast (SQ001)	76	23.53%
Southeast (SQ002)	58	17.96%
Southwest (SQ003)	28	8.67%
Midwest (SQ004)	98	30.34%
West (SQ005)	30	9.29%
Northwest (SQ006)	23	7.12%
Not completed or Not displayed	10	3.10%

Field summary for Q3

Please specify the geographic location of the department.



Field summary for Q4

What would the fire service role in the intelligence community look like?

Answer	Count	Percentage
Answer	115	35.60%
No answer	4	1.24%
Not completed or Not displayed	204	63.16%

ID	Response
1	Active. We need to know more of what is going on and have a seat within the IC. We know what different scenarios will mean to us--no one within the federal government understands that.
3	Information on credible threats to first responders. Information on locations of high risk to first responders. Ensure we are integrated into the response planning. Develop relationships with intelligence entities based on trust.
4	Gathering stats on shared systems to see real time trends. Using similar stats to understand and respond to atypical threats
5	Recipient of information, relay basic information, observations, conditions and such back.
7	- a seat at the table. Local and regional intelligence briefs.
10	Having an operational awareness on the Battalion Chief level.
11	The fire service role in the intelligence community should be one of support, and also be able to report back up the command chain any pertinent findings discovered during normal operations.
13	sharing of information about trends in housing and blight, large events which could be targets of terror, disaster response such as storms and other conditions that might interfere with response
17	Probably a lot of planning both proactive and reactive
21	Departments should be given just enough information to provide safety for their personnel. Too much information chatter will over provide information overload, and might be be read. We have a lot of information coming in daily, and the wheat might get lost in the chaff.
22	Collaborative sharing of pertinent information between fire & law. Better training of fire service personnel on roles and responsibilities.
23	Daily briefings based on intelligence received from law enforcement and/or fusion center partners. Especially if already vetted by a central fire service intelligence officer.
25	Receiving information, provide field and community level input. Ideally, and not normally done in our community, becoming a partner at the fusion centers. Terroism Liason Officers are receivers and not team members.
28	Information gathering for response preparation
29	For the southwest, we need to better understand how fire can be used as a weapon. We sent a delegation to Israel a few years ago and saw that fire was used as a weapon.
31	We should be part of fusion centers
32	Observing, gathering and reporting to fusion center. Active participation in regional arson task force.
33	One where the representatives from all levels of staffing, from administration to senior line people, are present at the local table to have meaningful communication about threats and strengths of the community.
34	Similar to that of a "Branch" in a Unified Command Structure, unless the event surround a service provided by the fire service.
40	Preparation/training and logistics for potential threats
42	I'm not really sure. I haven't thought much about this. I think (in a small town such as ours) simply being in the loop for information that would help us know if there are threats in the community that might effect our daily deployment decisions. If we know there's a threat at the college, we might vary our response routes, and if we don't know, we'll just do what we always do. It would be nice to know something threatened or going on before we decide to send a crew out of district for training or run with a short shift.
41	Receipt of applicable intel (influx of narcotics - type, unique characteristics; large crowds/gatherings; threats against public safety)
44	Subject Matter Expert and possibly as a analyst type person.
45	The Fire Service Role in the intelligence community can come from multiple sources within

	the fire service. Primarily through fire prevention with annual inspections. This aspect should not be take erroneously. Annual inspections have revealed not only fire code violations, but illegal operations as well, such as, massage parlors and human trafficking rings.
48	Street recon and regional reporting
54	Trusted agent of FS vets info using FS perspective rather than LE deciding what we need to know.
56	as a stakeholder with shared information
61	Providing data and analytics on different types of calls especially at Target Hazards.
62	receipt and sharing of info related to potential acts of terrorism or other crimes that may impact how fire depts plan for or respond to emergency incidents.
71	Not sure as we are often left in the dark
72	I haven't given this a lot of previous thought, but at a minimum: some kind of interface with local/state/federal intelligence information sources that provide credible risk-based information that would allow us to prepare, inform (train) our people, and respond appropriately. I would expect that there would need to be some kind of filter to ensure that we're getting the information that affects us, and doesn't bring us into intelligence sectors where we don't belong, or don't have any need to know.
75	The fire service is primarily a consumer of IC products but also a small but important contributor of information (through suspicious activity reports) and intelligence products (through participation in fusion centers as TLOs, the NCTC and other partnerships including with local law enforcement agencies.
79	Provide real time "boots on the ground" information and feedback.
87	Steps that are needed to mitigate the situation from a fire service aspect.
91	Primarily a recipient; occasionally a provider
93	Primarily a receiver of information. However, the fire service may be uniquely positioned to inadvertently witness situations that could contribute to the knowledge base, particularly if adequately trained to observe this.
96	Integrated with fusion center. Like the current fire service intelligence enterprise at the USFA
97	Active violence incident EMS and technical rescue response, pandemic planning, arson and bombing threat assessment.
98	We are on the front lines so we have the ability to gather some potentially important intelligence, and the flip side is we need to have access to a certain amount of intelligence to help keep our people safe.Therefore there needs to be an active two way communication between fire agencies and the intelligence community.
100	Target hazards, high risk populations, high profile residents and visitors, special events with increased visitor populations (festivals)
103	The fire service should be equally involved as law enforcement. FD need to have an OPSEC plan with specific personnel assigned with the appropriate security clearances. Appropriate info should flow to all levels so that all members have some awareness.
105	Having fire minded personnel giving pertinent info or intel that is relevant to existing situation
106	The fire service is more of an end user of the information to keep our members safe and prepared to respond to emerging threats. The fire service can also provide information but that is generally vetted through another agency. When something is noticed on the street by fire department members, that information is referred to law enforcement or other agencies for further investigating or vetting.
107	Input to Intel Community: Using fire service equipment in support of intelligence collection (aerials and drones to provide local imaging angles quickly; community preplans to provide information on locations of interest) Receive from Intel Community: Info about potential activities that could impact the local response area (e.g. flagged addresses which might represent a higher risk to first responders so FDs can preplan a modified response to that or neighboring addresses; briefings on increased activities or chatter in the response area which could lead to a mass casualty incident)
110	Active firefighters in the information gathering and dissemination
113	Connecting with local, state, and federal partners (building relationships and trust) to obtain information that can be disseminated to the members of the department. Also, the FD is one of the key players in the SAR initiative. Nearly unbridled access without legal issues such as warrants.

115	A heightened level of awareness and security which could effect operations and training.
117	Educating engine company officers of characteristics of potential threats, so that tells of impending activity may be addressed in a proactive vs reactive manner.
118	Working in cooperation with law enforcement for things such as fire as a weapon and trained observer
121	Being at the table with law enforcement and and other strategic intelligence briefings that pertain to your jurisdiction. Probably as "ears" instead of "mouth" participants.
127	I believe that the fire service should not only be an information recipient, but should also play a key role in providing information to our local, state, and federal partners. The fire service is unique in the fact that we are not a single discipline field. We respond and must be proficient in fire, EMS, HAZ MAT, wild land,high rise, high angle, and trench rescue. We also deal with vehicles, electricity, solar panels, railways, ect. I would like to see the fire service invited to the discussions as an equal as opposed to an entity that only receives information.
134	The fire department provides facility inspection information that includes point of contacts, layout and infrastructure locations. The FD also provides surveillance in situations where drugs, incendiary devices, precursors and other suspicious activities are observed during calls for service or community interaction.
135	We are a small town but still that state Capital. We are the primary emergency responder and should be in the know when pertinent to our mission.
138	Passing along to a fusion center any relevant information obtained from Operations folks, and receiving safety and operational information from law enforcement.
143	We see and hear a lot about our community, need to have a clearinghouse to give the information to in order to turn information into intelligence so everyone can act accordingly.
145	In Illinois there is a Fire Service Representative in the Statewide Terrorism & Intelligence Center (STIC). This individual is paid by MABAS and spends multiple days per week in the STIC monitoring everything from terrorism threats to weather to PPE shortages. You have to be vetted through DHS to receive daily updates from the STIC. Other reps. in the STIC include Illinois state police, military, state officials, EMA, IDPH, etc.
149	More as a user of the intel, but planning and reporting assets can be a collector and reporter of intel, if they knew what triggers or concerns other agencies may be looking at for intel.
155	Fire is the "All Hazard" service in the United States. If it doesn't take a gun to resolve, the incident is ours.. ie. Oklahoma City, or the Twin Towers and the Pentagon.
160	Providing intell on action occurring in the city, suspicious or non routine to PD or Sheriffs office
161	There is none.
163	An informed participant in potential emergency response.
165	Due to the fact that the fire service enters homes and businesses while responding to calls for service, they quite often see things that could assist intelligence. Info could be shared with a fusion center.
166	Provide increased situational awareness. Let staff know of specific concerns and information needed to allow for additional eyes on the street. Personnel safety.
173	In my opinion the fire service could potentially play a huge impact in the intelligence community. As first responders we are responding to numerous incidents that potentially have intelligence that is gathered and would be useful to other agencies. It would nice to have a reporting platform that allows agencies the ability to report their daily contacts to.
177	informational, advisory
178	depends on the hazards some hazards fd is following advice other hazards fd giving advice
181	As far as gathering, none. However, providing information from houses or businesses that are of interest, because we are inside on an ems call or a call that is non police related.
190	Subject matter experts contributing to the overall mission.
192	Gathering/sharing information from your coverage area, In turn, the information gathered would be shared through a secured means of communication
193	Observe and Report. Being available in the community allows the Fire Service to see things that might otherwise go unnoticed.
195	Knowing what the issues might be could be helpful in getting your organization prepared.
196	End user type information, such as how to respond to a particular threat, possibly pre-warning of potential threats for the purposes of readiness.
197	An "All Hazards" Fire Department needs to understand and receive pertinent information in real time. At the minimum, the Fire Service should be privy to "Law Enforcement Sensitive" bulletins and information.
199	-SAR Collection and awareness

	-Liaison personnel/collaboration with fusion center information sharing -Partnering/Intern positions with a fusion center -Collaboration with fusion center analysts to provide fire service industry perspective -Collaboration with fusion center analysts to ensure relevant, actionable intelligence products are generated
201	The fire service should be a collector, analyst, disseminater and recipient of intelligence
210	Evaluate information relative to fire service specific issues. Law Enforcement does not think in the same track as we do. Fire should work in tandem with LE to ensure that all aspects and impacts are considered when developing plans and evaluating/reviewing prior responses to establish a 360-degree picture that benefits all aspects of public safety and security of the public in general.
213	Membership within the local or regional JRIC, with active sharing of information up and down. Redacted intel passed down to the fire department floor personnel.
215	Providing details on risk assessments, monitoring for human trafficking and providing data, hazardous materials inspections, assessments, etc.
216	A single point of contact within the organization whose responsibilities include risk management. Their role would be to work closely with local, regional and federal LE and homeland security officials. Their perspective would identify a local view from a Fire and EMS organization.
217	Advisory....Listen and learn
224	Each state should have a TLO position back to the fire service to take care of ESF 4 issues.
227	It would look like a partnership with us and the PD, to help ID potential targets of terrorism and other preplanning initiatives specific to the FS
232	An assigned representative to be a liaison to the regions fire service.
233	To me we should be capture points for spotting and recognizing issues that may have need for analysis and follow through by other agencies. In Ky outside of Lexington and Louisville Fire Departments receive nothing from ANY agency about current or suspected threats or even what to be on the look out for other than bland generic everybody is a suspect stuff....
239	combination of all emergency services in group meeting
243	It's difficult to address regarding national security. At some level regional/ national threats need to be addressed and information forwarded to first responders without compromising national security...a gray area.
252	The fire service providers should probably have a clear and easily understandable way to know what threats are likely current in the area as well as a obvious and direct way to report any suspicious things observed by the fire service
253	Not sure
255	To participate in the JTTF /Fusion Centers and ensure that Chief Officers are signed up for law enforcement intelligence briefs.
256	Situational Awareness Planning Coordination and Collaboration with Law Enforcement Fire and Emergency Services Perspective
260	Data collection
262	Collaborative, at the table equally with JTTF and partners.
267	I have no idea
271	Receiving information that effects us daily. Having the training to know what we are looking at so we cn report things we see in the field
273	Provide insight into their abilities and operations so the intelligence community locally, regionally, or nationally can assess how best they might be utilized during incidents involving the intelligence community.
280	We need to be involved in most if not all of intelligence as it relates to Homeland Security. The reality is that the Fire Department is the first one to be involved in an incident and Law Enforcement of all levels only become involve after we have mitigated the incident. Our involvement is necessary so that we can properly plan for any and all attacks that impact our community
279	.
284	the fire service role in the intelligence community would look like
285	In the roll of public safety the fire service has access to certain buildings that law enforcement or other agencies may not have and can see things to possibly answer questions.
286	I would picture a virtual EOC with representation from a state or regional fire service representative, similar to LE intelligence gathering.
291	Ongoing Risk Assessment/Threat Analysis Program

	Ongoing needs Assessment Problem Type/Alarm Type monitoring Asset Availability Resource Availability/procurement
294	From an information consumer standpoint, the ideal state would be both law enforcement and the fire service receiving the exact same intelligence information at the same time - understanding that there is some law enforcement sensitive information that would likely be redacted. From a partner standpoint, the ideal state would be a fire service representative sitting in either the local/state/regional fusion center. This partnership would have the fire service representative researching, analyzing, and sharing information that is fire service specific - and serving as the fire service subject matter expert to the law enforcement representatives.
297	It should involved in the whole processes. Gathering, reporting, analysis, and management and targeting.
298	Information sharing regarding high-risk occupancies or behaviors - including places under investigation for suspected illegal manufacturing of drugs or locations known to house persons who have a track record of threatening public safety personnel. Awareness of undercover activities that may pose a risk to fire/EMS responders.
300	I have been selected to represent the department in this capacity and providing this new communication to our department.
302	AS first responders we sometimes see things before law enforcement does and this isn't always a good thing but it does help identify things quickly.
303	We see a lot of things on incidents outside of a law enforcement response that can be reported for follow-up. Further training is necessary for fire service folks to have the mindset needed to provide this information. Also, receipt of information from law enforcement related to gang activity and terrorist threats would be helpful to prepare for response.
306	Known threats so department can ensure appropriate response capability exists.
312	cooperative, collaborative support in a law enforcement based system. broad permission to receive and share intel.
316	A partner at the table, allowing us to be better prepared.
323	Both a source for information as well as pertinent class of professionals to share information with.
328	In our community it's critical. We're the agency citizens come to for information. We may be of much assistance on the front end, but we play a large roll on the back end.
336	Fire service should be a partner in briefings and training concerning trends in terrorism and homeland security. The fire service locally should be involved in briefings and planning for potential events as well as utilized for subject matter expertise in mass causality and fire related events.
339	Identifying hazardous materials and their dangers.
340	Taking part or having representation in regional or local fusion centers

Field summary for Q5

What are some fire department concerns about receiving intelligence?

Answer	Count	Percentage
Answer	114	35.29%
No answer	5	1.55%
Not completed or Not displayed	204	63.16%

ID	Response
1	We don't receive it in a timely fashion.
3	The information must be credible and based on facts, not speculative.
4	Not uniformly received, sparser, inconsistent, not particularly pertinent to FD
5	Inability to discern intel from fact. Indiscreet, any intel would have to be very basic OR disseminated to a higher rank in the Department that can ideally be trusted with more delicate information.
7	My department has none.
10	Ensuring the security of the information does not get leaked out to both the general public, which could cause alarm/panic, or to the individuals in which the intelligence is based on.
11	Some fire department concerns about receiving intelligence stem from the intelligence source not being fully aware of the fire service capability, including EMS response and transport operations capability if part of normal fire service operations.
13	FD often looked upon as neutral party
17	OPSEC
21	I have no concerns. Knowing existing or potential threats is good to know for daily operations.
22	Relevance and confidentiality.
23	Biggest concern, from practical experience, is that of firefighters protecting sensitive intelligence and understanding/following handling requirements.
25	Security of information, mission creep.
28	Managing classified information
29	We have the TLO program, but we would need additional training to understand how to interpret and act upon some of the intelligence. I think for a small department like mine, we struggle with the upkeep of intelligence. We really need the Feds to better support us.
31	We don't get enough
32	Timely 'roll call' information and maintaining OP SEC on sensitive issues/intel.
33	The security level of the information or not being familiar with how sensitive the information really is. Essentially not being familiar with all the players on the field.
34	One word - "leaks", confidential information leaked knowingly or unknowingly to family, co-workers, visitors to the station who hear things.
40	maintaining security to upper levels of management
42	We don't get any intelligence, except emails from the USCG. The police could be tracking a band of terrorists through the woods behind the fire station and nobody will bother tell us. Part of the problem is that law enforcement/defense are by nature secretive organizations and we are a transparent organization. It makes them uncomfortable knowing that we generally share information with all our staff. We aren't secure in their eyes, and we don't want to be secure in the way they are.
41	Often overlooked, not considered "secure" to share information with.
44	Security of intelligence internally, ops sec training for front line personnel, and basic understanding by upper and mid level management.
45	The top concern would be loose information sharing. While firefighters are trusted sources, there can be leaks.
48	creditability and timeliness
54	Timely, relevant. LE jargon free
56	legal action against the members
61	None
62	Handling and processing various levels of classified material
71	confidentiality, distribution
72	timely, relevant, credible, and coordinated. The information is one part of the equation,

	coordination with law enforcement is another.
75	As you know, most fire service personnel will only see FOUO products. All intelligence products require context to appreciate. My concerns as training officer include: 1) In an era of information overload, how many intelligence products should be shared in my fire agency? 2) A related concern is how to help members of my fire agency see the relevance of intelligence products to their work when we are a small municipal department. 3) Our regional fusion center appropriately restricts the sharing of intelligence products that we get from them to other sworn members of our agency. This is because others with a need to know, such as those from our local LE agency and other fire agencies, can register to get the info directly from the fusion center. The fusion center, and my agency in turn, distributes FOUO products by email and asks recipients not to share them with unauthorized persons. My concern is how to provide members of my fire service agency with the right education and motivation to respect restrictions against sharing intelligence products.
79	Timeliness, has it been vetted and does it conflict with other information and guidance.
87	Too infrequent.
91	Dissemination to the people that need to know; retaining confidentiality when needed
93	Single greatest issue is an overabundance of information that is likely not relevant. This discourages consistent review of the information and clouds out the important information.
96	Privacy/ civil liberties/ protection of information (leaks)
97	Confidentiality, stautory authority to handle law enforcement sensitive information.
98	We realize some intelligence is privileged for good reason, so the ability to keep it secure is one concern.
100	Sharing the information appropriately, Training all personnel on special hazards and special short term needs.
103	Obviously, sharing certain intelligence with unauthorized personnel. The cost and process to gain security clearances for assigned intelligence personnel and chief-of-department is time-consuming and costly. The question always is now that I have this information what do I do with it?
105	the information needs to be relative to the specific situation not what some civilian thinks is relative. This would probably answer the question above by having fire personnel in an intel gathering position and relaying that intel to those in the field.
106	If information is received and disseminated too broadly in the fire service, the sensitive information can be easily leaked. The fire service does not normally receive sensitive information.
107	Right Level: whole FD is probably not secure, so would need to create a small group to receive intel and conduct preplanning, only passing info to response crew when required. Right Training: needs to create generic training scenarios so crews can practice response skills for different types of intel before actual intel comes in
110	I see none, firefighters are on the front lines and educating them and Training them better prepares everybody
113	Lack of education in training. Example, most of the FD is not told what terms such as "FOUO" means and then may share information that isn't supposed to be shared.
115	That the sensitive information get spread beyond the desired group.
117	the culture of the fire department personnel is not one of law enforcement. Personnel may be volunteers within the community. Career or Volunteer they typically have a limited background check, lack of threat awareness, and typically do not view calls as confidential with frequent posts on social media. The FD culture nationally must change for the FD to be real player in the intelligence community
118	Spreading of information outside of work place
121	My jurisdiction PD doesn't even share info on local drug busts that may require FD response.
127	My concern with most intelligence is that it is germane to the safety and efficient operation of the fire service. Much of the information that come from law enforcement are meant for distribution to law enforcement. Its not a bad thing, it is just time consuming to sift through all the non applicable information for that one key thing that helps us out. I also have concerns about the information being accurate. We have all fallen into the clutches of inaccurate information. Having a way to verify info before it is sent to the department is key to making sure that our crews are safe.
134	The lack of understanding of the fire department's roles and need of intelligence as both a service provider and a target.
135	Not getting any when we should.
138	That we are not viewed as part of the team", because we are not law enforcement!

143	Fire fighter like to talk so information sometimes gets where it shouldn't.
145	We used to only get intelligence from our police department and a lot of the info was not relayed.
149	Security of sensitive. As a Law Enforcement Fire Marshal, I received some limited intel from our PD sources. Security was their concern as well. I shared generic information with our operational units, occasionally with them setting the information aside since it was limited and vague.
155	We face both international and domestic terrorism, as well active shooters. Our role is most of the time is done before the Governor, Mayor or Police Chief even arrive for the press conference. Without active intelligence, we go in blind - and someday soon we will again pay a huge price for this oversight.
160	Departments don't normally receive intel from our PD or Sheriffs office because they don't think outside their lines of communication, has gotten better in some instances since 9-11 but not where it needs to be.
161	We should certainly be getting the information we need to plan for possible events.
163	The lack thereof.
165	Ensuring the appropriate information in the right quantity is shared. Avoid "information overload"
166	Confidentiality, FOUO, Assuring information does not get into wrong hands.
173	I'm always concerned that intelligence received by fire agencies could often be shared accidentally or on purpose with individuals who should not have that type of intelligence information.
177	security of info
178	timely accurate and pertinent
181	It seems we rarely get intelligence unless its specifically to our city. I believe we should receive regional information as well since we respond regionally as well.
190	Timeliness and accuracy.
192	That the information is accurate and timely!
193	Irrelevant information can create a cloud of "noise" that overwhelms many on the street. Relevant information, however, is dependent on locations and community.
195	I don't have any issues.
196	Loose lips sink ships, We have a vary widespread range of views and no actual levels security clearance. We have many FD's that don't even do criminal background checks.
197	Unnecessary dissemination of sensitive material to the public. With the proper training and policies, this could be avoided.
199	Access to potential law enforcement sensitive (LES) information that may have impact on department personnel safety
201	Info/intel security
210	Generally poor ability to analyze and use intelligence. IN the case of smaller agec0n0ies there may not be any budget to conduct said analysis.
213	Intel that was shared amongst the floor personnel, would need to be redacted to ensure that certain particulars remained confidential. The fire department must ensure that personnel serve as the eyes of the JRIC, and not to become involved in the process beyond the reporting criteria.
215	Feel we need to be involved
216	Maintaining complete informational security as well as trust of partner LE agencies.
217	Information overload.... Irrelevant information...
224	Leaking information to the wrong people--as an example, Waco.
227	Reliability
232	A lack of a clear delivery method.
233	We are 20 miles East of the Louisville Metro area... We receive nothing from any state or federal sharing house of information
239	That the matters of concern remain with security group within all services
243	How much info is made available to to members without compromising a need to know or security level issue to ensure their safety.
252	This can occasionally make fire service providers feel more like they are in a law enforcement type of situation. Potentially creating a false sense of need for action or over-suspicion. This can interfere with the publics perception and willingness to call and utilize and cooperate with the fire service.
253	Accuracy
255	Frequency- Too many irrelevant intelligent communications will lead to overload and future briefs being ignored. Too little briefs may mean that important intel is not communicated in advance to possible events. This is a fine balance.
256	Data and information shared in inappropriate locations

	Compromise the intelligence
260	Information leaking
262	Movement of personnel due to promotions and transfers discipline for sharing intel, control of intel on existing networks
267	I have no idea
271	It gets to us last sometimes or when we do receive it it is not always as important.
273	Ensuring that the information is provided to only those that have been screened, have an appropriately level of clearance for the information, and how the information is received to ensure security.
280	I would not have any concerns, but the number of people privy to the intelligence would be limited so as not to interfere with law enforcement protocols.
279	.
285	The major concern is losing the trust of the community.
286	Accuracy and timeliness.
291	Making sure its accurate and disseminated appropriately and in a timely manner
294	I think the biggest concern is information security. The fire service does not have as good an understanding about what that means as law enforcement and that is what has kept the law enforcement community from being willing to share information. Said another way, us firefighters talk too much! I believe the way to overcome this is to have a limited and high level initial distribution of information to the fire department; that individual would this distribute the information to those with a need to know.
297	There should be no concerns about receiving intelligence as long as the sources are vetted, the proper clearance is had and the "need to know" is satisfied.
298	Ensuring that classified or sensitive information is not distributed to fire personnel who are not vetted or credentialed to the same level of their law enforcement counterparts. What level of the organization does sensitive information get distributed to?
300	This concept is still new to this department and still in its infancy stage.
302	Timely manner
303	How much information is too much information? How is the information used?
306	Inadvertent disclosure of same
312	Need to know at what levels, rumor control, inconsistent treatment of intel.
316	Security of confidential information.
323	Increased stress over the information that is being shared and not known about in the past.
328	Accuracy, especially as it as related to Covid-19. Timely, far too often we find out about things after the time for action has passed.
336	Fire service receives minimal amount of intelligence. We actually have to seek out information.
339	Up to date information.
340	Overlap of the role of law enforcement and the fire service. We don't want to ne seen as to "police"

Field summary for Q6

What type of interaction does the department have with state or local fusion centers?

Answer	Count	Percentage
Answer	114	35.29%
No answer	5	1.55%
Not completed or Not displayed	204	63.16%

ID	Response
1	Very little. We are left out in Washington State.
3	We are not currently involved in state or local fusion centers, however we have an excellent working relationship with our local police department.
4	not much
5	No day-to-day interactions. Previous intel information has all come from local PD, when they deem it essential for FD to be aware.
7	Minimal.
10	As needed.
11	My department works closely with the state and local fusion centers.
13	rely on local PD to share relevant information as needed
17	Very little if any
21	I have a good relationship with the FBI and receive monthly briefings on threats.
22	Select personnel assuming the role of terrorism liaison officer.
23	It is offered in Illinois to all FDs. Not all participate and fewer yet completely understand their role in the intelligence sharing community. The "intel" concept is new to Fire Service.
25	TLO program in California. We have a three person team assigned to monitor and interact with the fusion center. It isn't a high priority in the daily workload but is consistent.
28	Typically only information pushing.
29	As said above, we have on TLO - Terrorism Liaison Officer.
31	None
32	Direct
33	Not enough. All of the fusion centers only want to deal with drug trafficking or homeland security. The fire department is always an after thought or considered to be responsive in nature.
34	Information brought through either MABAS, FEMA or Local OEM.
40	Limited to county EMA
42	Limited. Occasional email notifications. One-way communication -- them to us.
41	Little to none
44	Currently none. It should be that they have a seat in the local fusion center and at least a connection to the state level one if not a rep of some kind there also.
45	Currently through local police departments only.
48	Very Limited
54	My FD has none.
56	very little, I am a TLO and have been for a long time. Not much shared interest among Fire Chiefs either lack of support for programs like this, prevention, education etc
61	Fire Chief and Assistant Chief are dual role and are involved with Emergency Management.
62	Currently have a working relationship with two regional fusion centers. Receive daily info via emails & granted permission to join online chat forums during certain situations.
71	Right now little to dnone
72	None
75	Several sworn members are TLOs. As one of them, I've checked in with our municipal LE agency to be sure that they engage with the fusion center, and I've lobbied our public works and water quality treatment plant folks to also participate (which our fusion center allows as "private partners.") I've also suggested to the emergency response team managers of several of our largest companies (in the same industry) that they should engage with the fusion center as private partners and with their industry ISAC. About 2015 we had our fusion center's fire service representative teach line folks a two-hour overview of terrorism. We would have him back except that we struggle to fit mandated training and

	local training needs (including EMS and rescue) into our calendar in the time we have.
79	Limited at this time. The only interaction is reactive.
87	Minimal
91	We receive email updates regularly
93	We are in Illinois. We have frequent (daily if desired) interaction.
96	Our is limited due to resources, but we have access via a TLO program.
97	Limited, open source, operations sensitive intel.
98	Very little
100	weekly email briefings unless specific threats are directed to our community.
103	Most of the firer service has little or none excluding major departments. FDs need to be more involved and assign personnel to these centers. At the national level, we do have a seat at DHS security ops. Unfortunately, the fire service has trouble staffing these position because the fire department does not want to pay some of the costs involved to have their member live and work in nation's Capitol. PD fills their spots. A good source of informatio9n is the International Association of Fire Chiefs' Terrorism and Homeland Security Committee.
105	Watered down, second and third hand information
106	Not much at all.
107	Our dept doesn't have any interactions that I am aware of at my level. The chief may be participating in some interactions, but we don't hear about them.
110	Very active with personnel with TS clearance
113	I am a "trusted partner" with the state and local fusion centers. I have access and typically will go in at least once a month in person and speak with our fire and ems rep weekly (sometimes daily), depending on the events going on.
115	Unsure.
117	career employee within the center
118	On mailing list, fusion center liaison
121	Unknown
127	My department has a good relationship with the other local departments. We also have a good line of communication with MEMA and other state agencies that allow for frequent table top exercises. I can't say that I have ever had any experience with a fusion center.
134	The FD should receive information from and deliver information to the fusion center. The
135	It's in town. But literally none. We can call and ask if need be.
138	Zero!
143	Extremely limited to most of the staff. Chief interacts some and disseminates information that needs to get down the chain.
145	There is a daily briefing on a regular basis, now with Covid-19 those updates include related materials. We also can register large special events with the STIC and receive any pertinent updates on weather, terrorism, and social media chatter for our events.
149	VA has a fire service asset in the fusion center, but there was little information that came from that desk to local departments. Most if the intel I received was through HSIN or local PD intel officers.
155	Not much. While we are active in the Regional Operations Center for any disaster, there are very instances when a Fusion Center shares anything AND it is usually information already available through the local media.
160	During certain times of the year have good interaction with the Fusion Center, but other times of the year not so much.
161	In PA, the law that created the fusion center specifically prohibits information from be disseminated beyond the police community.
163	Unknown.
165	Very limited, however, this should change.
166	Minimal
173	Our department has very little interaction
177	limited
178	sitting at the table with them
181	I am a new Fire Chief and I have no interaction what so ever.
190	Proactive and informative.
192	Currently interactions are through email, word of mouth, voice and video conference calls on unsure lines
193	Austin Regional Intelligence Center has create a Basic Intelligence Officer program for FD and local community providers such as Schools. They have included an Austin FD Captain in the ARIC to help identify information that would be pertinent to the local fire departments. All Battalion Chiefs and above have been trained through the ARIC program and receive emails with pertinent threats.
195	I receive information daily from our local fusion center.

196	We receive reports from our State Police Fusion center, and I suspect anything that we see that looks like it might be applicable to report would be directed to them.
197	None - In New York, the Fusion Center and DHSES stovepipes information and fails to include local municipalities (Fire Service). Years ago, my former City in Kentucky, I was active with the Fusion Center as well as all levels of government. Information sharing was very beneficial to the Fire Department, especially when i was heading the Arson Unit.
199	Significant. Too much to list in a paragraph. Reference the next question, "Does the organization supplying intelligence understand the fire department's intelligence needs?": Only because the region supplies a fire officer to the fusion center.
201	One Captain serves as the liaison
210	very limited.
213	Sharing of information occurs between both the local and state fusion centers. Our local JRIC representative then sends out the information to the fire department rep. Our FD rep then distributes it via email to the membership.
215	some
216	Good incident management relationships at the local, state and federal level with respect to planning for and managing large scale incidents.
217	Monthly briefing
224	connected through the state fire chiefs
227	As far as I know only in cases of emergencies or when a particular political event is coming to the region
232	We receive a daily email, which a big improvement
233	I know of them from Teaching for the state Fire Commission but they are staffed and interact exclusively with large metro and State police agencies. In Ky its a works program for retired FBI and KY State Police supervisors.
239	complete in an emergency declaration.
243	They should be very involved and try to balance security issues with members safety
252	I do not know the full extent but there is a fusion center that any member can get low clearance level alerts via email from.
253	Not sure
255	Our department assigns a liaison specifically to the local fusion center. Our Department/County EOC maintains informational awareness with the state.
256	We get regular fire and public safety briefings. Statewide system.
260	very little, just information from publications
262	High. All events, SA and relevant connections are made back to the Fusion Center
267	I have no idea
271	We have little to none
273	None, currently.
280	We receive daily/weekly reports from our fusion center and we have an excellent relationship with the local FBI and law enforcement members.
279	.
285	The agency I work with gets some fusion center information but this goes to certain individuals not the department as a single unit.
286	Currently, limited to EMA or local LE intelligence
291	I as the Chief have agreed to serve as a LE Liaison with the St Louis Fusion Center, so I have direct contact
294	See the first question with my answer regarding having a fire service representative embedded within the fusion center. Currently, our state fusion center has a part-time fire service representative seated (I think it should be full time). We do not have a fire department representative in our local PD's fusion center but we have a good relationship with them and they share information that they believe is relevant (therein lies the problem - they share information that they "think" we'd like to know).
297	Very limited.
298	We work with our Fusion Center here in Vermont for large scale events. In fact, we incorporate a fusion center employee in our emergency operations center. This allows for a real time transfer of information to fire/EMS/and Law Enforcement persons working the event.
300	I work closely as the liaison to UASI for the department
302	Chief receives updates currently

303	Little to no interaction.
306	None
312	integrated w/ Fusion center, unreliable info at best, failure around what they should share
316	For my current District, none. When I worked the Denver Metro area we were very engaged.
323	Outgoing - Statistics being shared concerning call types observed. Incoming - information concerning heightened security levels, or notations of possible high level incidents taking place.
328	We have very little other than through blast emails.
336	Our department has a member of the local fusion center.
339	None.
340	Ours has none - because or our role and the places and things we see on a daily basis integrating the fire service into fusion centers would be beneficial to everyone.

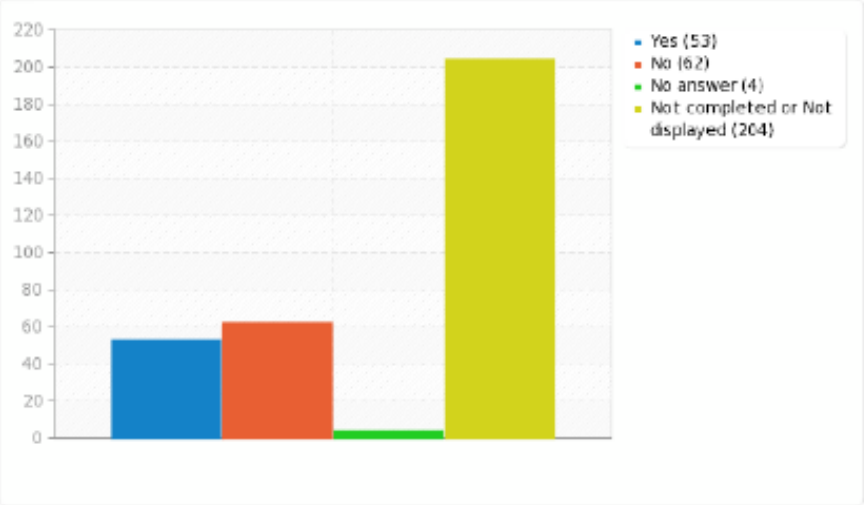
Field summary for Q7

Does the organization supplying intelligence understand the fire department's intelligence needs?

Answer	Count	Percentage
Yes (Y)	53	16.41%
No (N)	62	19.20%
No answer	4	1.24%
Not completed or Not displayed	204	63.16%

Field summary for Q7

Does the organization supplying intelligence understand the fire department's intelligence needs?



Field summary for Q8

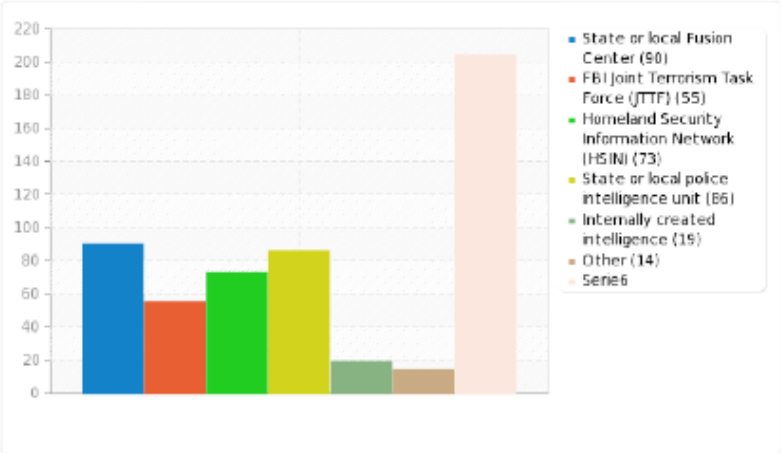
What are the department's preferred ways to receive information/intelligence? Please select all that apply.

Answer	Count	Percentage
State or local Fusion Center (SQ001)	90	27.86%
FBI Joint Terrorism Task Force (JTTF) (SQ002)	55	17.03%
Homeland Security Information Network (HSIN) (SQ003)	73	22.60%
State or local police intelligence unit (SQ004)	86	26.63%
Internally created intelligence (SQ005)	19	5.88%
Other	14	4.33%
Not completed or Not displayed	204	63.16%

ID	Response
32	Arson Task Force
33	Local briefings or special event
34	IL MABAS
103	shared with other FD
105	local jurisdiction
107	Impossible to answer since we don't typically get intel now
127	All of the above if relevant
143	local district S.O. commander
145	STIC combines all of these resources and our local PD provides info for our town.
161	none
163	local pd should share w/ fd
197	Tripwire and or BATS
252	Unknown by myself
297	IFIX

Field summary for Q8

What are the department's preferred ways to receive information/intelligence? Please select all that apply.



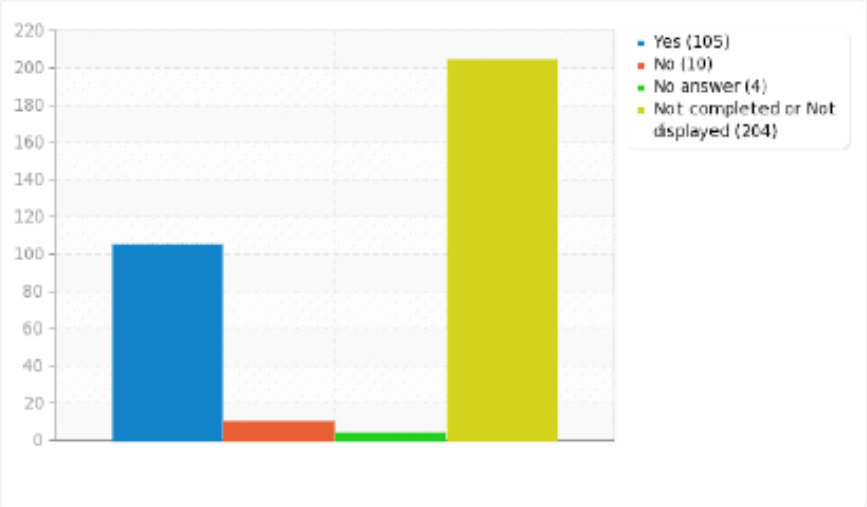
Field summary for Q9

Is received intelligence of value to the department?

Answer	Count	Percentage
Yes (Y)	105	32.51%
No (N)	10	3.10%
No answer	4	1.24%
Not completed or Not displayed	204	63.16%

Field summary for Q9

Is received intelligence of value to the department?



Field summary for Q10

How is intelligence disseminated to the rank and file?

Answer	Count	Percentage
Answer	114	35.29%
No answer	5	1.55%
Not completed or Not displayed	204	63.16%

ID	Response
1	If it is important we make it a training issue. If it is sensitive or too non-specific, we monitor the information as a leadership team.
3	It depends on the nature of the intelligence. If it is highly sensitive it is shared with Battalion Chief level and above. They will brief the affected crews verbally. If it is location specific the Computer Aided Dispatch (CAD) is updated with relevant information that crews can access when responding to that particular location. If it is general information it will be distributed via memo or email.
4	its not
5	Previously has gone from Admin, to the Operational Battalion Chiefs, then perhaps to the Captains in the affected/suspected areas.
7	As of right now, it is not, because we do not received sensitive LE info.
10	The level of Battalion Chief is made aware of the intelligence. It is then disseminated down to the people who work in specific fire stations who could be affected.
11	Only on a need-to-know basis down to the operational command level (battalion chief) in my organization.
13	email and command staff briefings
17	Currently it is not unless they respond to a specific incident that might be flagged in CAD
21	It is generally not disseminated below the officer level for operational security.
22	Those relevant issues are disseminated to company officers.
23	Should be face to face briefings with opportunities to ask questions and discuss. Also provides opportunity to reinforce proper handling / protection of sensitive intelligence.
25	TLO's receive information from the fusion centers, and the Division Chief of Community Risk Reduction receives information from the HSIN. If applicable it is shared department wide via email.
28	Email or targeting briefing
29	Primarily, our TLO updates me monthly and then we decide what to disseminate.
31	It is not
32	'Roll Call' briefings and arson task force
33	Currently on a need to know basis. Most line staff have not been trained on the sensitivity of critical infrastructure information or the ramifications of its misuse.
34	Directly to the Shift Commanders, with direction who shall be included with this information pas along.
40	Policy/procedure filtering down from administration to shift commanders to actual fire fighters
42	We are one station. Depending on the information (potential harm, imminence, effect on deployment, etc.) it might be as simple as me telling the duty staff in person, or it could be an email to shift commanders and other officers. Sometimes a department staff meeting (arson intel).
41	Supervisors notified by email or phone; department email sent out if appropriate
44	Currently, it is not. There is no one point of contact that officially receives it. There is some backdoor contacts through PD contacts that sometimes pass info along.
45	For Official Use Only (FOUO) emails
48	Chain of command using email, video conference or face-to-face when needed.
54	Much is not because they don't need to know. When it is, it is done verbally to avoid electronic sharing.
56	through ops meetings
61	Information is broke down and then given out to individuals on a need to know bases
62	Info that is deemed limited distro is only shared with officer cadre. Info that is allwoed to be more widely disseminated goes to all dept members as awareness info.
71	as needed
72	Not currently disseminated

75	Backtracking to "Does the organization supplying intelligence understand the fire department's intelligence needs?," I marked Yes because the info is of value. One could just as easily mark No if they don't see the value. Products with the most value are the EMR-ISAC Infogram, FDNY Watchline, and NCTC First Responder's Toolbox because they are concise and focused on our needs. The various cyber-security alerts and products are of medium usefulness. The NYPD Weekly Terrorism Briefing is less useful because it covers primarily foreign terror. On the question "What are the department's preferred ways to receive information/intelligence?," I checked everything but internally-created intel because I'm happy to receive relevant intel from any legit source, but so far our fusion center provides everything. The fusion center aggregates products into approximately 1 email per week, so I actually get the Infogram and Watchline more promptly from their creators. I stopped using HSIN because it was a pain to keep the login current and because HSDL and CHDS provide enough good info for my interest. On this question, my agency lets any TLO email everyone in the Suppression division with intelligence products. One particularly-engaged TLO sends almost all of the intel that rank and file get. We don't print or post products because we have non-sworn people in our fire stations.
79	Through the respective departments in place distribution systems.
87	Depending on topic and relevance, it is done via e-mail.
91	Email to appropriate recipients
93	Typically reviewed and consolidated. Some is put out as a training notice or incorporated into training. May be passed directly along through email if appropriate.
96	To the officers unless designated law enforcement sensitive. Those go to the fire investigators as appropriate. All intelligence is review by the TLO / ILO before dissemination.
97	Through company officers; generally e-mails or briefings.
98	E-mail
100	Daily crew briefings or email dependent on the risk profile and threat rating.
103	High ranking officers receive full intel. The intel is cleansed and distributed to all members in a redacted and need to know format.
105	Face to face briefings and breakout sessions
106	E-mail or in person by a Battalion Chief.
107	Its not.
110	limited due to the requirements by FBI
113	I typically distribute most via a list serve to the department members. There are some talks about placing it on a shared folder on the county network in the future.
115	Broad General Orders with limited information.
117	through an email. And typically this information is something that a google search would bring up.
118	Depends on the information. Some is and some is not.
121	If received, it would be passed down either in writing or a video meeting to share information with company officers who would need to know.
127	After the information is validated, it is either disseminated via email, posting on a board, through hands on training/walk through inspections, or via web based activity.
134	Command staff should discuss relevant information then set up a protocol for dissemination of relevant intelligence.
135	Need to know basis if applicable. But we really don't get any.
138	Thru the Executive Staff, decisions would be made about what and who information shold be disseminated.
143	Some is and some is not, most information seems to only be tailored to LEO agencies
145	I put pertinent reports on Target Solutions for our members to review as a company. If it's very important and pertinent these reports are shared at daily ops. meeting with the officers at all 10 stations.
149	Through our LE FM, to the senior operational leadership, mostly by word of mouth to avoid FOIA releases of emails.
155	The Fusion Center bulletin is conveyed both .at shift change and to individuals emails as needed
160	Brief personnel on an as needed basis depending on the subject. In the military (as a firefighter) kept personnel abreast of intelligence at all times as it changed during wartime operations.
161	It would be done by mass e-mail and shift briefings.
163	Chain of command

165	Currently, it isn't.
166	Depending on importance, briefings, email or memos
173	Carefully and on as a need to know basis.
177	depends on the info and confidentiality concerns, usually internal memo to rank and file
178	email and meetings
181	Through meetings and emails.
190	Follow the procedure for "Need-to-know" criteria.
192	Email through our company officers
193	When threats are identified to our community, it is passed on during daily briefings and/or face-to-face officer discussions.
195	Through the Chiefs office.
196	Relent things to watch for are posted, specific hazards are subject of shift briefings and training as necessary.
197	Memos or Advisories from the Chief to the Officers. Fire Investigation Unit as well.
199	Re: above question. More often the answer is no. Once again, this is lengthy description. Email and department intranet
201	Very seldomly is.
210	Via Staff meetings with senior leadership
213	General information is shared via group email. Individual specific intel is distributed via individual email to JRIC Department personnel.
215	Bulletins or Not for Distribution emails
216	Depends on sensitivity of information. Might be email, training or direct communication.
217	Email
224	filtered at Chief level, operational issues are shared widely, although source is scrubbed.
227	From the Chief down via written directive or voice if it is sensitive
232	Non-urgent, via email. Urgent is delivered directly via verbal discussion.
233	Would be done if any was ever received at the appropriate Shift Commander or district station level based on whats needed for that area or threat
239	by informing senior conmmand when necessary before rank & file involvement
243	Thru a regional threat assessment center but based on personal experience I believe a lot of info is withheld that directly effects members safety that could be "vaguely " disseminated to address enhance safer responses.
252	Email update from fusion center or possibly department email
253	Not sure
255	This information is sent through the chain-of-command or directly to effective units (example STAT team) depending on the "need to know", situation, and affected unit.
256	Shared with staff for situational awareness based on the specific information.
260	e-mail and department meetings
262	Filtered at the Chief level then shared directly and not electronic if it can be avoided
267	I have no idea
271	Email
273	While we do not currently receive any such information, it would be disseminated on a need to know basis, and only to those that have been properly screened and meet security clearance criteria.
280	We disseminate it on a need to know basis, but if we do disseminate it we try to frame it in a general way so as not to ruin the relationship we have built with law enforcement
279	.
285	email.
286	unclassified via email. Classified via phone or text messaging
291	As the Chief I receive the information first, then I dissemenate it among the rank and file as necessary
294	As noted above, a select few members of our organization receive U/FOUO information from our state fusion center. Those individuals (TLOs) will generally communicate and identify who to further distribute the information to within the department to be prepared. Like most internal communication, this "flows down" through the chain of command to those who would be most impacted. Occasionally, broad-based information will be distributed department-wide but this is rare.
297	Through limited means via memo.
298	Currently, sensitive information is distributed to the Chief of Department and the Deputy of Operations. The DC of Ops determines whether or not the information needs to be shared at the lower level of the organization - an informal risk v. benefit analysis is performed to determine what level of employee is brought into the circle of trust. If the risk is credible, information is often distributed via face to face conversation about geographic locations or addresses of concern to the Station Captain who oversees the fire district within the City.

	The Station Captain will then pass the information on verbally to his direct subordinates - often his/her Lieutenants who serve in that district.
300	Information is disseminated through the Fire Chief and the executive staff.
302	Through department e-mail
303	We don't receive specific intelligence from law enforcement regarding any threats.
	Occasionally a street officer will report a "be on the lookout" to our field crews, but there is no current systematic and habitual fusion of useful intel for us.
306	Stereotypical it is not, the rare times it's received it is kept at the officer level as it involves changes in response or response type.
312	through classified briefing tools
316	We currently don't have any intel input. Info should be on a need to know and via face to face if possible.
323	Face to face reports with notations of the need for other staff being advised.
328	Through Senior Officer group.
336	Informational briefings and through the command staff
339	Word of mouth.
340	Dependent on the situation, but normally through the chain of command.

Field summary for Q11

What type of intelligence or information does the department need for standing information requirements?

Answer	Count	Percentage
Answer	114	35.29%
No answer	5	1.55%
Not completed or Not displayed	204	63.16%

ID	Response
1	These days, any threat that could involved us as first responders.
3	Information on credible threats to first responders. Information on locations of high risk to first responders.
4	idk
5	When/where to be extraordinarily alert to surroundings,suspicious individuals, etc.
7	Homeland Security/Terrorism/Sovereign Citizen/Prior LE interaction in regards to devices and bombs
10	N/A
11	Perceived threat and type of threat.
13	info that might interfere with response
17	Not really sure on this one.
21	Outstanding terrorist threats against citizens in the state. Some national concerns are brought forward.
22	Recognition and safety information.
23	Trending threats, physical, cyber, etc., be they local or global. How to protect against those threats.
25	Contextual information is very important to achieve ownership for field personnel.
28	Any specific threats or national/regional trends.
29	Terrorism activities, human smuggling,
31	Terrorist traffic regarding our jurisdiction.
32	Timely and 'packaged' for Roll Call
33	Area of the response district, both primary and secondary, that have risks or intelligence concerns. All types of problems can end up including the fire department operations. The information should be all inclusive and screened by higher ranking staff for dissemination.
34	Fire service specific, EMS Specific and what special operations/equipment should be readied or prepared.
40	Pandemic, creditable threats to businesses and infrastructure
42	Arson intel would be nice. We find out about arson cases around at fire chiefs meetings or on Facebook. Immediate threats to the community -- criminal with gun somewhere, bomb threats, cyber threats.
41	As a resort community, things like daily occupancy levels at rental units (how many folks in town), any uptick in social media about parties (expect alcohol/drugs/underage etc)
44	Whats considered a hazard for LEO is not always a hazard for Fire and vice versa. Large events, for example, may not rise to a level of concern for LEO because its not a big terror threat, but the crowd size and weather conditions may give concern to FIRE for medical reasons or possible severe weather impact to an event that could cause injuries and cause a FIRE response.
45	site surveys- for safety reasons these can be held on the local CAD system.
48	Supply chain and logistics of required equipment
54	I don't understand your question, sorry.
56	any and all local threats
61	Target Hazard
62	Good question .. I need to put more thought into this one
71	what ever effects the cover protection area
72	Unsure at this point
75	I prefer intel on a wide variety of threats including cyber, bio, PRND, infrastructure (including water supply, transportation, electrical, natural gas),"first amendment audits," etc., not just about violent extremism. Bulletins about theft of first responder uniforms, vehicles, and equipment are also good.
79	Daily informational briefing.

87	Potential threats, changes to current threat level and reasons why.
91	Anything that impacts our operations or impacts our jurisdiction and neighboring jurisdictions
93	All based on applicability to our area and organization. Typically would be events in our area, groups known to be in or heading to our area or something that could be predicted to have a direct impact.
96	Our are inline with the fire service intelligence enterprise intelligence needs document. We rely on the fusion center to help distribute local intelligence bulletins.
97	Credible threats instead of general awareness.
98	Any info that could impact our operations by creating safety concerns.
100	Continued timely updates and special needs to address threats identified.
103	Credible threats both locally and nationally, who is involved, mode of operations, telltale signs
105	fact based with prediction built in in order to anticipate changes in the mission and to develop contingency plans
106	Anything that could involve a fire department response to ensure the right resources are in place and crews review/train for the potential operation.
107	Not sure we can answer this without seeing the types of intel available. We don't know what we don't know.
110	Where the crazy people are that we may respond to their residence as well as terrorism info specifically related to the bomb squad
113	Generally, threats that could involve the FD or the calls we may be facing. Also, general awareness that the FD may come across.
115	General threat assessment. Specific information related to credible threats.
117	potential threats in the area
118	Daily situational awareness
121	Would need information on anything that might involve a FD response.
127	Building plans, water, electric, gas infrastructure plans are vital to the safe and efficient operation of the department. Any changes to these plans are important to get to the working crews.
134	The FD should received the same information listed above: delivery or suspicion of precursors, weapons, drugs and other illegal behavior that poses a risk or danger to the community and or responders in the community.
135	Not sure
138	Potential safety and security information.
143	Some sort of heads up for crews responding to certain areas or addresses that are known problem locations. Responded solo to multiple drug homes or meth labs putting crews at risk that could be prevented. Again line crews don't need the info but dispatch could code them on the response to staff and wait or extra PPE whatever.
145	any current terror threats, we also get weekly cyber threats, trends on fires around the state or country.
149	Crime, drug activity, known or suspected threats, and anything that may threaten our members on duty or create resource demands (incidents) to the department.
155	Certainly what is anticipated for large gathering events - we stand up our own EOC, but it would be good to know what the eyes and ears of the Fusion Center knows (if any) to possibly prepare for.
160	Threats in our area
161	Any type of threat that is received. The assessment of that thread.
163	Who, what, where, when, how.
165	Civil unrest, drug labs, terrorism
166	Credible threats. General location of high risk police activity for preparedness and crew safety
173	Information that is likely to impact the fire departments ability or inability to respond to an incident.
177	latest up to date info on situation, real time data
178	how it affects: personnel operations equipment and supplies
181	Threat assessment of the specific event so we can prepare for the role we will play should the event take place.
190	Potential threats to vital infrastructure.
192	High Risk, Low frequency information

193	School threats, active shooter threats, disturbed persons with history/potential for violence (especially upon first responders), threats against medium and large busineses
195	All information is important. I think we should receive all intelligence.
196	Specific threats or things to be on the look out for.
197	Pertinent hazards or risks, precursors to terrorism or crime, trends etc.
199	narcotics, gang, health,protests, local government actions
201	Current threats, or pre attack indicators
210	Unknown
213	Local protests involving violence/barricades, also those protests involving individuals chaining themselves together, to inanimate objects, etc. Possible arson attacks, etc.
215	Anything from weather to tactical operations for events, projected transport of WMD agents, etc.
216	On an as needed basis.
217	Imminent threats.... latest trends....
224	trends and threats
227	Potential impacts on resource demands and EMS resources along with staffing issues and mutual aid concerns
232	Direct hazards to responders and those we serve.
233	Threats, targets, things to observe for while performing our other duties and how to report back
239	Hazmat,contaminated areas & locations. Personnel at risk or infected in case of virus contamination PPE Requirement & availability.
243	National , regional or specific threats that may effect normal responses for a region or department.
252	Unknown by myself
253	Not sure
255	Possible escalation of violence and civil unrest. Possible or planned terrorist events.
256	Current threats Potential Threats Impacts to public safety partners that may change our operations.
260	data for statistical review
262	Threats for events, special dates, identified addresses, etc
267	I have no idea
271	Anything that effects us in responding to fire and medical calls
273	Threats against public, public safety officers and representatives, threats against high value target locations within the jurisdiction.
280	Any and all information as it pertains to Homeland Security and/or other local terrorist threats.
279	.
285	Possible heavy gang areas for safety to responders.
286	Local community risk, trends from a state or region.
291	High Hazard areas, Terrorist threat readiness and preparation, imminent threat notification, known threat or known hazard standing orders
294	Primarily I think is would be related to daily law enforcement plans for interdicting known bad actors. We are fortunate that our tactical medics deploy with the SWAT team so we have that type of information. My recommendation would also include receiving information from law enforcement about known locations where criminal activities are occurring - weapons cache, bomb-making, drug houses, et cetera. I don't think that we need information about initial, developing, or even ongoing investigations until the information gets to the point where there will be action taken (except for receiving the location as noted above).
297	My department doesn't have standing information requirements. This is something that should be implemented through SOPs and superiors reading reports.
298	Who, what, when, and how. You may think this was done to get a laugh, but in all honesty - the more information the department has, the better prepared we will be for the next incident. We do not know where our next fire incident will be in our community - so we often will perform blanket pre-plans, targeting high-risk occupancies as a priority. The same thought process should occur with the distribution of sensitive information from law enforcement. If there is a risk to responders - fire and EMS personnel should be aware. It is time that these barriers

	have a structured method for information sharing across public safety departments. In today's operational platforms - fire/EMS/and Law Enforcement collaborate daily on incident scenes, we need to ensure that we are aware of the actions of each other, so we may support public safety as whole, not held to organizational silos.
300	A more formalized approach.
302	Locations that are potential hazards to crews
303	Gang threats, potential terrorist activity, higher-than-normal drug activity, school threats.
306	Threats, gatherings, protests
312	Hx of location for threats to public safety, threats to public safety from individuals. appropriate staging and deployment of resources
316	Where are the hot spots. Not just domestic terrorism but felony arrest. We were called in to a chest pain call at 3 AM to the same address SWAT was set up to arrest a murder suspect at 5 AM. Placed our crews at risk.
323	Any and all information which may lead to preventing loss of life.
328	Front end information and accurate situational awareness as the incident progresses.
336	Information on protests, local threats, and occupancies suspected to be involved in any type of event
339	Movement of hazardous materials.
340	First and foremost intelligence that could affect the safety of firefighters.

Field summary for Q12

How does the department use information/intelligence to support daily operations?

Answer	Count	Percentage
Answer	114	35.29%
No answer	5	1.55%
Not completed or Not displayed	204	63.16%

ID	Response
1	We plan. We prepare. We train our people.
3	The Deputy Chief of Operations reviews the information and shares the appropriate information with Assistant Chiefs and Battalion Chiefs.
4	Really doesn't
5	When/where to be extraordinarily alert to surroundings,suspicious individuals, etc.
7	NA
10	No.
11	My department staffs a special operations department, usually with 2 field personnel and a special ops battalion chief.
13	yes sometimes changing staging and or response patterns
17	Currently nothing
21	Only when there is a credible threat to our community.
22	An example was an advisory of an upcoming concert with possible attendance by rival gangs. Law enforcement staffed with additional personnel and fire resources at the event were advised to report observations and remain vigilant in their safety.
23	Can be used for things / areas to avoid, on scene operations, need to beef up response numbers, etc.
25	Daily operations aren't generally supported by this information. It is used more as a "watch-out" for return of information.
28	Equipment purchasing, training, "staffing up" if necessary.
29	rarely on a daily basis
31	We do not
32	Adjust response protocols and special event planning.
33	Primarily safety concerns of responders. However, it could be very beneficial for responders to gather intelligence if they were trained on the proper reporting or chain of command.
34	Readies personnel for the future, either through equipment preparations, safety awareness and what resources might be needed.
40	Dissemination/awareness to fire fighters on the street
42	If we knew of an actual or potential threat we might change our staffing or deployment for the day. We could make the station more secure. We could give our staff the awareness so they don't walk into a problem.
41	Similar to rip current forecast, if large numbers incoming may increase staffing, assign to special units, etc.
44	IT could be used to adjust staffing needs or alter unit locations based on anticipated call loads or potential impacts.
45	Call dependent
48	Short term policy and staffing adjustments
54	Usually doesn't. Used more for planning.
56	preparations for response, prevention, mitigation and recovery
61	Any threats on Target Hazards are then utilized on response matrix
62	Used in discussion w/ city PD & Public Safety dept heads to adjust Incident Action Plans for local events
71	Planning, scheduling, staffing
72	currently it does not
75	The most common use of intel is remind rank and file folks to secure fire stations and leave somebody with emergency vehicles when possible. We also use it to consider training and equipment needs.
79	Apply it to operations.
87	Operational awareness

91	Mostly as an advisory to keep personnel informed of possible issues
93	Passed on to members and used in planning.
96	Depends on the intelligence value, but it helps maintain situational awareness for all firefighters.
97	General situational awareness.
98	Protecting our members from going blindly into unsafe places.
100	Situational awareness, special training needs and necessary equipment to address identified threat or situation.
103	Two ways - general knowledge and chiefs' awareness and also modification of response operations
105	insures a proper response model and having a common goal for a common threat
106	Preparation and training
107	We don't right now that I am aware of.
110	General overview of threats
113	For the department as a whole, general awareness and safety.
115	Security and training.
117	it does not
118	Depends on inforamtion, some is shared to be on the lookout for and some is not.
121	Might be just a heightened awareness or might involve personnel call-backs to bolster staffing/apparatus. Might also be a planned bolstering of personnel/apparatus if lead time is enough.
127	Currently we use the information in our building pre-plan surveys. We are transitioning to having the plans and the information in truck mounted computers for easy reference.
134	Providing relevant training, preplanning, staffing and deployment of assets
135	Nothing as of now.
138	We don't receive any currently. Even our County OEM & HS views the fire service as outsiders.
143	We try our best to mitigate prior to the concern hitting our area, provide training ahead of the calls received for the hazard. Awareness and readiness
145	Increase awareness and vigilance.
149	As we used it, staffing levels and coverage have been adjusted when warranted.
155	We would if we'd have it. However, during the COVID-19 the systems used to convey information from our Health Department to a single responsible person has worked extremely well.
160	Staffing can be increased or adjusted based on perceived threat
161	It would depend on the specifics of the information recieved.
163	Prepare for potential responses.
165	Currently, just for enhanced situational awareness.
166	Increased situational awareness before responding into an area of increased risk. Preparing for potential low frequency response types.
173	The Chiefs carefully disseminate the information on a know as needed basis.
177	depends on situation, for Covid-19 we had positive addresses marked on our MDTs for PPE alerts
178	advising personnel ordering supplies
181	Helps us develop incident action plans and develop future training needs assessments with all branches of law enforcement.
190	Priority asset assignments.
192	When responding to alarms, the information is shared with on-duty crews to alert them of potential hazards upon arrival
193	we can increase responses and/or stage until the scene has been secured.
195	We look at the information that comes in. Such as drug information. Then the Chief will put out a memo from his office stating the facts in regards to new street drugs and the affects.
196	Again, using info to brief personnel on hazards, potential threats or persons/activity to watch for.
197	Role it into training and preplanning. Possibly equipment purchases.
199	At present, very rarely due to historical issues.
201	Not widely used yet.
210	not used
213	Intel deemed pertinent to the general membership will be passed down to the Company Officers by the BC on a CC.
215	Planning for major public events, of routine assessment and response to the community
216	Planning related to training, staffing requirements or standard communications.
217	Use the information as part of the morning briefing
224	situational awareness

227	For both short 24 hour operational plans and Long 7 day operational periods
232	Advisory
233	everything current is with and from local PD and SO but they dont receive anything either
239	by informing each Senior rank coming on duty for briefing of squads.
243	Most depts. are familiar and comfortable with daily SOG's, modifications may need to be made to address specific threats
252	Unknown by myself
253	Not sure
255	We infrequently act on information received. This is dependent on the type and credibility of the information.
256	Operational Updates and effectiveness
260	station and manpower placements, public education
262	Updates are made constantly as intelligence changes
267	I have no idea
271	When it involves issues we will alter our response and or handling of alarms
273	Do not receive any at the moment. But it might indicate staffing levels, staff loading in certain areas, increase or decrease depending on the situation to protect staff and yet respond if there were an incident. Be on the lookout for suspicious activity more so.
280	We utilize the information during special events to better protect our members and the public. For day-to-day ops we analyze the information as it pertains directly with our mission.
279	.
285	no
286	Distributes the information on an as needed basis taking into account reliability of the information and the sensitivity.
291	Depending on the threat or type of intelligence received, staffing levels or run procedures may be modified, specialized equipment may be added to the truck or chiefs vehicles. regional response plans or IAP's may be established, departmental SOPs may be established for specific needs based off intelligence reports
294	We use it to inform our chief officers about what illegal activities are of concern to our operations. The operational chief officers (Battalion Chiefs) will share that information to the company officers (Captains and Lieutenants) as needed for their safety.
297	It doesn't.
298	Our department often will use information/intelligence to facilitate EMS stand-by for high risk law enforcement activities - such as warrant searches. This awareness allows our personnel to stage close to an incident scene, don our tactical (ballistic) gear, and ensure that we have a proactive plan for the mitigation of the incident scene. Without this advanced notification, we find ourselves reacting to a situation with a delayed response, lack of PPE, and lack of awareness of the incident risks.
300	No.
302	it is used as a heads up
303	We don't receive enough intelligence to use during our daily operations.
306	If received, up staffing or discussion with mutual aid regarding response or automatic response.
312	see above
316	We don't receive any for LE
323	Intelligence drives vigilance as to what additional dangers that emergency responders my recognize and act accordingly.
328	In the current Covid-19 instance, we are adjusting county staffing through mutual aid to ensure all fire departments maintain critical staffing levels.
336	Information regarding potential events may alter staffing needs, more staffing available in certain locations. Equipment dissemination for specific needs, call-back of specially trained personnel i.e. hazardous materials technicians or structural collapse technicians.
339	When responding to incidents, location of hazardous materials important, in case HazMat is released. Type and amount of HazMat on highways are varied, but fixed sites do not change their quantity often.
340	Unfortunately we receive little intelligence.

Field summary for Q13

What type of intelligence is required for strategic decision-making?

Answer	Count	Percentage
Answer	113	34.98%
No answer	6	1.86%
Not completed or Not displayed	204	63.16%

ID	Response
1	Hard to say when you don't know what types are out there. I am in rural america--we don't get in on information like our big-city brothers do.
3	Information on potential credible threats to first responders involving target hazards. Information on potential locations of high risk target hazards to first responders. Information on up and coming groups who may target first responders.
4	threat assessment realistic, effects Purchasing, staffing
5	Known potential targets nearby.
7	Anything that effects our primary and secondary responses.
10	None
11	Any expected threat or perceived threat. This allows for adequate staffing, especially during a high profile special event.
13	yes if effects resources
17	Potential for extraordinary responses
21	Threat assessments that will affect us locally.
22	Good collaboration between fire & law with credible source information.
23	Thorough understanding of threats that could impact services. Swatting, Doxing, Denial of Service events, etc.
25	We would need very forward looking intelligence, and again, context. Emerging threats would need to be identified along with potential actions which could then be used to strategically plan.
28	National/regional trends.
29	We need to understand how the future might affect us. For instance, the COVID19 issue was not on our radar at all and we just updated our strategic plan.
31	Threat assessment data.
32	Trends
33	Any intelligence that involves safety concerns to responders or interruption of critical infrastructure.
34	Readies personnel for the future, either through equipment preparations, safety awareness and what resources might be needed.
40	Resources available at the state and federal level, including actual arrival times
42	Cyber threats to our IT system. I'm not sure...
41	Growth, threats, upcoming special events (concerts, etc.)
44	Threat level, impacts, crowd size, anticipated outcomes.
45	This can be used to guide short and long term plans for the department, as well as, information per call. For instance, dangerous entry.
48	relevant prediction and modeling
54	Trends. Critical infrastructure analysis.
56	the std who what where when and why
61	Any and all
62	Big picture changes in criminal / terrorist methods of operation that may drive FDs to purchase new, improved equipment, PPE, training to deal with these new TTPs
71	facts, up to date info, plans that are in place, so that you do not interfere with or conflict
72	community target hazards, threats, or vulnerabilities. Probably other information as well, but I haven't thought through all of the implications of this.
75	Chief, please consider providing a figure showing the relationship between strategic, operational, and tactical decision-making, supported by an accepted source. Perhaps this belongs in an early chapter like your lit review. There is a need for this because much business literature places tactical between strategic and operational, whereas fire service literature places operational in the middle. Strategic decisions require operational and tactical decision-making intel, plus intel required for longer term planning. Examples of intel required for strategic decision-making

	include threats used overseas, the context in which those threats exist, and analysis of the likelihood of each threat being used in the homeland. Typically technologies, tactics, techniques, and procedures spread globally when context and resources allow. Some types of adversarial attacks widely used overseas have not been used in the U.S. even though the necessary resources are widespread; this may be due to different contexts. Enough said on that; this isn't a how-to terror manual. Analysis of evolving demographics and emerging threats allow strategic decision-making.
79	?
87	Type of threat or issue and how it can effect the fire department operations.
91	Issues that impact the fire service and/or our operational area
93	Timeliness, impact, likelihood.
96	Emerging threats 6-12 months out
97	High level, vetted credible intel from law enforcement. Threat indicator intel to assist in supporting response planning needs.
98	Any info that could impact our operations by creating safety concerns.
100	Long-term and consistent threats that may exist. Special situation forecasting.
103	Intel that identifies potential threats which are not immediate but have a likelihood of occurring.
105	type of threat, threat potential, staffing and resources availability, updated weather conditions (especially out here in California) and communications
106	Long term trends or threats
107	Depends on what the decisions are concerning. This would be easier to answer if we knew what information we currently don't have but could have. We prepare based on what we think could reasonably happen in our communities. Since we currently operate without intel, we are not aware of what information we are missing. An intel brief on the types of info available would help us identify knowledge/awareness gaps so we can assess what info we need access to on a more regular basis.
110	We need to be on the same page s law enforcement
113	I think the best answer for this would be the threat spectrum and the general threat assessments that are completed by our local, state, and federal partners. It helps guide where training and equipment needs to be focused, especially in our special operations fields such as Haz Mat, the Fire Marshalls Office, and the bomb techs.
115	Depends on the intelligence received. May require the ordering of supplies or equipment.
117	higher level and more critical
118	I don't know
121	Threats to large gatherings or property. Types of threats.
127	Short term planning the most important information would be (commercial) building layouts, hazard classifications, processes preformed at an individual building. Residential structures would include period of time the structure was built, additions to the building, previous fire history. All together the utilities infrastructure is key to any of the short term events. Long term planning would include utilities available, building type, history of the building and or area. Knowing how old your municipal water system is, main size, testing cycle are all important factors. Run volume, types of calls, companies potentially moving into the district, age of the members on your department and fleet are things that need to be considered in the forecasting of budgets for needs of the department.
134	Trends in the community and/or region that could have substantial impact in the present or future deployment of first responders
135	None as of now.
138	Any information received would be evaluated.
143	Just that intelligence and not information, Ground truth and work with facts not rumors, hints of or whatever.
145	Anything that would affect special events, our specialty teams, such as haz-mat, TRT, or our EMA personnel etc.
149	Crime, drug activity, known or suspected threats, and anything that may threaten our members on duty or create resource demands (incidents) to the department.
155	The emphasis right now is on mass casualty incidents - primarily mass shootings, and very little is ever known about a shooter until they open fire. We need to get back to the terrorism lessons learned after 9-11 because we have a whole different generation of officers who may or may not have even been in the fire service 19 years ago.
160	Threat analysis for area
161	High-level briefings of world events and how they might impact us.
163	Who, what, where, when, how. What is perceived as coming
165	Anything that could give advanced info for the occupancies that we may be entering.
166	Trends being seen around the county.
173	Any information that may require an agency to supple resources that are outside of their

	normal daily operation.
177	real time, reliable data
178	all the "W's who what when where
181	Intelligence briefings can benefit us in conducting a risk assessment and formulate plans to deal with those risks.
190	Size and nature of threat.
192	Any and all information to protect crews for future
193	Intelligence that has been verified through ARIC or another credible source.
195	All intelligence is required so that we can keep our men/women safe on the streets.
196	Current threats and hazards, future threats and hazards, trends in particular populations.
197	Trends mainly. Long term and short trends in risk and hazards seen across the nation and world.
199	Very little. Again, same issue.
201	High level networking
210	economic forecasting
213	Large scale protests or attacks on critical infrastructure/freeways, etc.
216	Any intelligence that may impact normal operations or has potential to stress resource capability.
217	Trends/ up to date information
224	trend analysis, and major threat vectors
227	Expected target, anticipated victim numbers, methods used, reliability of intelligence source
232	Anything that impacts operations.
233	same as above
239	Exposure to Hazards,Necessity for evacuation,decision as to methods/tactics to be deployed.
243	Typical known threats should be addressed thru SOG's, operational bulletins etc. specific, new or regional threats may require temporary changes to those responses
252	Unknown by myself
253	Not sure
255	Civil unrest. Planned large-scale protect gatherings. High credibility threats to infrastructure/population bases.
256	Current threats Potential Threats Impacts to public safety partners that may change our operations. May impact capital purchases
260	incident numbers, population
262	Overall SA to mitigate risk and take measures where appropriate with organizational resources.
267	I have no idea
271	Something that has long term effects
273	Locations, type of threats or activity, magnitude so-as stocking of certain response equipment could be evaluated, etc.
280	National and local threats as it pertains to our community.
279	.
285	nothing at this time.
286	timely, accurate, intelligence that affects short and long time operations
291	We need to know WHAT, WHEN, WHERE and HOW to mitigate it, and WHO do we call for specific needs or resources
294	For the short team what is required are the basic "who-what-where-when-why-how" - I think this will inform our basic, day-to-day operations. From a long-term standpoint, I would love to know the data/statistics regarding known trends in our jurisdiction/region. That will help us identify gaps in our deployment and equipment that could be filled to keep our rank and file safe.
297	Long-range risk factors, trends in activities, Courses of Actions that may affect the strategic plan.
298	Ideally, levels of risk would be directly related to deployment of additional resources. Fire Departments do this now in response to fire alarms or incident types. They send the appropriate number and type of resources to an incident based upon the risk of the

	incident. A warrant search with known fellons poses a different risk from a high school student experimenting with a backyard Butane Hash Oil (BHO) lab. Levels of risk could be the triggers for information distribution.
300	Any relevant information is shared as its received via task force meetings and network information sharing.
302	Potential treats in the area
303	Potential terrorist activity; active shooter threats
306	Threats, gatherings, protests
312	location hx, contaminated scenes, threat awareness
316	Local threats and domestic potential that could hamper our ability to provide service.
323	Who, What, Where, & How
328	Policy decsions that are being directed at our agency that we have little to no input in.
336	Pre-plan of the specific target or threat. Background information regarding threat.
339	If any military haz mat is moving through area on highways.
340	information on emerging and immediate threats.

Field summary for Q14

What type of intelligence is requried for operational decision-making?

Answer	Count	Percentage
Answer	113	34.98%
No answer	6	1.86%
Not completed or Not displayed	204	63.16%

ID	Response
1	Hard to say. You need to ask a different question first: "do you know what kinds of intelligence is available" first.
3	Information on potential credible threats to first responders involving target hazards. Information on potential locations of high risk target hazards to first responders.
4	threat assessment realistic, effects Purchasing, staffing
5	Are normal FD operations at risk?
7	Anything that effects our primary and secondary responses.
10	The location, severity, and the basis of why the intelligence was developed in the first place.
11	Any expected threat or perceived threat.
13	current conditions
17	Situational and identified hazards
21	Threats that may affect local operations.
22	Same with common communications.
23	Current events and trending threats, etc.
25	This would need to be contemporary threat analysis and immediate actions.
28	Specific threats.
29	We need actionable items for every day use. For instance, we needed to be aware of the COVID impact so we could have better prepared.
31	Real time data related to threat potential
32	Timely and actionable.
33	This would be limited to intelligence that would limit operational ability or decrease staffing models.
34	Readies personnel for the future, either through equipment preparations, safety awareness and what resources might be needed.
40	pre-incident information to be utilized in a local, unified command setting
42	Is something going on in town right now, give us a heads-up. Is something threatened for the day that might require more than our usual fire/EMS resources.
41	unsure
44	size of event, layout, on site resources, outside influences, etc.
45	Weapons on site; suspected cell information.
48	GIS mapping - plume data
54	Impairments or potential impairments of infrastructure. Threats to workforce. Limits on support. Time delays in support.
56	sa
61	Any and All
62	Info that indicates a real threat/situation in the immediate region that again would drive some sort of operational response or change in normal procedures.
71	facts
72	specific risks, threats, and methods
75	Intel that allows short-term planning, such as how to prioritize training and equipment acquisition, supports operational decision-making. Operational decision-makers also need tactical intel.
79	Real time information.
87	Potential threats, changes to current threat levels, and nationwide decisions.
91	Issues that impact the fire service and/or our operational area
93	See above
96	Emerging threats 1-6 months out
97	High level, vetted credible intel from law enforcement. Threat indicator intel to assist in response planning.
98	Any info that could impact our operations by creating safety concerns.

100	Training/certification/education levels. Special team requirements, daily crew status.
103	Immediate threat, means of operation, telltale signs, past history of similar attacks, players
105	potential for threat on life, property and infrastructure, resource availability and reflex time, incident type and location, weather and fuel type
106	Timelines
107	Same answer as for strategic decisions. An intel brief would help us assess our gaps so we can identify which intel is useful.
110	Threats so the firefighters can be protected
113	General safety and awareness of threats to the region.
115	Security of stations and resources.
117	higher level and more critical
118	I don't know
121	Same as above.
127	Structure type, hazard class occupancy, utilities infrastructure, weather, and experience level of your crew along with limitations of your equipment are factors that effect the outcome of an event.
134	Current situations that warrant immediate changes to response patterns or staffing and equipping of responders
135	None as of now.
138	Any information received would be evaluated.But safety & security information is needed.
143	Intelligence we can work up and create smart objectives to train readiness and awareness for and build a tangible response to.
145	Same as above
149	Crime, drug activity, known or suspected threats, and anything that may threaten our members on duty or create resource demands (incidents) to the department.
155	Intelligence is only valuable if its actionable. The fire service, like law enforcement can be better prepared the more advance the notice AND the more specific the threat.
160	Threat in area
161	Specific threat information.
163	what, where, when, how
165	Anything that would lead our crews to wear the appropriate PPE before arriving on scene.
166	Specific hazards to pre-plan needed resources for response and mitigation.
173	Any information that may require an agency to supple resources that are outside of their normal daily operation.
177	real time, reliable data from the troops on the ground
178	same as above
181	Define specific needs required of the fire service. Can an individual department adequately meet those needs or will this be a coordinated regional effort?
190	Personnel allocations.
192	Any and all information to protect crews during their tour of duty
193	Intelligence that has been passed on from our LE, Intelligence that has been verified through ARIC or another credible source.
195	Again all intelligence is good for operational decision making.
196	Targets, specific hazards, availability of special resources.
197	Any information that will curb putting Firefighters and or the public at undue risk. Bulletins and Advisories.
199	n/a
201	enemy tactics and procedures, current threats
210	property-specific information and information about incidents of national significance
213	Number of individuals, type of materials involved or presence of a larger overarching operation (our needs dovetailed into their operation, etc.).
216	Advanced intelligence for potential impacts to operational planning regarding terrorism or other security related events.
217	See above
224	direct threat
227	Expected when, how and where event may take place
232	Anything that impacts operations.
233	same as above
239	Medical IMT awareness.Power energy supplies operational or down.Access to areas.Road way conditions.Nursing homes/Hospitals that are exposed.Aditional resourses for planning
243	New or evolving info.
252	Unknown by myself
253	Not sure
255	Law enforcement partners operational plans.
256	Current threats

	Potential Threats Impacts to public safety partners that may change our operations.
260	type of structures, number of structures in an area. Population in an area
262	Information on extremist groups in the region and any plans that may impact operations
267	I have no idea
271	Anything can will effect our ability to handle and mitigate emergencies
273	Suspicion of secondary targets, multiple targets, group or individual, type of attack, organized or "pop-up."
280	The typical information and intelligence that we receive from our fusion center is adequate for our use. For larger events in our community we are looking for specific threats or other actors that could impact the event.
279	.
285	LEO information.
286	More specific to shorter operational periods
291	What is the Long term effect, what is the Cost to be expected and will there be cost recovery or assistance
294	See the question immediately above.
297	More day-to-day type. Movements of adversaries, BOLO reports that should be shared, trends in gang and drug activity.
298	I am not sure that I will differentiate between operational and tactical decision-making. I will revert back to the who, what, when, where statement shared above, but I might add, "how". Fire departments often operate in two modes - One - where we have seen the problem before, and we have street level experience with a history of successful mitigation (Using recognition primed decision-making). This is typically an event that we can act fast on and employ established procedures to safely mitigate the event. The second mode is used when we are not sure of the situation, we have little to no experience dealing with it before, we do not understand risk, we do not know how to best resolve the problem, and we often need to reach out to a Subject Matter Expert (SME) for outside advice. Moving forward, if Fire Department personnel were exposed to increased information/intelligence sharing, the need for an outside SME may be reduced, because the operational actions have now transitioned into the RPDM category described above, because we have been here before, and we can act. There is risk associated with the category where we have no operational experience. This risk, coupled with the lack of discretionary time (See Gordon Graham) - is a recipe for failure, injury, or death.
300	Any relevant information that will enhance our response capabilities.
302	Potential treats in the area, as well as type of threat
303	Active shooter threats, daily school issues.
306	Threats, gatherings, protests
312	see above, go - no go decision making, risk management
316	Threat assessment, intel on protests, even cyber threats can impact our ability to respond.
323	Who, What, Where, Why, & How
328	Internally, operational staffing, apparatus availability, etc.
336	Incident specific information. Potential of the single incident escalating, threat to responders.
339	Type and quantity of hazardous materials.
340	Good question - anything would be nice since we get noting.

Field summary for Q15

What type of intelligence is required for tactical decision-making?

Answer	Count	Percentage
Answer	113	34.98%
No answer	6	1.86%
Not completed or Not displayed	204	63.16%

ID	Response
1	Again, your assumption that we know what is available is a bit over the top.
3	Information on known or credible hazards to which first responders will respond.
4	threat assessment realistic, effects Purchasing, staffing
5	Do we need to have another plan (or two)?
7	Anything that effects our primary and secondary responses.
10	Violent vs. Non-Violent intent towards first responders.
11	Any expected threat or perceived threat
13	limitations due to secondary events
17	SAA
21	The company officers need to know of local threats so that they may access problems that they may run into. Possible terrorist activity. Bomb makers. Emerging threats.
22	Same
23	Immediate known threats o personnel safety, such as areas of civil unrest, discovery of certain chemicals or explosives within a building, etc.
25	Action planning to include means of securing resources to execute the plan.
28	Specific threats or actual events.
29	We occasionally get some intelligence from local PD when on scenes. ie active shooter, bomb threat, fire with standoff
31	Real time data related to threat potential
32	Timely and actionable.
33	Anything that would prohibit all of the tools in the tool box from being considered as a mitigation to the problem.
34	Readies personnel for the future, either through equipment preparations, safety awareness and what resources might be needed.
40	Securing additional training to address targeted threats
42	I'm not sure.... as we are responding it would be good to get maximum info on what we are running into -- safe zones for staging.
41	threats, potential threats, how it may impact operation readiness
44	All of the above.
45	Weapons on site; suspected cell information.
48	local response trending
54	Same as operational DM.
56	sa
61	Any and All
62	Specific credible info that indicates a direct threat/concern/situation that would specifically impact my department
71	facts
72	specific risks, threats, and methods
75	Intel with specific indicators of WMD or drug labs, warnings about secondary devices, toxindromes, emerging threats (any realm including cyber and public health), vertical terror, complex coordinated attacks, violent intruders, etc. is most useful for tactical decision-making. Rank and file people need to know what threats are out there, including tactics used overseas that will eventually be used here, and especially what is already being used or actively threatened in the homeland.
79	None
87	Potential threats, changes to current threat level and reasons why.
91	Issues that impact the fire service and/or our operational area
93	See above
96	Imminent threats and awareness of critical infrastructure in the area of operation.

97	More specific credible intel focused on a defined area of concern vs general awareness.
98	Any info that could impact our operations by creating safety concerns.
100	Training/ certification equipment and proper briefing for identified threats.
103	identification of an incident and then the implementation of the department's operational plan. What is missing in this questionnaire is whether we are sharing intel with law enforcement. We are in people's homes and businesses and using our senses, we observe the environment. We can gather important intelligence but do we share it? PD needs to know that we can be active participants in the intel community, yet we fail to let PD know what we can offer.
105	known threat to life, location of incident and it's potential, natural barriers
106	Safety consideration, expectations of work to be done
107	Same answer as for strategic decisions. An intel brief would help us assess our gaps so we can identify which intel is useful.
110	Threats
113	General safety and awareness of threats to the region.
115	Depends on the nature of the intelligence and the incident.
117	higher level and more critical
118	I don't know
121	Same.
127	Origin of emergency, additional manpower and equipment resources available, life safety of occupants and of fire personnel. Type of emergency and the ability and training level of the crew responding to mitigate the hazard.
134	Immediate threats to security, community impact that will require rapid changes to deployment and normal operations
135	Not sure.
138	Any information received would be evaluated.But safety & security information is needed.
143	If we know how it is made we know how it will come down so give us the information needed to be able to go after something intelligently and not just shooting from the hip.
145	any intel that would affect the safety of our members or the people of our community. Weather, terrorism, severe weather, viruses etc.
149	More detialed inteligence on the tactical incident at hand. This has largely been done through on scene command officers between PD and FD.
155	At the tactical level it would great if law enforcement understood what a Unified Command actually consists of and looks like. As recent as the Las Vegas mass shootings, while Fire tried to set up a Joint Command Post to initiate Unified Command, I am told the police had no less than 5 CPs and not even a single IC on their end.
160	Threat in area
161	Specific threat information.
163	what, where, when, how
165	Scene safety
166	Specific location or hazard needs to minimize risk and proper PPE
173	Any information that may require an agency to supple resources that are outside of their normal daily operation.
177	good feedback from troops in the trenches
178	same
181	Resources needed to care out operational goals.
190	Resource allocations.
192	Any and all information to protect crews while responding to alarms
193	Type of threat that is involved in the intelligence.
195	Again all intelligence is good for operational decision making.
196	Targets, specific hazards, availability of special resources.
197	Same
199	n/a I'll just throw this in here in case there isn't a place to allow the exchange of contact information. I am the Fire Service Intelligence Analyst for Northern Virginia. I am the Fire Liaison to 12 federal and local fire departments covering approximately 5,000 personnel. You are welcome to contact me (initially via email) and we can discuss in detail if you like. michael.taylor@fairfaxcounty.gov
201	Precursors, pre attack indicators and current threats
210	Property and incident specific data
213	Materials involved, type of action, etc.

216	Direct and timely information that may affect incident response capability or current incident management.
217	See above
224	direct threat
227	The what may be used and the how it maybe carried out, along with the where
232	Anything that impacts operations.
233	same as above. To be honest we (Police, Fire and EMS)are kinda in a pre - 9/11 status for intelligence sharing in in our community and county.
239	Expected future Operational planning for command in deciding deployment ,when to extend or exit the specific strategies should the hazard extend beyond control.
243	See above
252	Unkown
253	Not sure
255	Law enforcement partners operational plans. Common operating pictures.
256	Current threats Potential Threats Impacts to public safety partners that may change our operations.
260	haz-mat, building construction features, fire loads
262	Names/photos/identifiers of suspects or POI
267	I have no idea
271	Anything can will effect our ability to handle and mitigate emergencies
273	All the above leads to these decisions.
280	The typical information and intelligence that we receive from our fusion center is adequate for our use. For larger events in our community we are looking for specific threats or other actors that could impact the event.
279	.
285	LEO information
286	Immediate threat
291	An analysis of the ongoing operation, and the effectiveness of our efforts, and proficiency of our operations, are their any changes or new information that changes our game plan
294	See two questions above.
297	Day to day type intelligence, what has happened in the last 72 hours that is affecting the next 24. Shootings, robberies, drug shortages, arson, bomb scares are examples.
298	See my operational decision-making response above.
300	Any relevant information that will enhance our response capabilities.
302	Potential treats in the area, as well as type of threat
303	Specific threat locations.
306	Threats, gatherings, protests
312	deployment choices, crew size, resource type, law presence
316	same as above.
323	Who, What, Where, & How
328	Level of individual training and skills sets that available for the shift that's on. (We're a small rural department, so everyday is different)
336	Specific information to premises involved, material involved, and protective measures
339	Type and quantity of hazardous materials.
340	Daily intelligence briefs on local and immediate threats.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Carter, David. *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies.*, 2nd ed. Washington, DC: Department of Justice, 2004. https://it.ojp.gov/documents/d/e050919201-IntelGuide_web.pdf.

Carter, David, Steve Chermak, Jeremy Carter, Jack Drew. *Understanding Law Enforcement Intelligence Processes: Report to the Office of University Programs, Science and Technology Directorate*. College Park, MD: National Consortium for the Study of Terrorism and Responses to Terrorism, 2014. https://www.start.umd.edu/pubs/START_UnderstandingLawEnforcementIntelligenceProcesses_July2014.pdf.

Castro Garcia, Andres de, Florina Cristiana Matei, and Thomas C. Bruneau. "Combatting Terrorism through Fusion Centers: Useful Lessons from Other Experiences?" *International Journal of Intelligence and CounterIntelligence* 30, no. 4 (2017): 723–42. https://doi.org/10.1080/08850607.2017.1297119.

Center for Development of Security Excellence. *Marking Classified Information Job Aid*. Linthicum, MD: Defense Security Service, 2017.

Central Intelligence Agency. "INTelligence: Signals Intelligence." Last updated April 30, 2013. https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/intelligence-signals-intelligence-1.html.

Chapman, Robert, Shelly Baker, Veh Bezdikian, Pam Cammarata, Debra Cohen, Nancy Leach, Amy Schapiro, Matthew Scheider, Rita Varano, and Rachel Boba. "Local Law Enforcement Responds to Terrorism Lessons in Prevention and Preparedness." *COPS Innovations*. Last updated April 5, 2002. https://cops.usdoj.gov/RIC/Publications/cops-w0125-pub.pdf.

Cloud, Rosemary R. "Future Role of Fire Service in Homeland Security." Master's thesis, Naval Postgraduate School, 2008. http://hdl.handle.net/10945/3935.

Covert, Robert M., II. "Evolving the Local Fire Service Intelligence Enterprise in New York State: Implementing a Threat Liaison Officer Program." Master's thesis, Naval Postgraduate School, 2012. http://hdl.handle.net/10945/27813.

Dahl, Erik J. *Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond*. Washington, DC: Georgetown University Press, 2013.

Department of Homeland Security. *2013 National Network of Fusion Centers Final Report*. Washington, DC: Department of Homeland Security, 2014. https://www.dhs.gov/sites/default/files/publications/2013%20National%20Network%20of%20Fusion%20Centers%20Final%20Report.pdf.

———. *2015 National Network of Fusion Centers Final Report*. Washington, DC: Department of Homeland Security, 2016. https://www.archives.gov/files/isoo/oversight-groups/sltps-pac/national-network-of-fusion-centers-2015.pdf.

———. *Fire Service Intelligence Enterprise: Concept Plan*. Washington, DC: Department of Homeland Security, August 2009.

———. *Safeguarding Classified and Sensitive but Unclassified Information: Reference Booklet for State, Local, Tribal and Private Sector Programs*. Washington, DC: Department of Homeland Security, 2005. https://homeport.uscg.mil/Lists/Content/Attachments/2110/SecurityReferenceStateLocalTribalPrivateSector.pdf.

Department of Homeland Security and Department of Justice. "Case Study: Crime Prevention and Information Center." Washington, DC: National Criminal Intelligence Resource Center, November 2007.

———. "Fire Service Information Sharing Workshop: Fusion Center Resource." Washington, DC: National Criminal Intelligence Resource Center, September 2010.

Department of Justice. "Fire Service Integration for Fusion Centers: An Appendix to the *Baseline Capabilities for State and Major Urban Area Fusion Centers*." Washington, DC: Department of Justice, 2010.

Department of Justice and Department of Homeland Security. *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*. Washington, DC: Department of Justice and Department of Homeland Security, 2006. https://www.it.ojp.gov/documents/d/fusion_center_guidelines.pdf.

District of Columbia Homeland Security and Emergency Management Agency and National Capital Region Threat Intelligence Consortium. *Emerging Incident Playbook*. Shawnee, KS: Guest Communications Corporation, 2019.

Executive Office of the President. *National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing*. Washington, DC: White House, 2007. https://apps.dtic.mil/dtic/tr/fulltext/u2/a473664.pdf.

German, Michael. *What's Wrong with Fusion Centers*. New York: American Civil Liberties Union, 2007. https://www.aclu.org/files/pdfs/privacy/fusioncenter_20071212.pdf.

Goldstein, Scott E. "Comparative Analysis of Fusion Center Outreach to Fire and EMS Agencies." Master's thesis, Naval Postgraduate School, 2015. http://hdl.handle.net/10945/47952.

Gonzales, Rebecca L. “Transforming Executive Fire Officers: A Paradigm Shift to Meet the Intelligence Needs of the 21st Century Fire Service.” Master’s thesis, Naval Postgraduate School, 2010. http://hdl.handle.net/10945/5157.

Harrison, Kevin. “Improving Information Sharing in the NYC Emergency Response Community.” Master’s thesis, Naval Postgraduate School, 2018. https://www.hsdl.org/?view&did=814723.

Heirston, Bryan. “Terrorism Prevention and Firefighters: Where Are the Information-Sharing Boundaries?” Master’s thesis, Naval Postgraduate School, 2009. https://calhoun.nps.edu/handle/10945/4930.

Henke, Keith. “Fire Service Intel and Info Resources.” Presentation, Department of Homeland Security, November 2019.

Homeland Security Advisory Council. “Intelligence and Information Sharing Initiative: Homeland Security Intelligence & Information Fusion.” Washington, DC: Department of Homeland Security, 2005.

Interagency Threat Assessment and Coordination Group. *Intelligence Guide for First Responders*. 2nd ed. Washington, DC: Office of the Director of National Intelligence, 2011. https://permanent.access.gpo.gov/gpo12126/ITACG_Guide_for_First_Responders_2011.pdf.

International Association of Fire Chiefs. *Homeland Security: Intelligence Guide for Fire Chiefs*. Fairfax, VA: International Association of Fire Chiefs, 2012. http://the-security-institute.org/userfiles/file/IntelGuide4FireChiefs.pdf.

Johnson, Loch K., and James J. Wirtz, eds. *Intelligence: The Secret World of Spies: An Anthology*. 5th ed. New York: Oxford University Press, 2019.

Joint Chiefs of Staff. *Joint Intelligence*. JP 2-0. Washington, DC: Joint Chiefs of Staff, 2007.

Joint Counterterrorism Assessment Team. *JCAT Intelligence Guide for First Responders*. Washington, DC: Office of the Director of National Intelligence, 2015. https://www.dni.gov/nctc/jcat/jcat_ctguide/intel_guide.html.

Jurevicius, Ovidijus. “PEST & PESTEL Analysis.” Strategic Management Insight, February 13, 2013. https://www.strategicmanagementinsight.com/tools/pest-pestel-analysis.html.

Lowenthal, Mark M. *Intelligence: From Secrets to Policy*. 7th ed. Los Angeles: CQ Press, 2017.

Minks, Cody. “Hacking the Silos: Eliminating Information Barriers between Public Health and Law Enforcement.” Master’s thesis, Naval Postgraduate School, 2018. http://hdl.handle.net/10945/58345.

Monahan, Torin, and Neal A. Palmer. “The Emerging Politics of DHS Fusion Centers.” *Security Dialogue* 40, no. 6 (2009): 617–36. https://doi.org/10.1177/0967010609350314.

National Commission on Terrorist Attacks upon the United States. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*. Washington, DC: Government Printing Office, 2004. https://digital.library.unt.edu/ark:/67531/metadc123526/.

New York City Fire Department, Center for Terrorism and Disaster Preparedness. “*Watchline*: FDNY’s Flagship Intelligence Product.” Presentation, New York City Fire Department, February 8, 2018.

Office of Homeland Security. *National Strategy for Homeland Security*. Washington, DC: White House, 2002. ProQuest.

Office of the Director of National Intelligence. *2018 Information Sharing Environment*. Washington, DC: Office of the Director of National Intelligence, 2018. https://www.dni.gov/files/documents/FOIA/2018_Information_Sharing_Environment_Annual_Report.pdf.

———. *Domestic Approach to National Intelligence*. Washington, DC: Office of the Director of National Intelligence, 2016. https://www.dni.gov/files/documents/Newsroom/DomesticApproachtoNationalIntelligence.PDF.

———. “What We Do.” Accessed April 17, 2020. https://www.dni.gov/index.php/what-we-do.

Offices of the Inspectors General of the Intelligence Community, Department of Homeland Security, and Department of Justice. *Review of Domestic Sharing of Counterterrorism Information*. Washington, DC: Inspectors General of the Intelligence Community, Department of Homeland Security, and Department of Justice, March 2017. https://www.dni.gov/files/documents/Newsroom/Domestic_Sharing_Counterterrorism_Information_Report.pdf.

Peterson, Marilyn. *Intelligence-Led Policing: The New Intelligence Architecture*. NCJ 210681. Washington, DC: Bureau of Justice Assistance, 2005. https://www.ncjrs.gov/pdffiles1/bja/210681.pdf.

Pfeifer, Joseph W., Sean S. Newman, John M. Esposito, Thomas J. Currao, Timothy A. Carroll, Christopher Flatley, Christopher P. Ward, Mark A. Donohue, Michael Gomez, and Kristin Eng. *FDNY Counterterrorism and Risk Management Strategy*. Edited by Janet Kimmerly. New York: New York City Fire Department, 2011. https://www1.nyc.gov/assets/fdny/downloads/pdf/FDNY_ct_strategy_2011_12.pdf.

Regan, Priscilla M., and Torin Monahan. "Beyond Counterterrorism: Data Sharing, Privacy, and Organizational Histories of DHS Fusion Centers." *International Journal of E-Politics* 4, no. 3 (2013): 1–14. https://doi.org/10.4018/jep.2013070101.

Regan, Priscilla M., Torin Monahan, and Krista Craven. "Constructing the Suspicious: Data Production, Circulation, and Interpretation by DHS Fusion Centers." *Administration & Society* 47, no. 6 (2015): 740–62. https://doi.org/10.1177/0095399713513141.

Richardson, Thomas J. "Identifying Best Practices in the Dissemination of Intelligence to First Responders in the Fire and EMS Services." Master's thesis, Naval Postgraduate School, 2010. http://hdl.handle.net/10945/5137.

Robson, Thomas A. "A Burning Need to Know: The Use of Open Source Intelligence in the Fire Service." Master's thesis, Naval Postgraduate School, 2009. http://hdl.handle.net/10945/4913.

Russo, Joseph. "Out from Under the Rock: Improving FDNY Information Sharing." Master's thesis, Naval Postgraduate School, 2017. http://hdl.handle.net/10945/53042.

Salvatore, Shane A. "Fusion Center Challenges: Why Fusion Centers Have Failed to Meet Intelligence Sharing Expectations." Master's thesis, Naval Postgraduate School, 2018. http://hdl.handle.net/10945/58358.

Smartsheet. "The Complete Guide to Gap Analysis." Accessed February 24, 2020. https://www.smartsheet.com/gap-analysis-method-examples.

Warner, Michael. "Wanted: A Definition of 'Intelligence.'" *Studies in Intelligence* 46, no. 3 (2002).

Zegart, Amy B. *Spying Blind: The CIA, the FBI, and the Origins of 9/11*. Princeton, NJ: Princeton University Press, 2007.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California