NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

A COMPREHENSIVE FUSION LIAISON OFFICER PROGRAM: THE ARIZONA MODEL

by

William F. Wickers Jr.

March 2015

Thesis Co-Advisors: Lauren Wollman
Patrick Miller

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2015	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE
A COMPREHENSIVE FUSION LIAISON OFFICER PROGRAM: THE ARIZONA MODEL

5. FUNDING NUMBERS

6. AUTHOR(S) William F. Wickers Jr.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

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

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

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

Many of the fusion centers recognized by the U.S. Department of Homeland Security have established a liaison officer program with the intent of sharing information. In Arizona, the Arizona Counter Terrorism Information Center's Terrorism Liaison Officer (TLO) Program has become an institution that is relied upon by participant jurisdictions for intelligence and information sharing between federal, state and local governments, along with unifying critical infrastructure initiatives and responding to major events. The network provides professional and vetted-out partners throughout the public safety community to assist jurisdictions in addressing many high-risk events and incidents. In the Phoenix urban area, TLOs respond to moderate and large scenes to support incident commanders with critical infrastructure data, a law enforcement intelligence research capability and a fire/emergency medical service/hazardous materials coordination capability that did not exist prior to the TLO program's establishment. The Arizona Counter Terrorism Information Center's TLO program can serve as a model for fusion centers by demonstrating how multilayered and multijurisdictional relationships can be leveraged into a comprehensive network to address complex issues.

14. SUBJECT TERMS
fusion center, liaison officer, responder, Homeland Defense Bureau (HDB), terrorism liaison officer (TLO), Arizona Counter Terrorism Information Center (ACTIC), intelligence liaison officer (ILO)

15. NUMBER OF PAGES
97

16. PRICE CODE

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

NSN 7540-01-280-5500

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

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

A COMPREHENSIVE FUSION LIAISON OFFICER PROGRAM: THE ARIZONA MODEL

William F. Wickers Jr.
Sergeant, Phoenix Police Department
B.A., State University of New York College (Cortland), 1990
M.A., Northern Arizona University, 1999

Submitted in partial fulfillment of the
requirements for the degree of

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

from the

**NAVAL POSTGRADUATE SCHOOL
March 2015**

Author: William F. Wickers Jr.

Approved by: Lauren Wollman
Thesis Co-Advisor

Patrick Miller
Thesis Co-Advisor

Mohammed Hafez
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Many of the fusion centers recognized by the U.S. Department of Homeland Security have established a liaison officer program with the intent of sharing information. In Arizona, the Arizona Counter Terrorism Information Center's Terrorism Liaison Officer (TLO) Program has become an institution that is relied upon by participant jurisdictions for intelligence and information sharing between federal, state and local governments, along with unifying critical infrastructure initiatives and responding to major events. The network provides professional and vetted-out partners throughout the public safety community to assist jurisdictions in addressing many high-risk events and incidents. In the Phoenix urban area, TLOs respond to moderate and large scenes to support incident commanders with critical infrastructure data, a law enforcement intelligence research capability and a fire/emergency medical service/hazardous materials coordination capability that did not exist prior to the TLO program's establishment. The Arizona Counter Terrorism Information Center's TLO program can serve as a model for fusion centers by demonstrating how multilayered and multijurisdictional relationships can be leveraged into a comprehensive network to address complex issues.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACAMS	Automated Critical Asset Management System
ACTIC	Arizona Counter Terrorism Information Center
AOR	area of responsibility
AZ	Arizona
CFIX	Central Florida Information Exchange
CI	critical infrastructure
CIA	Central Intelligence Agency
CIAC	Colorado Information Analysis Center
CFR	Code of Federal Regulation
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DOD	Department of Defense
DOJ	Department of Justice
DPS	Department of Public Safety
EMS	Emergency Medical System
FBI	Federal Bureau of Investigation
FOG	Field Operations Guide
FLO	fusion liaison officer
HazMat	hazardous materials
HDB	Homeland Defense Bureau
HSPD	Homeland Security Presidential Directive
ICS	Incident Command System
IGA	inter-governmental agreement
ILO	intelligence liaison officer
IMT	Incident Management System
INTERPOL	International Criminal Police Organization
ISE	Information Sharing Environment
I&A	intelligence and analysis
JTTF	Joint Terrorism Task Force
LES	law enforcement sensitive

MOU	memorandum of understanding
NCIC	National Crime Information Center
NCRIC	Northern California Regional Intelligence Center
NDA	non-disclosure agreement
NPS	Naval Postgraduate School
OSR	on-scene response
PASS	Partners in Arizona's Safety and Security
PCII	Protected Critical Infrastructure Information
PSA	Protective Security Advisor
SBU	sensitive but unclassified
SOP	standard operating procedure
SWAT	special weapons and tactics
TEW	terrorism early warning
TLO	terrorism liaison officer
TMU	threat mitigation unit
TVA	threat and vulnerability assessment
UASI	Urban Area Security Initiative

ACKNOWLEDGMENTS

There are many people that I must thank and acknowledge for support during my participation in this venture. Thank you to the City of Phoenix and Chiefs Brunacini and Hurtt for having the foresight and initiative to unify the efforts of the fire and police departments in 2003. Thanks to Detective Todd Richard White, Commander T. J. Martin, and Lieutenant Michael DeBenedetto for the concepts and hard work it took to build a new program from scratch. It has turned into so much more than I could have ever imagined. Thanks to my friend and mentor, Captain Rickey Lee Salyers of the Phoenix Fire Department. Rick, you are the godfather of the ACTIC Fusion Liaison Officer program, and I consider myself blessed to have met and worked with you for these many years.

Thanks to Ken Ruben, Chris Sweeney, Joel Justice, and Dave Brown along with the rest of the unique and exceptional professionals of 1105 and 1106 that made my CHDS experience. God bless Mark Carr.

Thank you to FEMA and the CHDS staff for this opportunity of a lifetime. Special thanks to my thesis advisors, Lauren Wollman and Patrick Miller. Your patience paid off.

There is one person whose support was beyond any reasonable hope or expectation. To my wife, Nora, thank you for being you. For the many months I was engaged in this program, I have traveled to the four corners of this country for work and school. You have taken care of every detail and issue that our family has had. Our Madeline (11), Bridget (10), Billy (7), and Nora (3) could not have a better mother, and I can never adequately express my thanks to you for being the exceptional wife that you are. Without your constant over-watch and caretaking of every aspect of our lives, I would never have been successful in this endeavor. I must have done something spectacular in another life to have been graced with you as my partner. 138

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

Many fusion centers, as recognized by United States Department of Homeland Security (DHS), have established a liaison officer program to share information. Many fusion centers will host liaisons from their participant jurisdictions for a one-day class to instruct the liaisons on the current threat environment and further instruct them on how to send homeland security related information to the fusion center. Many times this deteriorates into a seldom used email exchange system.

Arizona's fusion center, the Arizona Counter Terrorism Information Center (ACTIC), is recognized by DHS as Arizona's only fusion center. ACTIC's participating jurisdictions send selected members of their public safety staff to be trained and equipped as liaison officers by the ACTIC. This training includes instruction in the fusion center network along with the capacities and capabilities of the Terrorism Liaison Officer (TLO) Program. Uniting these jurisdictions in a liaison officer programs that are managed at the fusion center allows jurisdictions the information, guidance, and network necessary to address many of their homeland security related needs.

In Arizona, the ACTIC's TLO Program has become an institution relied upon by participant jurisdictions for intelligence and information sharing between federal, state, and local governments along with unifying critical infrastructure initiatives and responding to major events. The network provides professional and vetted partners throughout the public safety community to assist jurisdictions in addressing many high risk events and incidents. In the Phoenix urban area, the TLOs respond to moderate and large scenes to support incident commanders with critical infrastructure data, law enforcement intelligence research capability, and a fire / emergency medical service (EMS) / hazardous materials (HazMat) coordination capability that did not exist prior to the TLO Programs' establishment.

B. RESEARCH QUESTION

How can the Arizona Counter Terrorism Information Center serve as a national model for liaison officer programs?

C. METHOD

This thesis is a case study of the ACTIC TLO Program. The case study method is defined by Yin as "an empirical inquiry about contemporary phenomenon (e.g., a 'case'), set within its real-world context—especially when the boundaries between the phenomenon and context are not clearly evident."[1]

There is limited direction from national fusion center leadership and limited consistency between liaison officer programs that have been implemented by DHS recognized fusion centers. This case study will demonstrate how a specific liaison officer program is being leveraged by a fusion center to address a majority of its basic functions through a unified and trained cadre of public safety participants called TLOs. These TLOs efforts are consolidated to support their home jurisdiction along with ACTIC's intelligence and information sharing, critical infrastructure protection and on scene response. Fusion centers can select from these compartments to build a model that meets their needs in achieving their baseline capabilities.

Baseline capabilities for fusion centers are produced to ensure that state and major urban area fusion centers are able to perform the basic functions of a fusion center. These basic functions include "…operational capabilities such as Suspicious Activity Reporting (SAR; Alerts, Warnings and Notifications; Risk Assessments; and Situational Awareness Reporting."[2] DHS and the United States Department of Justice (DOJ) conduct assessments of fusion centers to identify if they meet the baseline capability. These assessment areas are used in this thesis to demonstrate how TLOs are leveraged by the

[1] Robert K. Yin, *Applications of Case Study Research* (Thousand Oaks, CA: Sage, 2009), 18.

[2] U.S. Department of Homeland Security [DHS], and U.S. Department of Justice, Bureau of Justice Assistance, *Baseline Capabilities for State and Major Urban Area Fusion Centers: A Supplement to the Fusion Center Guidelines.* Supplement (Washington, DC: U.S. Department of Homeland Security, and Bureau of Justice Assistance, 2008), http://www.fema.gov/pdf/government/grant/2010/fy10_hsgp_fusion.pdf, 20.

ACTIC to help it achieve its baseline capabilities. Since there is a lack of direction for fusion centers concerning establishing, managing and growing liaison officer programs there is limited consistency This can be used as a model for fusion centers that need to achieve their baseline capabilities and to operate as a fusion center.

The ACTIC's TLO Program represents a federal, state, tribal, and local partner capabilities that move a fusion center from attempting to achieve a baseline capability to a mature one that addresses a majority of its baseline capabilities. This program illustrates a liaison officer format that can be used by any fusion center.

D. LITERATURE REVIEW

The 9/11 Commission report provides a number of recommendations. A significant recommendation refers to information sharing. According to the report, "Information procedures should provide incentives for sharing, to restore a better balance between security and shared knowledge."[3] The report further details issues with the "Command and Control within First Responder Agencies" and "Lack of Coordination among First Responder Agencies."[4] Furthermore, the report explains,

> The lesson of 9/11 for civilians and first responders can be stated simply: in the new age of terror, they-we are the primary targets. The losses America suffered that day demonstrated both the gravity of the terrorist threat and the commensurate need to prepare ourselves to meet it. The first responders of today live in a world transformed by the attacks on 9/11. Because no one believes that every conceivable form of attack can be prevented, civilians and first responders will again find themselves on the front lines. We must plan for that eventuality.[5]

According to the Departments of Justice and Homeland Security, fusion centers can be effective and efficient information sharing and collaboration mechanisms.[6] Lieutenant McGhee of the Aurora, Colorado Police Department addressed the collaborative effort when he said, "those working in the federal government and the

---

[3] National Commission on Terrorist Attacks upon the United States, *Final Report of the National Commission on Terrorist Attacks upon the United States* (New York: W. W. Norton, 2004), 417.

[4] Ibid., 319, 321.

[5] Ibid., 323.

[6] DHS, and DOJ Bureau of Justice Assistance, *Baseline Capabilities*, 39, 48.

intelligence community have a limited understanding of how SLTTP entities operate and what they can offer."[7] Fusion centers receive information from a variety of sources, including federal, state, and local entities, and ensure timely and relevant information is provided to the right stakeholders within their geographic area of responsibility. Lieutenant McGhee went on to say, "because of the newly created relationships between the federal government and state, local, tribal, territorial and private sector entities [SLTTP], as well as steady advancements in technology, complicated issues have arisen in gathering date."[8] Furthermore, the *Fusion Center Guidelines* describe the need for fusion centers to operate with a consistent framework acknowledging that each center will be unique.[9] The federal government uses fusion centers as the primary focal points within the state and local environments for the receipt and sharing of terrorism-related information. In addition, federal agencies provide terrorism-related information to state, local, and tribal authorities primarily through these fusion centers, which may further customize such information for dissemination to satisfy intra- or interstate needs.[10]

Fusion involves turning information and intelligence into actionable knowledge.[11] A fusion center is defined by DHS as a "collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity."[12]

Fusion centers have guidelines and baseline capabilities provided to them by the Department of Homeland Security, the Department of Justice and the Global Information

---

[7] Sam McGhee, "Impacting the Evolution of Information Sharing in the Post-9-/11 United States," *The Police Chief*, February 2015, http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display&article_id=3636&issue_id=22015

[8] Ibid.

[9] Global Justice Information Sharing Initiative, *Fusion Center Guidelines* (Washington, DC: U.S. Department of Homeland Security, and U.S. Department of Justice, 2006), https://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf, 3.

[10] U.S. Department of Justice, *Fact Sheet: 2009 National Fusion Center Conference* (Washington, DC: Federal Information & News Dispatch, Inc., 2009).

[11] Ibid., 10.

[12] U.S. Department of Homeland Security, *National Network of Fusion Centers Fact Sheet*, August 6, 2014, http://www.dhs.gov/files/programs/gc_1296484657738.shtm

Sharing Initiative. These guidelines provide them the basic direction they need to succeed. The capabilities in the guidelines include coordination, risk assessments, suspicious activity reporting, alerts and warnings, situational awareness and coordination with response and recovery officials.[13]

The U.S. Department of Homeland Security's *Fusion Center Guidelines* describes the need for fusion centers to operate with a consistent framework acknowledging that each center will be unique.[14] The federal government uses fusion centers as the primary focal points within the state and local environment for the receipt and sharing of terrorism-related information. Federal agencies provide terrorism-related information to state, local, and tribal authorities primarily through these fusion centers, which may further customize such information for dissemination to satisfy intra- or interstate needs.[15]

In September of 2011, Secretary Janet Napolitano explained,

> We now have the 72 fusion centers. We've moved our own analysts into the fusion centers themselves so that they can help not only with the gathering and receipt of information but with the analysis of information. And that itself is helpful. If you look at Zazi and you look at Faisal Shahzad and you look at Pauline-Ramirez, who was connected with Jihad Jane, in all of those cases you would see fusion center activity that was very, very helpful. And indeed, these past three days and ongoing, with the ongoing threat that has been described to you, fusion centers are active in that as well.[16]

Lieutenant McGhee recently commented on the national network of fusion centers:

> Today fusion centers range in size and capability, but the 78 centers across the United States compose the National Network of Fusion Centers [NNFC or the National Network], which has become a powerful entity

[13] Global Justice Information Sharing Initiative, *Fusion Center Guidelines*; DHS, and DOJ Bureau of Justice Assistance, *Baseline Capabilities*.

[14] Ibid.

[15] Ibid.

[16] "Remarks by Homeland Security Secretary Janet Napolitano to the National Fusion Center Conference in Kansas City, Mo. on March 11, 2009," March 13, 2009, U.S. Department of Homeland Security, http://www.dhs.gov/news/2009/03/13/napolitanos-remarks-national-fusion-center-conference

> connecting essential partners from state and local law enforcement agencies, federal partners, fire and emergency medical services, public health departments, emergency management offices, and private sector entities.[17]

U.S. DHS has placed intelligence and analysis personnel at fusion centers. The Federal Fusion Center Initiative has deployed hundreds of DHS and Federal Bureau of Investigation (FBI) personnel to assist fusion centers in blending law enforcement and intelligence information analyses along with coordinating security measures to reduce threats in local communities. The assignment of these federal personnel to fusion centers helps to integrate capabilities by co-locating resources.[18] When a local incident generates an impact nationally, it becomes necessary to communicate across many levels of government. An established network is beneficial to communicate seamlessly across intergovernmental lines. Fusion centers provide a standardized relationship between their constituent jurisdictions and the Department of Homeland Security. This can be important in day-to-day operations and can be especially important when a communication loop needs to be established between DHS and the state, county or local police chief, emergency manager, fire chief, or public health officer for an expanding incident. This institutionalized relationship is also important when DHS has information about indicators, watches, and warnings of hazards that it needs to get into the hands of its state and local partners.[19] The TLO network can institutionalize the information sharing environments communication loop between constituent members of the fusion center network, the fusion centers, and their DHS partners.[20] In addition, repetitive use of this communication loop creates a standardized information sharing environment. However, Michael Price from the Brennen Center for Justice cautions, "… the standards

---

[17] McGhee, "Impacting the Evolution of Information Sharing."

[18] Program Manager, Information Sharing Environment, *Information Sharing Environment, Annual Report to Congress*, June 2011, http://www.ise.gov/sites/default/files/ISE_Annual_Report_to_Congress_2011.pdf

[19] Office of Intelligence and Analysis, *Office of Intelligence and Analysis Strategic Plan Fiscal Year 2011–Fiscal Year 2018* (Washington, DC: U.S. Department of Homeland Security, 2011), http://www.dhs.gov/xlibrary/assets/ia-fy2011-fy2018-strategic-plan.pdf, 9–11

[20] U.S. Department of Homeland Security, *Information Sharing Strategy* (Washington, DC: U.S. Department of Homeland Security, 2008), https://www.dhs.gov/xlibrary/assets/dhs_information_sharing_strategy.pdf, 6.

for collecting and disseminating that information are so lax and variable that they not only endanger civil liberties, but risk hobbling the entire enterprise."[21]

The Department of Homeland Security encourages fusion centers to create TLO programs. In 2010, 23 percent of the 72 fusion centers in the U.S. had Terrorism, Intelligence, or Fusion Liaison Officer Program.[22] In March of 2008, the ACTIC was awarded the National Fusion Center Conference Partners' Award of Excellence in recognition of achievements in 2007—for its outstanding Terrorism Liaison Officer Program and overall contribution to the national network of fusion centers.[23]

The *Fusion Center Guidelines* describe what needs to be addressed by fusion centers but does not provide direction concerning the personnel, network, or capabilities that are necessary to do this work. The personnel and networks that the information sharing environment requires are present across the federalist system including federal, state, regional, and local partners. The capability to unite these personnel and networks is fusion. Some partners may operate seamlessly while others may never have contact until there is an emergency. In other words, the gap may not be between the fusion center and their federal partners. The gap may be between the federal partners, fusion centers, and their counties and cities.

Director of National Intelligence James Clapper stated,

> Fusion centers, which I think are a great step forward, something that didn't exist 10 years ago and there are now some 72 of them. And very candidly, some are much better than others. I've visited some that I think are extremely capable. There is a federal nexus to ensure that

[21] Michael Price, *National Security and Local Police*, Brennan Center For Justice, 2013, http://www.brennancenter.org/sites/default/files/publications/NationalSecurity_LocalPolice_web.pdf, 23.

[22] 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), https://www.hsdl.org/?view&did=16026

[23] National Fusion Center Partners, *Award of Excellence* (Washington, DC: National Fusion Center Partners, 2008).

> appropriately designated information is shared quickly with state and local officials."[24]

TLO programs like the ones in Arizona and Colorado are important to their fusion center's success. In 2010, the CIAC was named Fusion Center of the Year. The center's Director, Major Steve Garcia said "at the heart of CIAC is the Terrorism Liaison Officer program."[25]

Benefits of a fusion liaison officer may include improved crime and terrorism prevention, force multiplication, improved efficiency of existing resources, informed decision making, and increased situational awareness. The TLO concept is a flexible and scalable model with a wide and deep information sharing network. This creates increased opportunities for identifying issues of which the fusion center wants and needs to be aware.[26]

Fusion center baseline capability assessments have provided the foundational standard for what centers need to achieve. The question becomes who supports the fusion centers needs in the regions and jurisdictions that the fusion center is responsible for? The National Network of fusion Centers addressed this by stating "By expanding fusion centers' networks, FLO programs enable the National Network to grow stronger, broader, and deeper."[27] The TLO program gives the fusion center and its partner jurisdictions the link between entities to share information and capabilities. Trained TLOs will know what the fusion center requires. These TLOs will be provided the fusion center information and intelligence products to review and distribute to their jurisdiction. The question of "who"

---

[24] *Hearing by Senate Select Committee on Intelligence & House Permanent Select Committee on Intelligence* (2011) (testimony of James R. Clapper), https://nfcausa.org/(X(1)S(yczd1ejdufegzvtuswlko1je))/ScreenPrintInfoPage.aspx?menuitemid=158&menusubid=0

[25] Matthew Harwood, "A Model of Intelligence Sharing," *Security Management*, April 1, 2012, https://sm.asisonline.org/Pages/A-Model-of-Intelligence-Sharing.aspx

[26] Kevin Saupp, "Fusion Liaison Officer Programs: Effective Sharing of Information to Prevent Crime and Terrorism," *The Police Chief Magazine*, February 2010, http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=2013&issue_id=22010

[27] National Network of Fusion Centers, *2014–2017 National Strategy for the National Network of Fusion Centers*, 2014, http://ise.gov/sites/default/files/National%20Strategy%20for%20the%20National%20Network%20of%20Fusion%20Centers%202014.pdf, 16.

are the members of the ISE and "who" will exchange the information that the fusion centers requires to fulfill its baseline capabilities is answered in Arizona with the ACTIC TLO.

Beginning in 2004 the state of Arizona and its local partners developed an information sharing network that became known in Arizona as the Terrorism Liaison Officer (TLO) Program. The TLOs are made up of sworn law enforcement, sworn firefighters, members of the U.S. military and analysts working for a law enforcement agency.[28] These are the agencies and operators that will have the responsibility for the coordination of critical public safety capabilities across the state. This is recognized by in the 2011 *National Strategy for Counterterrorism*, which states, "The capabilities and resources of state, local, and tribal entities serve as a powerful force multiplier for the federal government's counterterrorism efforts."[29] The 2014–2017 National Network of Fusion Centers strategy includes the vision of a "multidisciplinary, all-crimes/all-threats/ all-hazards information sharing network that protects our nation's security and privacy, civil rights, and civil liberties of our citizens."[30]

TLOs provide the participant jurisdiction and discipline a specific and accountable link to the fusion center and intelligence community. One of the approaches of the Information Sharing Environment's *Strategic Implementation Plan* during fiscal year 2015 is to "enhance collaboration between fusion centers and field-based information sharing entities to increase (fusion center) analytical competencies and collaboration."[31] Examples of enhanced collaboration include TLOs who are members of the fire service, who have provided examples of the TLO program in their disciplines

---

[28] Rickey Salyers, "TLO Roles & Responsibilities" (internal document, Arizona Counter Terrorism Information Center Terrorism Liaison Officer Basic School, May 2011).

[29] White House, *National Strategy for Counterterrorism* (Washington, DC: White House, 2011), https://www.whitehouse.gov/sites/default/files/counterterrorism_strategy.pdf

[30] National Network of Fusion Centers, *2014–2017 National Strategy for the National Network of Fusion Centers*, 2014, http://ise.gov/sites/default/files/National%20Strategy%20for%20the%20National%20Network%20of%20Fusion%20Centers%202014.pdf, 16.

[31] Information Sharing Environment and National Security Staff, *Strategic Implementation Plan for the National Strategy for Information Sharing and Safeguarding*, 2013,https://mise.mda.gov/drupal/sites/default/files/20140103%20Final%20NSISS%20Strategic%20Implementation%20Plan_0.pdf, 28.

publications. When firefighters come across suspicious activity, to whom and how do they report the activity? When fire departments (or any department) have a TLO, the reporting mechanism is clear. The firefighters TLO speak the same language as their peers and can communicate that information to the fusion center using the techniques taught in the basic TLO course.[32]

The Arizona Counter Terrorism Information Center is recognized by the U.S. Department of Homeland Security as the state and local fusion center for the state of Arizona. State and major urban area fusion centers are owned and operated by state and local entities, and are designated by the governor of their state. The federal government recognizes these designations and has a shared responsibility with state and local governments to support the national network of fusion centers.[33]

Fusion centers may create their own mechanism for information sharing by implementing a TLO program. Legalities involving information sharing across the homeland security spectrum have been addressed in executive orders and legal opinions. Information and intelligence are not the same thing. Confidential or classified Homeland Security Information can be broken down into broad categories. These categories include federally classified information that is restricted by members of the federal intelligence community as confidential, secret and top secret. Second is criminal background information which is governed in Arizona by National Crime Information Center and Arizona's Criminal Justice Information System. Finally there is criminal intelligence information which is governed by federal statute, 28 CFR Part 23, which addresses state and local intelligence databases.[34]

There are a number of perceived issues with the TLO program and information sharing. Notably, the ACLU believes, "The issue that arises may be inevitable. Without

---

[32] Rickey L. Salyers, and Troy Lutrick "Best Defense," *Fire Chief*, February 2011, 48–53, http://firechief.com/preparedness/firefighting_best_defense/

[33] U.S. Department of Homeland Security, "Fusion Center Locations and Contact Information," January 2014, http://www.dhs.gov/fusion-center-locations-and-contact-information

[34] Electronic Code of Federal Regulations, "28 CFR Part 23 Criminal Intelligence Systems Operating Policies," September 1993, http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=e8d03d893ffe820b7bff662c197257a8&n=pt28.1.23&r=PART&ty=HTML

clear guidance and direction these centers may stray off their intended paths."[35] The ACTIC has a civil rights/civil liberties policy that meets the DHS standard for fusion centers. [36] Concerns have been voiced about threat assessments that target academic institutions and minorities.[37] Civil rights and civil liberties policies are in place at the ACTIC and all TLOs are signatories on their understanding of these policies. Each ACTIC TLO must sign the following privacy policy dissemination acknowledgement:

> The recipient acknowledges attendance at the Privacy Policy training course and receipt of a copy of the ACTIC Privacy Policy and Procedures Guide. Recipient further acknowledges his/her responsibility to read and become familiar with this policy within 10 days from the date of receiving it. Failure to review this policy in a timely fashion or failure to comply with any provision of the policy may result in suspension of access to ACTIC information or other administrative actions or sanctions as appropriate.[38]

Access to this federally classified information requires a security clearance. The federal intelligence community (e.g., Central Intelligence Agency [CIA], FBI, Department of Defense, [DOD], DHS) use classification systems for gathering and sharing sensitive information.[39] Federal classifications of confidential, secret and top secret are detailed in section 1.3 of Executive Order 13526.[40] To have access to classified information, an individual is required to have the commensurate level of security clearance along with the right and need to know the information.

---

[35] J Monaco, "Spying on First Amendment Activity: State-by-State," American Civil Liberties Union, accessed November 28, 2011, https://www.aclu.org/free-speech-technology-and-liberty/spy-files-spying-first-amendment-activity-state-state

[36] U.S. Department of Homeland Security, Office for Civil Rights and Civil Liberties, *Civil Liberties Impact Assessment for the State, Local and Regional Fusion Center Initiative*, 2008, https://www.dhs.gov/xlibrary/assets/crcl_civil_liberties_impact_assessment_12_11_08.pdf

[37] Katherine McIntire Peters, "DHS-Supported Fusion Centers Raise Civil Liberties Concerns," Government Executive, 2009, http://www.govexec.com/defense/2009/04/dhs-supported-fusion-centers-raise-civil-liberties-concerns/29076/

[38] Warren Simpson, *Dissemination Acknowledgement Form ACTIC Privacy and Procedures Guide* (Phoenix, AZ: Arizona Counter Terrorism Information Center 2010), 1.

[39] Office of the Director of National Intelligence, "Intelligence Community," accessed March 14, 2105, http://www.dni.gov/index.php/intelligence-community/members-of-the-ic

[40] Exec. Order No. 13526 The White House Office of the Press Secretary December 29, 2009 http://www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information

Aside from federal level of classified information, there is state and local information classified as sensitive but unclassified (SBU), also known as law enforcement sensitive (LES). Additionally, the FBI maintains the National Crime Information Center (NCIC) and the attorney general has created guidelines to structure the information in the database and outline with whom the NCIC information can be shared.[41] The information contained in NCIC and Arizona's version of NCIC, called Arizona Criminal Justice Information System,[42] is considered SBU.

In July of 2003, President Bush signed Executive Order 13311, which deals with information that is sensitive but unclassified and entering into nondisclosure agreements with appropriate "State and local personnel." Authority to promulgate these procedural regulations was delegated to the Secretary of Homeland Security in Executive Order 13311.[43]

Members of the ACTIC TLO program sign a dissemination acknowledgment form ACTIC privacy policy and procedures guide form[44] (more commonly called a non-disclosure agreement) as part of the ACTIC privacy policy portion of basic TLO school. In short, TLOs have access to SBU information.

In April of 2005, President Bush signed another executive order clarifying state and local homeland security information sharing with "an individual who falls within the category of 'State and local personnel' as defined in sections 892(f)(3) and (f)(4) of the Act shall have access to information classified pursuant to Executive Order 12958 of April 17, 1995."[45] Executive Order 12958 of April 17, 1995 details what classified national security information consists of (confidential, secret and top secret).[46] In short,

---

[41] U.S. Department of Justice, *The Attorney General's Report on Criminal History Background Checks*, 2006, http://www.bjs.gov/content/pub/pdf/ag_bgchecks_report.pdf, 71.

[42] Arizona State Legislature, "Title 13. Public Safety Criminal Identification Section Arizona Revised Statute. 41-1750," http://www.azleg.state.az.us/ars/41/01750.htm

[43] Exec. Order No. 13311 (2003), http://www.gpo.gov/fdsys/pkg/WCPD-2003-08-04/pdf/WCPD-2003-08-04-Pg998.pdf

[44] Simpson, *Dissemination Acknowledgement Form*, 1.

[45] Exec. Order No. 12958 (1995), http://www.gpo.gov/fdsys/pkg/WCPD-1995-04-24/pdf/WCPD-1995-04-24-Pg634.pdf

[46] Ibid.

TLOs with the commensurate level of security clearance have access to federally classified information when they "need to know" the information.

Criminal intelligence policies are defined in what state and local law enforcement commonly refers to as 28 CFR Part 23, which details what information can be maintained by a state or local law enforcement agencies on an individual or group; how the information will be submitted, secured, viewed, disseminated; and when it should be purged.[47]

President Bush provided the executive orders concerning classified information and the Department of Justice provided the background document concerning information sharing in an opinion letter from the Department of Justice, Office of Justice Programs, Office of General Counsel to the Director of the Homeland Security Operations Center in 2005. The letter states:

> Professionals engaged in seeking to detect, defeat, or deter terrorist acts are thereby engaged in law enforcement activities for purposes of 28 C.F.R. pt. 23. Accordingly, those professionals, whether working at HSOC or another Federal, State, or local agencies engaged in this pursuit, may appropriately be provided access to the information they need to do the same, regardless of whether or not they themselves, or the agency in question, carry the title 'law enforcement officer' or 'law enforcement agency.'[48]

The 28 CFR Part 23 information can be shared among homeland security operations center (fusion center) partners in their official capacity.[49] ACTIC TLOs meet who legal standard and have access to the information they require.

The ACTIC TLOs fuse public safety intelligence and information. In addition, the TLOs communicate between response agencies and the ACTIC during moderate and large size incidents and special events. TLOs who respond to incidents need not be from the jurisdiction addressing the incident because the mutual aid system allows for cross

---

[47] Electronic Code of Federal Regulations, "28 CFR Part 23 Criminal Intelligence Systems."

[48] John J. Wilson, Office of Justice Programs Office of General Counsel, letter to Matthew E. Broderick, Homeland Security Operations Center, March 31, 2005.

[49] Ibid.

jurisdictional response.[50] The TLOs are trained and equipped to address the information sharing needs of jurisdictions and the ACTIC across the state. Adam Stone addresses the important role of fusion centers in threat and response de-escalation in his article titled "National Fusion Center Model is Emerging" when he says, "Some say the role of the fusion center is to ensure the information is not wrongly elevated to the status of a national security threat."[51]

There are recent articles detailed how TLOs can help fusion centers meet key benchmarks in the federal fusion center guidance and fusion center baseline capabilities. These include the creation a collaborative environment for the sharing of intelligence and information among local, state, tribal, and federal law enforcement and public safety partners along with the private sector. The TLO achieves the fusion centers goal of a diversified representation of personnel based on the needs and functions of the center. Brenda Leffler of the Colorado State Patrol explained how Colorado "incorporate[s] non-law enforcement entities into the center. So from the beginning, we said that firefighters, emergency services workers, critical infrastructure sector owners—all have a role in homeland security, and we have to do this together."[52] The fusion center baseline capabilities that are met include: planning, requirements development, information gathering/collection, and recognition of indicators and warnings along with the processing and collation of information. The TLO parent jurisdiction and the fusion centers become active participants in the personnel assignments, training, management, and governance of the TLO program and fusion center.[53]

TLOs also provide the link to the fusion center from within jurisdictions. Members of the fire service have written about the benefit of the TLO program in their professional publications. Who do fire fighters receive information on suspicious activity from and to whom do firefighters report suspicious activity? When fire departments (or

---

[50] Salyers, and Lutrick "Best Defense," 48–53.

[51] Adam Stone, "National Fusion Center Model is Emerging," *Emergency Management* (January 2015), http://www.emergencymgmt.com/safety/National-Fusion-Center-Model-Is-Emerging.html

[52] Harwood, "A Model of Intelligence Sharing."

[53] Saupp, "Fusion Liaison Officer Programs;" Global Justice Information Sharing Initiative, *Fusion Center Guidelines.*

any department) have a TLO, the reporting mechanism is clear.[54] TLOs can be assigned by their jurisdiction to work with the fusion center full time or part time depending in the size and needs of the jurisdiction. The basic FLO courses can take a day or a week, depending on the fusion center. This provides flexibility for the fusion center and the jurisdiction. Responsibilities of the TLO can include incident support, special events, threat, and vulnerability assessments, subject matter expertise and other areas that are important to the fusion center and the jurisdiction.[55]

Page 13 of the *Fusion Center Guidelines* depicts fusion center information sharing as concentric information circles that partially overlap each other.[56] Federal, state, and local staffing, equipment, facilities, and databases overlap at the fusion center. The conceptual model may not work if entities like critical infrastructure, elected officials, hazardous materials, or law enforcement are missing. When a fusion center establishes a TLO program the state and local information sharing circles can be linked at the fusion center.[57] Political entities at the state and local levels can generate focus and engage in policy and funding of the fusion center. The TLO can be the link that can get fusion center information to the political entities like governors and mayors.[58]

Much of the literature is dedicated to fusion center baseline capabilities and detailing why fusion centers are a good idea. The secretary of homeland security continues to state her commitment to fusion centers.[59] TLOs become the liaisons between their agencies and the fusion center to facilitate regional and national information

---

[54] Salyers, and Lutrick "Best Defense," 48–53.

[55] Salyers, "TLO Roles and Responsibilities."

[56] Global Justice Information Sharing Initiative, *Fusion Center Guidelines*, 10.

[57] Ibid.

[58] Yi-Ru Chen, "Tell Me What I Need to Know: What Mayors and Governors Want from Their Fusion Centers" (master's thesis, Naval Postgraduate School, 2009).

[59] "Remarks by Homeland Security Secretary Janet Napolitano;" Bart R. Johnson, "DHS Office of Intelligence and Analysis: Supporting the Front Lines of Homeland Security: Renewed Emphasis Designed to Improve Service to State and Major Urban Area Fusion Centers," *The Police Chief* 77, no. 2 (2010) http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=2011&issue_id=22010

exchange.[60] A TLO can be a jurisdictional and fusion center asset when it comes to operating in the information sharing environment.

The TLO may became the "who" when it comes to who would fulfill the missions that are required of fusion centers like the ACTIC. Each fusion center can determine what professional capability (e.g., law enforcement, fire, EMS, private security) is appropriate to fulfill the role of the TLO to their individual fusion.[61] According to the ACTIC, TLO basic course the roles and responsibilities of the TLO are:

> Arizona TLO's operates from the Arizona Counter Terrorism Information Center (ACTIC). The TLO program provides a platform for Federal, State, Local and Tribal representatives to share information related to local and global terrorist and criminal threats and potential incidents. Arizona's TLO Program provides an expansive statewide network of personnel by combining law enforcement and fire service personnel resources linked to Federal, State, Local and Tribal information and intelligence, which provides an effective and viable communication flow to and from the Arizona Counter Terrorism Information Center.[62]

Much of the operational work that the information sharing environment requires is possessed at the state, region or local level. The ACTIC TLO program fulfills the needs of the information sharing environment (ISE) including federal partners, the fusion center, and the home jurisdiction of each TLO. The literature describes different entities that participate in the state and major urban area TLO programs. Many TLO programs include law enforcement, fire service, EMS, public health, and other disciplines. Some programs incorporate the private sector. Each center is owned and operated by its unique state or major urban area. Fusion centers can determine what professional capabilities (e.g., law enforcement, fire, EMS, private security) are appropriate to fulfill the role of the TLO within their individual fusion.[63]

---

[60] Anthony Lukin, "Criminal Justice Terrorism Liaison Officer," California Emergency Management, August 22, 2011, accessed January 20, 2012, http://www.calema.ca.gov/CSTI/Documents/Course%20Catalog/Terrorism%20Liaison%20Officer.pdf

[61] Federal Emergency Management Agency, *Technical Assistance Catalog*, 2009, http://www.fema.gov/pdf/about/divisions/npd/npd_technical_assistance_catalog.pdf; DHS, and Bureau of Justice Assistance, *Baseline Capabilities*, 10; Saupp, "Fusion Liaison Officer Programs."

[62] Salyers, "TLO Roles & Responsibilities."

[63] Saupp, "Fusion Liaison Officer Programs."

State, local, and tribal law enforcement and homeland security officials are being asked to do more with less. Fusion centers offer a way to leverage financial resources and the expertise of numerous public safety partners to more effectively protect communities. Elected officials and homeland security leaders can better utilize limited resources to make effective decisions about public safety matters and address threats to the homeland by embracing their fusion center partners. TLOs may provide the link or capability that the information sharing environment needs.[64]

E. CHAPTER OVERVIEW

The first chapter of this thesis has focused on the ACTIC's TLO Program as a conceptual model for homeland security fusion centers. Fusion centers need to build an institutionalized relationship with their fusion center partners that foster an information sharing environment across the fusion centers federal, state, tribal, and local constituents. The ACTIC TLO Program can be a model for burgeoning fusion centers that want to leverage the need to build information sharing communication loop while simultaneously furthering the fusion centers efforts in achieving the baseline capabilities of a fusion center. The literature review of this chapter attempts to encapsulate the variety of literature that addresses fusion center intentions, capabilities, and needs.

The second chapter will provide a historical perspective to the reader on the creation of the post 9/11 city of Phoenix's Liaison Officer Program, the Arizona Counter Terrorism Information Center, and their unified efforts in creating the Terrorism Liaison Officer Program.

The third chapter describes the focus areas of the ACTIC TLO. The three focus areas of the TLO are information sharing, critical infrastructure protection, and on scene response. The information sharing capability specifically addresses the threats, hazards, and issues that the ACTIC TLOs focus on. The chapter goes on to describe the TLO stakeholder jurisdictions and the TLO roles and responsibilities along with their issues, dynamics, and challenges. The chapter concludes with the weakness that are present in

[64] DHS, *National Network of Fusion Centers Fact Sheet*.

the program along with the committees and handbook that have been developed to provide guidance to the program.

The fourth chapter looks at the capacities and capabilities of three separate fusion center liaison officer programs. In addition, the chapter demonstrates the nuanced ways different fusion centers leverage their liaison officer programs to address various fusion center priorities. This also shows that the fusion liaison officer model is not a one size fits all solution to fulfilling any fusion center gaps.

The fifth chapter looks at how the ACTIC TLO Program can be used as a model nationally. While there is no one size fits all solution to create and sustain a fusion liaison officer program, there are baseline capabilities that fusion centers must address. The ACTIC model provides a framework in which liaison officers are leveraged to the fusion centers' benefit to address baseline capabilities and further benefit their home agencies.

Chapter VI provides the reader recommendations and conclusions, which recommendations include leveraging liaison officer programs to address many of the requirements of the fusion center and address the foundational needs of fusion centers to create an information sharing environment. The information sharing environment, created through the implementation of a liaison officer program, can institutionalize the relationship between the fusion center and its constituent and partners. The chapter finishes with recommendations that a liaison officer program be included in the definition as a necessary component of a state and major urban area fusion center. The chapter also recommends that the baseline capabilities for state and major urban area fusion centers be modified to make a liaison officer program a necessary component of a fully capable fusion center.

Finally, Chapter VII concludes the thesis and notes the importance of creating an institutional relationship across all levels of government in the homeland security arena. Fusion centers have been created to foster information sharing environments along with adding capacity and capability to states and urban areas. The key to institutionalizing the fusion center relationships is a baseline capability of a liaison officer program.

II. ARIZONA'S FUSION CENTER HISTORY

There were significant changes in the United States government at all levels in the years following the September 11, 2001, attacks. The federal government began implementing the U.S. Department of Homeland Security (DHS). Arizona's governor generated an executive order called "The Roadmap to Securing Arizona." The city of Phoenix's management unified the homeland security efforts of the police and fire departments with the city's emergency management coordinator and the public health manager in a unified command Homeland Defense Bureau.

In Arizona, Governor Janet Napolitano's 2003 *Roadmap for Arizona Homeland Security* fostered a collaborative homeland security atmosphere. The executive order directed 10 action items.[65] Action item seven directed the establishment of "a 24/7 intelligence/ information analysis center that will serve as a central hub to facilitate the collection, analysis and dissemination of crime and terrorism related information."[66] This later became known as the Arizona Counter Terrorism Information Center (ACTIC). Action item three directed the establishment of "formal protocols that facilitate multiagency coordination during critical incident response,"[67] which later became known as the ACTIC Terrorism Liaison Officer (TLO) Program.

A. CITY OF PHOENIX HOMELAND DEFENSE BUREAU

In late 2002, Phoenix Fire Chief Alan Brunacini and Police Chief Harold Hurtt agreed to link Phoenix's homeland security efforts under one unified command. The core members of the team were the city's emergency management coordinator, public health manager along with the police and fire department units responsible for homeland security issues. The city's public safety management acknowledged that none of the departments can thoroughly impact any moderate or large scale incident or event without

65 Janet Napolitano, *Securing Arizona: A Roadmap for Arizona Homeland Security*, April 23, 2003, http://azmemory.azlibrary.gov/cdm/ref/collection/statepubs/id/3089, 1–2.

66 Ibid., 2.

67 Ibid., 1.

the support and engagement of the other public safety department. In Phoenix, the fire department is responsible for fires, emergency medical services, arson investigations, technical rescue, and hazardous materials operations typically referred to as special operations.[68] The fire department manages, mans and participates in an automatic aid dispatch system. Automatic aid dispatch runs the radio and data communications capability for the vast majority of the region. In addition, this dispatch center is commonly referred to as the Alarm Room. Twenty five regional fire services are dispatched and managed from the Phoenix Alarm Room.

The police department is responsible for all law enforcement operations in the city. These responsibilities include patrol, investigations, SWAT, aviation, and other special operations capabilities. In 2002, the city of Phoenix had fulltime staff working on a variety of homeland security initiatives. The Phoenix Fire Department had assigned a fire captain to the burgeoning initiative of Fire Service Intelligence. The police department had assigned detectives to work on initiatives like critical infrastructure protection, community outreach, incident response, and information sharing.

In early 2003, the city moved the unified group into the building just below the Alarm Room at fire headquarters. The team was then named the City of Phoenix Homeland Defense Bureau (HDB) and included members from the police, fire, public health, and emergency management. The team was directed to develop a plan to unify the city's homeland security efforts. The bureau's efforts focused on the city of Phoenix's homeland security operations and new opportunities in grant funding. Fire Chief Alan Brunacini and Police Chief Harold Hurtt agreed that one of the jobs of the newly assigned staff was to develop a police/fire homeland liaison officer position.[69] The liaison officer duties eventually came to include incident response to support fire and police commanders in the field. These liaison duties unified disparate public safety incident command posts and addressed the burgeoning homeland security threat. At the

[68] Phoenix Fire Department, *Strategic Plan 2014–2016*, https://www.phoenix.gov/firesite/Documents/strategicplan.pdf, 11.

[69] Phoenix Police Department, *Transfers and Reassignments William Wickers, Sergeant from Maryvale Precinct to the Office of Administration* (internal document, Phoenix Police Department, Phoenix, AZ, December 2002).

time, the concept was named the tactical liaison officer. The tactical liaison officers began by responding to large hazardous materials incidents, complex technical rescue incidents, and major police incidents. Additionally, they assumed the responsibility of responding to these incidents and working with their discipline's counterpart command. On moderate and large incidents, the police liaison responded to the fire command and the fire liaison responded to the police command. Furthermore, the tactical liaison officers built bridges and worked out issues between public safety command posts. This core group was the same team that later developed and staffed the Terrorism Liaison Officer Program.

In a time of significant change, focused on homeland security, the city researched smart practices in jurisdictions facing similar issues. The HDB members identified similar initiatives that were being developed in other jurisdictions like Lt. John Sullivan's Terrorism Early Warning (TEW) Program in Los Angeles along with the California Terrorism Liaison Officer Program, which had been conceptualized by the South Bay Police Chiefs' Terrorism Advisory Group, chaired by Redondo Beach Police Lieutenant John Skipper in southern California.

Members of the Homeland Defense Bureau traveled to California to identify current practices in unifying public safety efforts in homeland security. The group met with Los Angeles Police Department's Jim McDonnell and John Miller along with their staff and later the general manager of the city's Emergency Management Department James Featherstone. They traveled and met with other leaders, including Lt. John Sullivan's at Los Angeles' TEW facility. These initiatives were later foundational in the development of the ACTIC TLO Program. Bureau members noted that the perspectives of the different initiatives and strategies were each appropriately tailored to meet the needs of each jurisdiction.

In 2004, Chief Brunacini assigned a Phoenix fire captain to the Homeland Defense Bureau to focus on incorporating the fire service into the intelligence

community.[70] In retrospect, the addition of that particular fire captain, including his skills, knowledge, and abilities became a cornerstone upon which the TLO program was built. The captain, a senior firefighter paramedic who was returning from a Marine Corps deployment, was assigned as the intelligence officer and tactical liaison officer representing the Phoenix Fire Department. With his robust military intelligence background, the captain easily articulated the need for a public safety, as opposed to a law enforcement approach to intelligence and information sharing.

B. ARIZONA COUNTER TERRORISM INFORMATION CENTER

In 2003, members of the Homeland Defense Bureau met with the commander of the Arizona Department of Public Safety's (DPS) Intelligence Detail and the FBI assistant special agent in charge who was responsible for the Phoenix Joint Terrorism Task Force. The concept of the fusion center was discussed. The parties moved forward with unifying their homeland security efforts with the intent of funding the fusion center capability using homeland security grant funds. The DPS assigned a lieutenant to identify the location and manage the budgeting issues. In addition, the DPS lieutenant formed a committee and managed the fusion center from concept through to implementation. In October of 2004, the doors of the ACTIC, the only federally recognized fusion center in the state of Arizona, opened, and it has been in operation ever since. The ACTIC located in Phoenix, Arizona, which lies in the center of the state and in the center of Maricopa County. Phoenix is the sixth most populated city in the United States and lies within the fourth most populated county in the country.[71] Furthermore, the ACTIC's members had access to over 100 databases, and it was the INTERPOL link in Arizona. The city of Phoenix assigned many of the Homeland Defense Bureau fire and police officers to work at the ACTIC.

---

[70] John Maldonado, *Phoenix Fire Department, Transfers and Reassignments—Rickey L. Salyers from Station 8 to Homeland Defense* (internal document, Phoenix Police Department, Phoenix, AZ, December 2004).

[71] United States Census Bureau, "Quick Facts," 2011, http://quickfacts.census.gov/qfd/states/04/04013.html

The mission of the ACTIC is to "protect the citizens and critical infrastructures of Arizona by enhancing and coordinating counter terrorism intelligence and other investigative support efforts among local, state and federal law enforcement agencies." Furthermore, the vision of the ACTIC is "to prevent terrorism and related crimes, thereby providing a safe and secure environment for the citizens of Arizona."[72] Additionally, the goal of the ACTIC is to "fuse local, state, tribal, federal public safety agencies information sharing capabilities and involve public & private sectors in the process."[73]

The ACTIC structure is composed of full-time staff from many jurisdictions across the federal state and local public safety spectrum. The federal agencies include U.S. Department of Homeland Security investigations, intelligence and analysis along with the reports officer. The state agencies include the Arizona Department of Public Safety Intelligence, Global Imaging Unit (mapping), Hazardous Materials Squad, Criminal Investigations Research, Computer Forensics unit, terrorism liaison officer statewide coordinator, and ACTIC management. Maricopa County is represented with their homeland security and facial recognition units. The city of Phoenix is represented by its Homeland Defense Bureau including its Terrorism Liaison Officer Program, Intelligence and Investigations Unit, Major Offender/Career Criminal Unit, Computer Forensic Squad, Threat Mitigation Squad, and the Criminal Intelligence Analyst Unit.

The ACTIC Intelligence Unit is staffed with a DPS supervisor and analysts who create documents specific to the needs of the fusion center. These documents include suspicious activity, situational awareness and informational updates relevant to public safety and private sector partners across the state. The unit works closely with the U.S. DHS I&A representative, and it creates or participates in creating threat assessments concerning special events like National Basketball Association and Major League Baseball all-star games, playoff games for any of the professional sports teams, or events that may generate civil unrest. The analysts leverage the TLO Program to assist in the collection of data that is needed to create the products.

---

[72] Arizona Counter Terrorism Information Center, "Mission Vision," 2004, http://www.azactic.gov/About/Mission_Vision/

[73] Arizona Counter Terrorism Information Center *ACTIC Overview* (internal document, Arizona Counter Terrorism Information Center, Phoenix, AZ, May 2011), Slide 2.

After a few months of working at the ACTIC, it was clear to many that the Phoenix fire captain was the driving force in creating a trusted partner relationship among fusion center participants. His position in the fire service remained focused on fire service intelligence, but he was asked to take over the responsibilities of a program that had started as a tactical liaison officer program in Phoenix. The statewide coordinator position was an additional duty. The new program was intended to address information and intelligence sharing along with critical infrastructure protection and incident response. The initiative was called the Terrorism Liaison Officer Program.

C. TERRORISM LIAISON OFFICER

Opening in October 2004, the ACTIC provided the hub where Arizona's public safety network would be formed. The ACTIC had the opportunity to create an institutionalized relationship with its partner entities. The city of Phoenix tactical liaison officers was the logical staff to work with the ACTIC as the ACTIC worked toward building its information sharing environment (ISE). A group of city of Phoenix staff moved into the ACTIC when it opened.

Information sharing is the core capability of the ACTIC and any fusion center. The TLO program provides the ACTIC a network capable as the backbone of the states ISE. In Arizona, the TLO ISE is complimented by two other TLO program capacities. The second capacity provides a link between the ACTIC and critical infrastructure partners through the TLO program members who have established relationships between their jurisdictions and their local critical infrastructure. Lastly, the TLO Program provides direct support to its member jurisdiction with TLOs, who respond to critical incidents in jurisdictions across the state. This "on scene response" (OSR) provides the ACTIC and decision maker's access to information directly from the scene of an incident, and it provides the incident commander and responder's at the actual incident access to data and resources that are available through the ACTIC.

The TLO is essentially the team or individual that is designated by a jurisdiction as their trusted partner to exchange information with the ACTIC. Depending on the size of a jurisdiction and their ability to participate in the program a TLO may serve in a full-

time capacity or as an additional duty to a jurisdictions employee. Many jurisdictions in Arizona commit to having their TLOs participate in TLO related work 10 to 25 percent of their shift.

The ACTIC TLO program has been compared to a milk stool. The program relies on three legs, or components, which include the ISE, CI protection, and OSR. Furthermore, the three compartments are not interdependent and can be sustained separately.

THIS PAGE INTENTIONALLY LEFT BLANK

III. THE THREE FOCUS AREAS OF AN ACTIC TLO

A. INFORMATION SHARING ENVIRONMENT

Police, fire, EMS, public health, and their other public safety partners typically meet at an incident, addressed the needs of the incident, and go their separate ways. Mass casualty events along with manmade and natural disasters typically reveal a void in communication. The TLO Program created a trusted partner environment between public safety partners by bringing these disparate disciplines together to address public safety issues and events in Arizona. This ACTIC liaison officer trusted partnership was a new and smart practice in Arizona that has been beneficial during countless critical incidents. Jurisdictions cannot assemble an ad-hoc group of trained, vetted, and trusted liaisons from public safety agencies as situations arise. Fire, law enforcement, public health, and other TLO Program participants know critical incidents are not a surprise. The ACTIC TLO Program is a best practice model for jurisdictions and fusion centers that know that critical incidents and the need for information sharing are no surprise and it is in the best interest of the fusion center and their constituent jurisdictions to unite in a strong information sharing network.

The TLO is Arizona's method of addressing the national strategy for information sharing direction that "…fusion centers… serve as the primary focal points within the state and local environment for the receipt and sharing of terrorism-related information."[74] The TLO Program takes operators from disparate disciplines and creates an information sharing environment where homeland security issues can be addressed seamlessly. The intention of the program is to build bridges between these partner disciplines and address gathering and sharing of information, critical infrastructure protection, and response to critical scenes. The fusion center and its partners have homeland security interest in each of these capacities and capabilities.

[74] White House, *Sharing Information with State, Local, and Tribal Governments* (Washington, DC: White House, 2007), http://georgewbush-whitehouse.archives.gov/nsc/infosharing/

Multidisciplined TLOs respond to expanding incidents, planned events, attend the same training, and are provided the same equipment. This has created a trusted network of public safety officials who exchange necessary information with and through the ACTIC. Participants in the TLO program are trained about the sensitivity of the information that is available to them through the ACTIC and they sign non-disclosure agreements. Many TLOs from a variety of disciplines get a security clearance so they can view information that is classified at the federal level.

When the ACTIC opened as Arizona's fusion center its federal partners committed to sponsoring security clearances for state and local personnel assigned to the facility. The TLOs that are assigned by their agencies to participate in the ACTIC submit their application for their secret clearance after graduation from the TLO school and six months of active participation in the program. The addition of a security clearance to a TLOs resume removes an information sharing prohibition that previously existed. Non-traditional partners that have their clearance through the ACTIC include public health managers, firefighters, and fire prevention engineers. The benefits of the security clearance are seen consistently. The clearance fosters a trusted partner relationship between the individuals who may over-classify or section off important public safety information and it includes access to appropriately classified material for national security purposes. Information that is important to public safety employees across the spectrum is available to them. These are the same individuals who are responding to homes, businesses, and critical infrastructure across the state. The incorporation of these partners is a force multiplier and does not require the addition of any new staff.

The TLO program makes information available to public safety officers outside of law enforcement. Like an analyst, access is granted to law enforcement sensitive information as long as the participant is assigned to the TLO program. Fire service employees who are assigned to the fusion center as TLOs have access to law enforcement databases. The intention of the program is to create an environment where the need to share critical or safety information trumps the need to maintain stovepipes of information under the umbrella of a security classification (see Figures 1 and 2).

Figure 1. Disconnected Capabilities and Needs

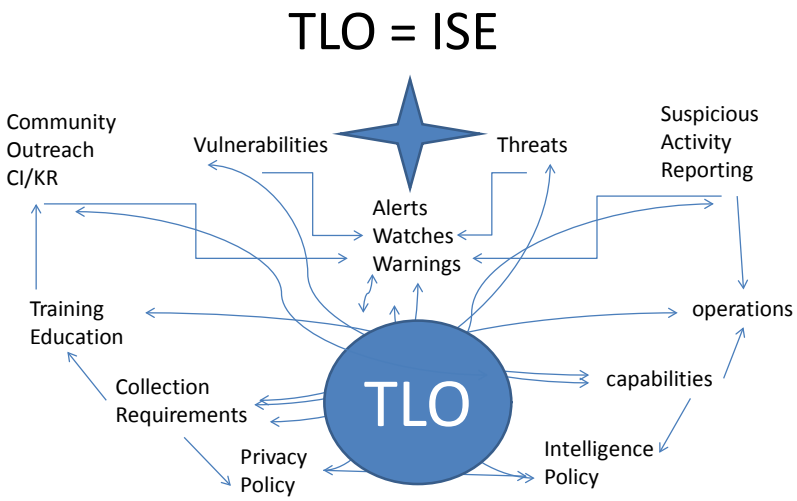

Figure 2. Fused Capabilities and Needs

ACTIC's information sharing core capability has been addressed and documented with the published collection plan. The collection plan provides TLOs and other ACTIC partners the structured and defendable list of areas the fusion center focuses on. The core of the suspicious activity reporting system is having a plan that identifies the specific information that ACTICs partner jurisdictions require to address their areas of responsibility.

The ACTIC, DHS, and the FBI each maintain a list of collection requirements that they each publish. Each collection requirements lists the information that the individual entities require to fulfill their responsibility to the intelligence community. Examples include information on drug trafficking organizations, terrorism, and terrorist organization along with other areas that the agencies are responsible to address. During the basic TLO School, the ACTIC collection requirements are distributed and are taught to the TLOs. Reportable events occur and information is collected by TLOs in jurisdictions across Arizona. Each jurisdictions TLO can provide the necessary information to the ACTIC along with the FBI and DHS through a standard reporting mechanism that the TLO is trained to use. When the ACTIC, DHS, or the FBI have information that is relevant to the jurisdictions in Arizona the information is distributed to the TLOs for further distribution throughout their particular jurisdiction.

One of the best practices of the ACTIC was the development of an intelligence collection plan. The ACTIC Collection Plan was developed by the ACTIC Intelligence Committee after it surveyed Arizona's law enforcement agencies. The survey demonstrated that the ACTIC has three areas of concern consisting of threats, hazards and issues. The survey further demonstrated twelve focus areas that require information collection and documentation (Table 1). The information is collected by the ACTIC's Watch Center from TLOs and anyone wishing to contribute in a 28-CFR compliant database housed at the ACTIC, which is managed by the ACTICs analysts. Documents created from this data include situational awareness bulletins and public safety/criminal case support. The ACTIC collection plan is unclassified. Table 1 represents the focus areas of the collection

plan. “Collection derives directly from requirements” explains why each of the 12 focus areas of the Plan has specific collection requirements.[75]

Table 1. ACTIC Collection Priorities

THREATS	**HAZARDS**	**ISSUES**
Domestic and International Terrorism	Health Hazards	Regional Crime Trends
Threats to Law Enforcement, Public Safety and other officials	Natural Hazards	Border Issues, Violence, Human/Weapon Trafficking
Threats and Assessments of Critical Infrastructure		Strategic Narcotics Intelligence
Threats to Special or Public Events	Critical Incident Support	Gang Intelligence
Special Interest Alien Threats to the Community		

Each category in the collection plan has detailed subcategories that reveal sources and methods concerning ACTIC’s information collection. These subcategories are called collection requirements. The collection requirements are classified as “public safety sensitive” (PSS).[76] TLO member jurisdictions are not solely law enforcement organizations so this is an important caveat. The reason for the sensitivity is the harm that could occur to an individual or institution if the name of the information’s source or the method an institution used to collect the information is revealed. The state of Arizona’s PSS classification standard is intended to be similar to the federal governments controlled unclassified information standard.[77]

The information can come in from law enforcement, TLOs, ACTIC partners, community partners, and the public. The ACTIC has police officers and analysts assigned to take in, document, and make notifications concerning suspicious activity reports. The

[75] Mark M. Lowenthal, *Intelligence from Secrets to Policy* (Los Angeles: Sage, 2012), 62.

[76] Arizona Counter Terrorism Information Center *ACTIC Information Classification, Access, Dissemination, Storage and Destruction Policy* (internal document, Arizona Counter Terrorism Information Center, Phoenix, AZ, March 2006).

[77] Exec. Order No. 13556 (2010), http://www.hsdl.org/?view&did=14168

ACTIC strategic intelligence analysts develop products based on the collection plan and collection requirements from the data that the police officers enter. The analysts create law enforcement, public safety, official use, and unclassified information products from the information they receive.

The ACTIC is sensitive to the civil rights and civil liberties issues that come along with collecting and maintaining intelligence and information data. Each TLO is requires to take and pass the online 28 CFR part 23 training before he or she starts the basic TLO school. The TLO school instructs the students on the type of information the ACTIC needs to collect. That information is based on a criminal predicate or a threat to public safety. In addition, the information needs to be based on reasonable suspicion that the individual or group has committed or is planning to commit criminal/terrorist act. The information should be relevant to investigation or the prosecution of suspected criminal/ terrorist incidents, law enforcement, or crime prevention. The data should be useful in analysis and focused on public safety.

The information is used in crime suppression efforts, which includes terrorism, and assists agencies concerning the deployment of assets for law enforcement and prosecution. The information can be tactical or strategic and should focus on the existence, identification, capability of individuals and organizations suspected on criminal or terrorist activity.

The ACTIC does not pursue or maintain information based on constitutionally protected activities including race, ethnicity, citizenship, origin, age, disability, gender, sexual orientation, religion, political, and social activities or activities that are not criminal. Rather, the ACTIC concentrates on dependable information sources so its products will be accurate, relevant and current. Many times this dependable source is the TLO.

The ACTIC maintains this data in a secure database that has access controls and is audited to assure compliance with the policies of the ACTIC along with state and federal law. The release of information contained in the database will follow state and federal law. These laws are commonly referred to as sunshine laws.

B. CRITICAL INFRASTRUCTURE

The city of Phoenix group that moved into the ACTIC included a detective whose background and education included undergraduate and graduate studies in architecture, design and construction along with over a decade of training and experience as a city of Phoenix bomb technician. The detective had been conducting threat and vulnerability assessments of sites the city of Phoenix considered critical for years before 9/11. After 9/11, he shouldered the responsibility of threat mitigation, or what we now call critical infrastructure (CI) protection.

Homeland Security Presidential Directive 7 (HSPD-7) addresses critical infrastructures that provide the essential services that underpin American society.[78] The nation possesses numerous critical infrastructures, whose exploitation or destruction by terrorists could cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction, or could profoundly affect our national prestige and morale. In addition, there is critical infrastructure so vital that its incapacitation, exploitation, or destruction, through terrorist attack, could have a debilitating effect on security and economic well-being.

Critical infrastructures is defined in U.S. Code as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[79] Key resources are defined in U.S. Code as "publicly or privately controlled resources essential to the minimal operations of the economy and government."[80] According to DHS,

---

[78] U.S. Department of Homeland Security, *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection*, 2003, http://www.dhs.gov/homeland-security-presidential-directive-7#1

[79] "Critical Infrastructures Protection Act of 2001 42 U.S.C. 5195c," Government Printing Office, accessed February 16, 2014, http://www.gpo.gov/fdsys/pkg/USCODE-2010-title42/html/USCODE-2010-title42-chap68-subchapIV-B-sec5195c.htm

[80] "6 U.S.C. 101 Definitions (10)," Government Printing Office, http://www.gpo.gov/fdsys/granule/USCODE-2012-title6/USCODE-2012-title6-chap1-sec101/content-detail.html

> Critical infrastructure is the backbone of our Nation's economy, security and health. We know it as the power we use in our homes, the water we drink, the transportation that moves us, and the communication systems we rely on to stay in touch with friends and family. [81]

DHS goes on to make clear that

> fusion centers serve as the focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information and have additional responsibilities related to the coordination of critical operational capabilities across the statewide fusion process with other recognized fusion centers.[82]

The detective, the fire captain, and the HDB group conceptualized a program where the homeland security needs of the CI community, the ACTIC, and the public safety agencies in the Arizona's communities would be met. The concept became a key component of the TLO program. The plan was to secure grant funding for the TLO program by having the TLOs focus their efforts on CI protection. This complimented the information sharing efforts that the ACTIC was developing. The CI data is not beneficial sitting in a data storage devise at the fusion center. Public safety agencies can benefit from the data in their jurisdictions to make themselves and their community safer. The logical solution to collecting data and conducting threat and vulnerability assessments was to provide TLOs the capability to assess the CI in their jurisdictions. They realized that CI information could be stored securely at the ACTIC and the data could be linked through a TLO to an incident commander who was responsible for addressing incidents at the CI. They worked to develop and maintain a secure internet accessible database for maintaining the CI data, and the database was later made available to TLOs in the field responding to incidents at the CI. The group, working out of the state's fusion center, was focused on regional and statewide capabilities and not the capabilities and issues of a single jurisdiction.

The information included in the CI database accessible to responders through the TLO include the facility's hours, photos, maps, hazardous materials, plans, procedures,

---

[81] U.S. Department of Homeland Security, "Critical Infrastructure Security & Resilience Month," 2012, http://www.dhs.gov/cipr-month-2012

[82] Ibid.

and other information, including points of contact. The TLO is a member of the diverse assessment team that conducts a threat and vulnerability assessment (TVA) on the CI. This team includes trained TLOs who use their expertise during the TVA. The TLO disciplines that participate in the assessments typically include law enforcement, fire service, EMS, hazardous materials technicians, special weapons and tactics tacticians, bomb technicians, and others. TLOs who are assigned a level "A" or "B" kit are responsible for participating in the threat mitigation of CI on behalf of the ACTIC and their agency. This includes the identification, collection, and proper documentation of Automated Critical Asset Management System (ACAMS) information.

This TVA is useful for a variety of reasons. For example, the TVAs are used by the city and region to demonstrate the need for homeland security grant funding. In addition, the TVA data is beneficial to incident commanders and responders who address the myriad of calls for service at these facilities. Moreover, the TVA provides a one-stop shop for critical information.

A fusion center that plans to address CI needs to identify the system that will work best for its needs. The basis for the method the TLO program uses in Arizona is the capability to view the CI data in the field by the TLO specific disciplines and jurisdictions. This is in place so the assessment data is available to an incident commander addressing the myriad of issues that occur at these critical facilities.

To collect and maintain CI data DHS and the ACTIC has used ACAMS, which maintained the documented critical infrastructure information in an accessible format. In Arizona, the TLOs conduct the threat and vulnerability assessments of CI and input the data into the system. The information in the system is protected critical infrastructure information (PCII).

DHS estimates that 85 percent of critical infrastructure is owned and operated by the private sector.[83] Members of the private sector depend on the security of proprietary information that they use to operate their businesses. Some of this proprietary

[83] Federal Emergency Management Agency, *Ready Business Mentoring Guide*, 2014, http://www.fema.gov/media-library-data/1392217307183-56ed30008abd809cac1a3027488a4c24/2014_business_user_guide.pdf, 8.

information is important to enhancing the security of the critical infrastructure so it is documented in ACAMS. There are federal and Arizona state laws prohibiting the release of PCII. The PCII Act of 2002 defines PCII as "Information not customarily in the public domain and related to the security of Critical infrastructure or protected systems."[84] Violation of the Arizona or federal law may result in imprisonment, fines, loss of employment, or related penalties.[85]

DHS assigned a protective security advisor (PSA) to Arizona. Arizona's PSA is responsible for conducting threat and vulnerability assessments along with providing national coordination for critical infrastructure protective programs in Arizona. They work in response and recovery efforts to reduce risk to the critical infrastructure,[86] which is a tall order for any individual or agency. The logical avenue for Arizona's PSA to work through is the ACTIC and with the TLOs who have the relationships and points of contact throughout the state's critical infrastructure.

ACTIC TLO program members from the ACTIC's Threat Mitigation Unit (TMU) work in partnership with the PSA to conduct threat and vulnerability assessments, also known as critical infrastructure assessments. The TLOs who conduct the assessments will be from the representative disciplines of the TLO Program including fire, HazMat, police, SWAT, bombs, and related disciplines. This assures that the assessments are done from an all-hazards perspective. There is a training block on how to conduct the assessments that is available through the TLO Program.

When the assessment is complete, the TLO will have a number of recommendations for the CI partners to consider as they move forward. These are recommendations and not requirements; the recommendations are intended to reduce or remove vulnerabilities at the facility. The ACTIC, TMU, and the TLO Program are not regulatory entities.

---

[84] 6 CFR 29.2 *Protected Critical Infrastructure Information* http://cfr.regstoday.com/6cfr29.aspx#6_CFR_29p2

[85] *Critical Infrastructure Information System* Arizona Revised Statutes Article 7.1 41-1805; 6 CFR 29.9 Protected Critical Infrastructure Information http://cfr.regstoday.com/6cfr29.aspx#6_CFR_29p2

[86] U.S. Department of Homeland Security, "Protective Security Advisor Program," December 2013, http://www.dhs.gov/sites/default/files/publications/PSA-Fact-Sheet-508.pdf

Identification of CI may seem as simple as checking the DHS website, which shows clearly the 18 CI sectors are agriculture / food, banking and finance, chemical and hazardous materials industry, defense industry base, energy, emergency services, information technology, telecommunications, postal and shipping, public health, transportation, water, national monuments and icons, commercial assets, government facilities, dams, nuclear power plants, and critical manufacturing. Identification of these sites may require that the TLOs to work with their dispatch or communication units. TLO jurisdictions will likely have the locations documented as site specific hazards, and jurisdictions with hazardous materials assets can leverage that knowledge to identify critical sites. For example, a fire service TLO may have a relationship with sites that have specific response needs, such as bulk foam for fuel tank farms, or public health TLOs may have a relationship with radiological assets because they store potassium iodine in the case of an incident. Additionally, some large jurisdictions may have a special hazards unit that may assist the TLO with asset identification. Furthermore, some sites may meet local or regional criteria that show they are critical to the local or regional community, but they may not rise to the level of a nationally critical asset. Arizona's ACAMS system can be used to collect the data for use by the local community's responders, the TLOs, the ACTIC, and DHS.

The ACTIC maintains an Arizona specific database that contains all the local, state and national CI data. The system is linked to the national ACAMS system, and the nationally significant data is uploaded to DHS. The ACTIC uses a secure server that can be accessed by TLO computers through the use of air cards so the data can be entered into the system and can be accessed as needed. This enhances the response capabilities of the ACTIC public safety partners. The TVA information is protected by Arizona and federal laws and policies, and each TLO is trained in the related laws and policies.

The Department of Public Safety has the statutory responsibility to store, manage and secure the protective critical infrastructure information (PCII) according to state law (ARS Title 41, § 1801-1804).[87] The PCII data is managed at the ACTIC where the data

[87] "Critical Infrastructure Information System Arizona Revised Statutes Article 7.1 41-1801—41-1804," accessed November 28, 2014, http://www.azleg.gov/ArizonaRevisedStatutes.asp?Title=41

that is collected by the TLOs is stored and used as needed. This database is available to TLOs in the field who are supporting incident commanders who address events and incidents at these critical locations. This unification of effort and databases concerning critical infrastructure is a best practice. The state law provides legal protection for the sensitive data, and the trained and equipped staff maintains the data for use during critical incidents or special events.

C. ON-SCENE RESPONSE

The history of the city of Phoenix TLO's involved the expectation that TLOs would provide a capability to responders in the field. Intelligence-based decision making is the way many public safety decision makers in Phoenix refer to the addition of the TLO capability.

The TLO program has leveraged ACTIC and Phoenix Homeland Security Grant Program funds to support CI assessments and information sharing. The TLO Program purchased laptop computers and air cards to link the TLOs in jurisdictions across the state to the ACTIC. The TLOs collected and entered the data into the ACTIC CI databases. With their TLO laptop, they can also access the CI information they had entered along with the information contained in and accessible through the ACTIC's many criminal, intelligence, and investigative databases.

On-scene response is based on jurisdictional needs. On-scene response provides the participating jurisdiction immediate reach back to ACTIC which provides incident command with real time intelligence. The TLO's become the intelligence branch of NIMS.[88]

In the Phoenix region, TLOs are dispatched through the Phoenix Fire Department's data and voice communications center called the "Alarm Room." When TLOs are requested by first responders and jurisdictions operating in the field, the TLOs get a page on their cell phone or pager. In response, the TLOs will call the dispatch center or the incident command post to determine the nature of the call and identify what

[88] Salyers, "TLO Roles & Responsibilities."

intelligence assets will be needed to appropriately address the incident. Those assets include the ACTIC's facial recognition unit and criminal investigations research unit of any number of assets. The TLOs will place that capability on standby, which means that the operators working in those areas will focus their efforts on the incident currently being addressed in the field as a priority.

The TLOs are also automatically dispatched during a standard list of specific calls for service across the region. TLOs are deployed to calls ranging from weapons of mass destruction (WMD) (e.g., suspected cases of anthrax, ricin, radiological), significant HazMat, unknown substance, bomb callouts, to Metropolitan Medical Response System (major medicals), moderate- and high-risk search warrants, drug laboratories, and officer shootings among others.

TLOs respond to three categories of incidents referred to as tiers. A Tier III incident is a local event that does not require resources outside of the TLOs' jurisdictions. These incidents include supporting the SWAT team or HazMat team on incidents they are resolving. Tier II incidents are incidents that require a number of jurisdictions or a number of TLOs to address the issue. These incidents may include officer involved shootings and complex hostage barricades. Tier I incidents are complex critical incidents that require multiagency unified command, such as a large structural collapse, a terrorist event, or major medical event.

While terrorism liaison officers normally operate in pairs of one law enforcement officer (detective or sergeant) and one fire services (company officer), intensive cross training and certification makes it possible for both law enforcement and fire services TLOs to operate independently. The intent is having a unified intelligence public safety capability at the scene of these incidents.

The fire service staffs the position commensurate with their shifts. They cover 24 hours a day, seven days a week 365 days a year. The police staff the position on duty seven days a week and respond from a standby status during off hours. All level "A" TLOs have a vehicle, and they respond individually. One TLO from a discipline, like the fire service, will arrive first at an incident command post. That first on-scene TLO has the

same capability and training as the TLOs from the other response TLO disciplines. The first on-scene TLO can begin accessing all the intelligence, information, and data that is available through the ACTIC.

The Phoenix region TLOs communicate on an encrypted radio channel that is sponsored by the Phoenix Police Department. The 800MHz based system covers the majority of the 9,200 square miles of Maricopa County, which is larger than seven U.S. states.

Incident commanders in jurisdictions with TLOs now rely on information and intelligence support provided by one of their staff who is assigned as the jurisdiction's TLO. The TLOs in Arizona's Maricopa County also have access to a secure communications channel. They communicate directly with TLOs from partner jurisdictions and the ACTIC to request and provide information, intelligence, and request support as incidents expand.

The TLO can leverage the ACTIC and the resources available to them through the network to positively impact the incident. Furthermore, the ACTIC provides response TLOs with a checklist or algorithm of ticklers to ensure that the resources and data available to the incident commander are accessed and provided to the responders and investigators.

Responder safety is one of the focuses of the TLO. Fire service TLOs can identify the parameters of a scene and restrict the response of fire and EMS units into the vicinity of the incident. As fire/EMS units are called to the vicinity of the scene, the TLO is notified and the public safety calls for service are de-conflicted. If the call is related to the incident, then the loop is closed with incident command and the decision is made how to safely proceed. If the call is within the perimeter of the incident but is unrelated, the TLO can work with the incident commander to get the fire/EMS resources in and out of the incident within the incident in a safe manner.

Jurisdictions in Arizona typically use the Incident Command System (ICS) to address moderate and large incidents. These jurisdictions may call for incident management organizations to manage incidents and events that expand to include

multiple jurisdictions covering a large geographic area and/or requiring multiple operational periods. In the ICS model, the TLO is an intelligence asset to the incident commander and the investigations units. When a Type I, II or III incident management team assumes management responsibility for an incident or event, the TLOs become the intelligence section chief. They may be assigned to the command staff and report directly to the incident commander or they may fall under a general staff position like planning. The Phoenix Urban Area Security Initiative (UASI) Incident Management Team (IMT) uses the TLO in the intelligence liaison position on its command staff during deployments out of the jurisdiction and under the Intelligence Branch on the general staff during planned events in town.

Incident response was the core capability that united first responders and demonstrated the need for a liaison officer program. Throughout the development of the TLO Program, the liaison officers have responded to critical incidents and provided on-scene intelligence and information support from the fusion center. This real-time exchange of information that supports incident commanders builds value in the program daily. In addition, field operators and incident commanders become consumers of the TLO and fusion center information and value is built in the ACTIC and the network of the liaison officer program. This is a best practice of the ACTIC TLO model.

D. STAKEHOLDERS

The stakeholders in the TLO program have grown since its inception. Each stakeholder represents its jurisdiction and professional capacity. Issues faced by many fusion centers involve the links and relationships they have into each of the entities throughout our federalist system. When there is an incident outside a military post that the U.S. secretary of homeland security needs information on, who does the homeland secretary's office call? When the local fire captain identifies a novel and unique arson threat that could have significant homeland security implications, who should he or she call? Who does the fusion center provide intelligence or informational documents to when the FBI or DHS (among others) create situational awareness documents concerning threats or special events/circumstances for public safety? How are alerts, watches,

warnings, and situational awareness documents distributed? The logical answer is to utilize the fusion center to address these information sharing requests. This raises the question of who, at the end-user level—the police officer, sheriff, public health, military, or firefighter—has the knowledge about the fusion center, its capacity, and capability and who knows how to supply or query necessary information from across the federalist landscape.

Examples of jurisdictions that participate in the ACTIC TLO program include tribal law enforcement agencies, Arizona department of corrections, university police departments, U.S. military, border patrol, sheriffs, local firefighters, public health, local law enforcement, Transportation Security Administration, task force officers assigned to the Joint Terrorism Task Force along with railroad police and others. Each of these stakeholders has a professionally vested interest in keeping our nation, state, county, region, and community safe.

The TLO is the mechanism and ACTIC's member jurisdictions are the stakeholders involved in addressing the new, novel, and fractured components that are encompassed in Arizona's homeland security efforts. The diversity of the membership is a best practice and is pivotal to the program's success.

E. ROLES AND RESPONSIBILITIES

Each fusion center is responsible for creating a strategic relationship with its federal, state, and local partners. The role of the ACTIC TLOs is to represent their jurisdiction and professional capability to the ACTIC and the TLO network. One example includes hazardous materials incidents. Fire service partners in Arizona typically maintain the hazardous materials response capability. The technicians that operate on these calls have a specific skill set. Where does law enforcement, public health, or DHS engage with fire hazardous materials technicians that are addressing a criminal act with casualties involving the intentional use of a hazardous material? The TLOs role is to engage at the incident command level and unify efforts by engaging their network to positively impact the incident. In addition, the TLOs have access to specific CI, intelligence, and information that impacts many aspects of the incident. The intent of the

TLO Program is not to make law enforcement officers or public health professionals into hazardous materials technicians; rather, the intent is to create a network where the professional capabilities are networked to address situations where specific expertise is required. No single Arizona jurisdiction maintains all conceivable homeland security capabilities.

The role of the TLO is to bring their professional competency into the ACTIC network. The TLOs' role is to use their initiative and ability to build bridges or relationships between themselves and TLOs from other levels of government and different disciplines. The network is the strength of the program.

Applications to become an ACTIC TLO include the endorsement by the applicant's supervisor acknowledging the level of commitment and engagement that will be expected of the applicant. The application also includes a portion that details the level of commitment (A, B, C, or D—explained below) the jurisdiction and the ACTIC will expect of the TLO. The ACTIC, pursuant to state law, enters into an intergovernmental agreement with the TLO's agency. The Inter-Governmental Agreement (IGA) addresses the purpose of the IGA, details concerning the participation and time commitment of the TLO, equipment, finances, and other boiler plate IGA language dealing with discrimination and liability.

A level "A" TLO are assigned a package of grant funded equipment that includes an automobile for response, an internet capable laptop computer for information sharing, and a variety of other equipment to respond to incident as well as conduct threat and vulnerability assessments of critical infrastructure and key resources. Level A TLOs are sponsored by the ACTIC for a federally sponsored secret security clearance, and successful completion of the secret security clearance investigation is a requirement for a level A. Additionally, the home jurisdiction of a level A TLO is required to sign a memorandum of understanding with the ACTIC concerning TLO equipment, roles, and responsibilities.

A level "B" TLO are assigned a package of grant funded equipment that includes an internet capable laptop computer for information sharing and a variety of other

equipment to respond to incident as well as conduct threat and vulnerability assessments of critical infrastructure and key resources. Level B TLOs are also sponsored by the ACTIC for a federally sponsored secret security clearance, and successful completion of the secret security clearance investigation is a requirement for a level B TLO. Like for the A level TLO, the home jurisdiction of a level B TLO is required to sign a memorandum of understanding with the ACTIC concerning TLO equipment, roles, and responsibilities.

A level "C" TLOs are be assigned an equipment package that is purchased by their home jurisdiction. This equipment package typically includes a computer for intelligence and information sharing. In addition, the package may include a variety of other equipment to conduct TLO operations, including threat and vulnerability assessments of CI.

A level "D" TLO is an individual that a jurisdiction has sponsored to participate in the TLO program. The focus of this individual is the exchange of information and intelligence on behalf of their organization with the ACTIC.

Each ACTIC TLO attends a 40-hour basic course. The U.S. Department of Homeland Security approved course includes TLO roles and responsibilities, the signs of terrorism, domestic and international terrorism, fourth generation warfare, ACTIC capabilities, civil rights and liberties, intelligence products, the FBI JTTF, DHS Intelligence and Analysis (I&A), protective security advisor (PSA), criminal investigations research, intelligence-led policing, and suspicious activity reporting. The 28 CFR part 23 is the Code of Federal Regulation that addresses state and local intelligence gathering, documenting, and retaining. The TLO course has a prerequisite requiring that each candidate take and pass the Department of Justice Bureau of Justice Assistance on-line course called 28-CFR part 23.[89]

F. ISSUES, DYNAMICS, AND CHALLENGES

The creation of the ACTIC TLO program resulted in a number of unintended consequences. Some of them were disruptive. The ACTIC TLO program had many

[89] Bureau of Justice Assistance *Log In to 28 CFR Part 23 Online Training* National Criminal Intelligence Resource Centerhttps://www.ncirc.gov/28cfr/Default.aspx

strategic implications. When the program was conceptualized, it was opposed by a number of individuals. Some felt they would be yielding or making sensitive information available to other professions or agencies that may not have a right to see or know specific information. Some were concerned about reporting on incidents outside of the closed law enforcement community, while others did not like the political influence that was present in the program. In an attempt to allay the concerns, the ACTIC mandated that any individual who had access to sensitive information due to their assignment to the TLO program would be required attend training dealing with sensitive information and then sign a non-disclosure agreement.

The issue concerning political influence had roots in the grants and budgets of some jurisdictions. Law enforcement is typically a significant percentage of a jurisdictions budget. In many cases, the fire service and emergency medical services are significant percentages also. Individually, these groups exert influence over public safety service and funding, and they each have considerable influence. As the TLO program unifies the efforts of these public safety partners to address homeland security issues at the local, county, and state level, the partnership it creates a highly influential group with significant budgetary impact. Public safety managers typically pursue the same public safety dollars as their partner disciplines. In the TLO arena, this is not necessary. The TLO Program allows managers to unify their efforts and leverage their individual budgets to benefit the homeland security environment.

Many individual and agency agendas are affected by the TLO Program. The ACTIC and the TLO initiative can be seen as a direct threat to currently funded programs that focus on information sharing. Many entities create elaborate information sharing mechanisms that are not used. Experience has shown that many ISE initiatives are not used because they are developed, and then the public safety entities are engaged. Budgets trump collaboration. The TLO program focuses on the relationships between agencies and the creation of a trusted partnership.

The TLOs collect and report information and they focus their information collection based on the needs of the fusion center and the intelligence community. One issue related to collecting information involved the definition of parameters of the

specific information the ACTIC needed. To address this issue the ACTIC created and implemented a collection plan that provided direction concerning the specific articulable activities that the ACTIC needed information on. Examples of the information include terrorism, threats to public safety, crime trends and threats to critical infrastructure, among others. This information can be used to generate ACTIC products like alerts, watches, warnings and situational awareness bulletins.

When the ACTIC opened its doors it had an issue concerning the collection and maintenance of CI information. The Arizona Legislature passed a law assigning the responsibility for CI information and maintenance to DPS. DPS leveraged the ACTIC as the location where the data would be collected and secured. Each one of the CI facilities lies within a local, county or state jurisdiction that must respond to any and all emergencies at the facility. There is, or should be, an established relationship between the first response jurisdiction and the CI operator. The ACTIC leverages the TLOs in the jurisdiction to collect and conduct threat assessments. The TLOs use their TLO laptops to enter the data into the ACTIC's CI data systems. At the end of the day, these critical infrastructure and key resources are the specific locations where public safety focuses the majority of our terrorism prevention activities.

G. WEAKNESS OR FAILURE

There are specific areas of weakness that are associated with the TLO Programs intelligence, prevention, and protection subprograms. There are no matrices to measure the effectiveness of these programs. How would one measure the fact that an incident did not occur? The matrices that are produced tend toward the number of outreach programs or how many documents are created.

The TLO Program relies on the home jurisdiction of the TLO to ensure they are meeting the commitment to the program. Each jurisdiction that receives a grant funded level A or B TLO kit is required to sign a memorandum of agreement with the ACTIC that commits that the trained and equipped TLO will use the equipment to address ACTIC TLO issues, including information and intelligence exchange, CI protection, and on scene response. Public safety generally relies on a specific organizational structure to

address the areas for which it is responsible and accountable. The TLO Program is a network and does not have authority over the activities of its TLO partners.

One consequence of the TLO Program may be the dulling of specific public safety operational focus. Public safety professionals are authorized and funded to accomplish a specific goal (e.g., law enforcement, fire, emergency medical), and each of these professional capabilities is unique. While they are unique, they do each need a level of public safety information or intelligence to keep the community and themselves safe. One consequence of the program may be that the professions uniqueness may be blurred, and individuals and managers may come to think they can fulfill some or all or the roles of a partner discipline. Each of the different disciplines involved in the TLO program support the homeland security environment to some degree. One example is the fire service. The number of structural fires has declined significantly over the past decades for reasons including the fire services efforts in fire prevention, zoning, local ordinances, and codes along with new building materials. However, the TLO Program offers the fire service the opportunity to engage in homeland security activities that fulfill their missions in public safety and address the future threats to their jurisdictions.

The TLO Program has failed to bring two significant partners into the program as participants. Members of the FBI JTTF and DHS I&A, along with reports officers, do not participate as members of the TLO Program. The JTTF and the Department of Homeland Security I&A officers have two separate roles concerning terrorism. The FBI's Joint Terrorism Task Force is in place to address many of the investigative concerns with which the TLOs work. The DHS I&A officer is in place to engage the homeland security partners and ensure they get access to the information they have the right and need to have access to. The FBI and I&A officer instruct portions of the TLO basic course to new TLOs. The roles of the FBI and the I&A officer overlap in homeland security related information sharing. The JTTF focuses on investigations and oriented to address specific cases, while the DHS's I&A focuses on fostering an information sharing environment where everyone who should have information or have access to information gets that information or access. The TLOs actively work with both the JTTF and I&A officer throughout Arizona concerning their core capabilities and capabilities. The I&A officer

and FBI sit on the ACTIC Management Board and the intelligence committee; however, neither FBI JTTF special agents nor the I&A officer have attended the TLO class as a student. Both the FBI and DHS could build value and networked partnerships throughout Arizona's public safety community by attending the TLO school and becoming members of the network.

H. COMMITTEES

The ACTIC management board is the executive leadership group that addresses policy and budgeting of the ACTIC, including the statewide TLO program. The group is made up of executives from the agencies that participate in the ACTIC.

The TLO program has a standing committee in the ACTIC management structure. Statewide TLO training and policy is developed and recommended at the TLO committee level. The TLO program also has a standing meeting twice a month. The first meeting addresses situational awareness, program updates, and briefings, and second addresses training needs of the program.

The ACTIC also has an Intelligence Committee, which focuses on intelligence and information collection, analysis, and production. The TLO and Intelligence Committee work is implemented at the direction of the Management Board.

The TLO Committee focuses on the statewide TLO community. The core of the program is the capacities and capabilities that are represented by the participants. Each participant must successfully complete the TLO school. The basic TLO school is 40 hours of instruction and has been presented in different locations across the state to incorporate the greatest number of federal, state, local, and tribal participants. Upon successfully completing the school, the TLOs have the knowledge and network necessary operate as a FLO. They bring their own skills and ability to the network.

The Intelligence Committee focuses its efforts on engaging the ACTIC partners to consolidate the information and intelligence requirements of the state and its regions. Annually, the Intelligence Committee surveys Arizona's public safety community

concerning the priority information needs of each community that the ACTIC should focus on. The ACTIC survey focuses on 13 areas that the community rates as priorities.

These priorities are incorporated into the annual ACTIC collection plan. The collection plan is used by TLOs, analysts, and partner jurisdictions as they address incidents or suspicious activity. The information is reported, collated, and entered into the ACTIC database. The database is compliant with the federal regulation that focuses on state and local intelligence gathering. Individuals may understand the concept of suspicious activity. The collection plan gives specifics concerning suspicious activity and provides a framework for partners and analysts to identify, report, collate, and document what the community has identified as its priorities.

I. TLO HANDBOOK

The ACTIC TLO handbook is a public safety sensitive document that addresses specific duties, responsibilities, and capabilities of the TLO and the ACTIC. The handbook contains algorithms with if-then guidelines for TLOs who respond to calls across the public safety spectrum including bomb calls, SWAT support, suspicious substance calls, investigative support, and methods of identifying outstanding suspects. The handbook is also a guide for TLOs' as they address issues that for which the program is responsible. In addition, the handbook includes a phone roster, specific directions on intelligence, incident response, and operational security. The handbook ends with instructions on key items that a TLOs should consider to keep the members of their agency or jurisdiction safe as they address incidents.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. FUSION LIAISON OFFICER MODELS BY COMPARISON

Fusion centers across the country have established various forms of outreach and liaison programs. The programs are typically called terrorism (TLO), fusion (FLO), or intelligence liaison officers (ILO). Among homeland security practitioners, it is often said, "if you have seen one fusion center then you have seen one fusion center." This is especially true for fusion centers' individual liaison and outreach programs. Centers are owned, operated, and funded by states and major urban areas. Each fusion center that has created a liaison officer program has tailored the program to the serve its unique region. Many liaison officer programs include participants from private sector critical infrastructure along with their public safety core. There is no consistency among fusion centers about the way they engage their constituent jurisdictions. In addition, there are no baseline requirements for fusion center outreach. The common thread that is universal in fusion center outreach through liaisons is information sharing. Members of fusion centers know they must fulfill the task of creating an information sharing environment within the governance structure they operate in; however, there are no clear standards in relation to fusion center liaison and outreach programs that define success.

Each liaison officer program is unique and each fusion center trains its liaison officers to a different standard. Some centers provide an eight -hour basic course while others have a 24- to 40-hour course. Furthermore, liaison officers come from many state and local agencies. This creates a funding issue when the fusion center needs to address training. The ACTIC Program requires liaison officers to take a prerequisite course in 28 CFR Part 23 before the first day of class. This frees up two hours of the 40-hour course for other important topics. Additionally, many fusion centers incorporate the 23CFR Part 23 training in their classroom time.

The ACTIC leverages different Department of Homeland Security Grants to fund the training and equipping of the liaison officers. These funds come from the Phoenix Urban Area Security Initiative and Arizona's State Homeland Security Grant funds. The ACTIC TLO school is approved by the Department of Homeland Security so the ACTIC can use DHS funds to put on the course and the students can use travel funds to attend the

training that may be hosted in a different part of the state. To provide continuing education to the TLOs the ACTIC's annual TLO conference is partially funded with the use of homeland security grant funds.

This chapter will compare the ACTIC with two regional fusion centers and one statewide fusion center. The two regional fusion centers are the Central Florida Information Exchange (CFIX) and the Northern California Regional Information Exchange (NCRIC). The statewide fusion center is the Colorado Information and Analysis Center.

A. CENTRAL FLORIDA INFORMATION EXCHANGE

Florida is broken up into seven regional domestic security task forces. The Central Florida Intelligence Exchange (CFIX) represents region 5 and serves nine Florida counties in its region from its headquarters in Orange County. CFIX refers to their liaison officers as intelligence liaison officers (ILO).

The CFIX recruits ILOs from within the law enforcement, emergency services, and private sector entities. Similarly to the ACTIC, the CFIX ILOs report suspicious activity and disseminate CFIX products between their agency and the fusion center. In addition, the CFIX provides training including terrorism, organized group or gang recognition, critical infrastructure, intelligence rules, and regulations along with reporting and sharing information to those ILOs who come from law enforcement, emergency services, and government along with private organizations, such as Disney World, Epcot Center, and Universal Studios. The ACTIC has one statewide TLO coordinator who deals primarily with the public safety participants of the program. The CFIX focuses its coordination efforts in two areas. One focuses on the private sector while the other focuses on the public sector.

The CFIX implemented an Intelligence Liaison Officer Program with a focus on creating an information sharing environment based in the concepts of intelligence-led policing. The purpose of the CFIX ILO is to "provide local agencies within the region with an increased intelligence capability, and to enhance the concept of *intelligence led policing* by providing a regionally developed reporting and trend analysis capability to

our regional partners based upon ILO reports."[90] According to the CFIX's ILO Concept of Operations

> The goal is to make our government agencies (both law enforcement and non-law enforcement) *first preventers* rather than first responders, relative to the increase in violent and gang related crime, major organized theft, terrorism and other threats to our economy, citizens and visitors.[91]

The CFIX incorporates and trains public safety and private sector partners in their program. New public safety and private sector ILOs attend a 16-hour basic ILO course together, which "encourages networking and fosters the philosophy of intelligence sharing"[92] The ACTIC focuses its training efforts across the all hazards environment. TLOs receive an advanced course in the current national security threat environment, which is complimented with training in blocks of instruction on law enforcement and fire service special operations (SWAT, bomb, HazMat) along with the fusion centers expectation when TLOs respond to expanding incidents.

Part of the CFIX ILO program focuses on a private sector ILO program. Private sector ILOs are individuals at management level within their home organizations who would logically work with the fusion center. The private sector ILOs typically represent businesses that are part of the regions critical infrastructure and key resources. These private sector ILOs work with the emergency services and private sector coordinator at the CFIX. The CFIX model utilizes two coordinators to manage the programs participants. One coordinator works with law enforcement ILOs including police and sheriffs, and the other coordinator manages four sector specific coordinators who focus their efforts on their particular sector. These four specific sectors are fire (with emergency medical services), emergency management, public health, and the private sector. According to the Central Florida Intelligence Exchange:

> The ILO Program promotes the involvement of nominated individuals working in collaboration with other ILOs within the region of Central

---

[90] Central Florida Intelligence Exchange, *Intelligence Liaison Officer Program Concept of Operations* (Orlando, FL: Central Florida Intelligence Exchange, 2011), 3.

[91] Ibid., 3.

[92] Ibid., 8.

> Florida through a comprehensive prevention program. This program provides a platform to collect and share information and plan operations in relation to local and state hazards, threats and criminal activity. Information sharing will be facilitated through a clearly defined architecture to promote the sharing of information critical to the stakeholders of Central Florida's prevention, preparedness, and security efforts.[93]

Similarly to the CFIX, the ACTIC considers its professional firefighters, EMS, public health, and emergency management partners members of the ACTIC's public safety community. They are vetted by their agency and many pursue their security clearance as they begin participating in the program.

However, unlike CFIX, the ACTIC does not incorporate private sector partners in the TLO program. Also unlike the CFIX, the ACTIC created a separate program, the Community Liaison Officer Program, which focuses on outreach in a collaborative effort along with the Phoenix FBI's Infraguard coordinator and Arizona's protective security advisor from DHS's Protective Security Coordination Division.

B. COLORADO INFORMATION AND ANALYSIS CENTER

The Colorado Information and Analysis Center (CIAC) is Colorado's fusion center. The CIAC refers to its liaison officers as terrorism liaison officers (TLO). The TLO Program in Colorado also incorporates public and private sector representatives, as CFIX does. The CIAC maintains a TLO coordinator who coordinates the CIAC's activities with the TLOs that are spread throughout the state. According to Wolfinbarger, "The CIAC was designed as the State's (Colorado) fusion center to create cross-jurisdictional partnerships between local, state and federal agencies and to include private sector participants."[94] The intent is to further the information sharing efforts of the Department of Homeland Security, and the core capability associated with the CIAC TLO program is information sharing. The two way flow of information was created to

---

[93] Ibid., 10.

[94] *Statement of James Wolfinbarger Director/Major Colorado Department of Public Safety Office of Preparedness and Security Colorado State Patrol Homeland Security Branch Before the Committee on Homeland Security's Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment United States House of Representatives* (2007), http://chsdemocrats.house.gov/SiteDocuments/20071003133633-91688.pdf, 3.

share information between local, state, and federal agencies to address terrorism and criminal threats.

Similarly to the ACTIC, the CIAC TLOs serve as their agencies point of contact and fusion point in their jurisdiction and for the CIAC concerning information collection, reporting, terrorism training, information dissemination, and briefings to their respective chains of command along with regional partners. Additionally, they are their jurisdictions and their regions intelligence collection point in their agency who engages with the CIAC. Each CIAC TLO receives training in a variety of homeland security areas, including handling and safeguarding sensitive information, threats, intelligence, critical infrastructure protection, prevention activities, and CIAC databases.[95]

The CIAC TLOs are provided a list of specific target areas that the CIAC TLO can refer to when addressing their responsibilities. These lists are referred to as collection targets. Collection targets include terrorism, gangs, threat groups, various traditional and nontraditional organized crime groups, officer safety, threats, major incidents, and international incidents that have a local impact. The ACTIC refers to its collection targets in their annual collection plans which are similar to the CIAC's.

CIAC TLOs assist with threat and vulnerability assessments, which are conducted by a team they refer to as Rubicon. According to the Colorado Information Analysis Center:

> The Rubicon team is responsible for conducting full-spectrum integrated vulnerability assessments on Colorado's most critical infrastructure and key resources (CI). The assessments include detailed on-site inspections that identify vulnerabilities from an all-hazards approach, such as crime, natural disasters, sabotage, and acts of terrorism.[96]

This is similar to the ACTIC's Threat Mitigation Unit (TMU). TMU members are TLOs that become specialized in conducting threat assessments and working with the public or private sector entity to close any threat gaps with the use of technology or fixed defenses to protect the infrastructure.

---

[95] Colorado Information Analysis Center, *Terrorism Liaison Officer Handbook 2008* (Denver CO: Colorado Information Analysis Center, 2008).

[96] Ibid.

The CIAC publishes a TLO handbook. Each Colorado critical infrastructure sector is addressed in the CIAC TLO handbook. The threat to the infrastructure is explained and possible indicators of tactics and techniques are delineated for the CIAC TLO. This CIAC TLO handbook unifies the efforts of the TLOs and the Rubicon team at the CIAC.

The ACTIC's TLO handbook is called Arizona's *Terrorism Liaison Officer Field Operations Guide* (FOG). Each TLO is issued this pocket guide that consolidates the programs standard operating procedures into the FOG. The ACTIC's FOG goes into detail concerning TLO roles and responsibilities, which include topics like TLO operations in support of incident commanders in the field and expectations and capabilities of TLOs at expanding incidents.

C. NORTHERN CALIFORNIA REGIONAL INFORMATION CENTER

The state of California is divided up between five regional information centers. The fusion center in northern California operating in Sacramento is called the Northern California Regional Intelligence Center (NCRIC). The NCRIC has both a terrorism liaison officer and infrastructure liaison officer (ILO) program. A major focus of the NCRIC is to enhance communication between public safety organizations and the private sector.

The NCRIC TLO program incorporates homeland security related government agencies who engage in an information sharing environment with the fusion center. The NCRIC TLO "is limited to: Active Peace Officers, Firefighters, State Investigators, Federal Agents, Military Investigative personnel, or other government employees (working within the public safety /homeland security community) employed within the NCRIC's Area of Responsibility (AOR)."[97] NCRIC TLOs attend an introductory eight-hour course and have access to NCRIC data and information after completing the NCRIC's nondisclosure agreement.

[97] Northern California Regional Intelligence Center, "NCRIC Terrorism & Infrastructure Liaison Officer Programs," 2015, https://ncric.org/default.aspx?menuitemid=629

The ACTIC has a similar requirement which requires each TLO to sign and maintain a current nondisclosure agreement. Training on civil rights, civil liberties and information sensitivity is part of the ACTIC's basic 40-hour TLO school. The NCRIC represents northern California's entities and falls under the state of California police officers standards. The statewide training standard for a basic TLO in California is the California eight-hour course. This can be supplemented later with other training. The NCRIC provides training, communication, access to official use documents, memberships in the DHS federally supported NCRIC website on the Homeland Security Information Network creating an information sharing environment between ILOs, TLOs, and the NCRIC.

Similar to the ACTIC's Community Liaison Officer Program, the NCRIC has an Infrastructure Liaison Officer (ILO) Program that engages the private sector who are members of the CI community. "The standards for membership with the Northern California Regional Intelligence Center (NCRIC), Private Sector Partner Program are based on both a 'right' and a 'need' to know sensitive information connected to public safety."[98] The NCRIC staffs a private sector outreach program manager. This free program furthers their efforts in information sharing with their vetted private sector partners to meet the regions public and private sector information sharing needs.

The NCRIC is a signatory on the (California) State Threat Assessment System, which demonstrates the fusion centers commitment to "Standards and Procedures for Maintaining Criminal Intelligence Files and Criminal Intelligence Operational Activities."[99] The policy addresses information collection, maintenance, sharing, and destruction. Additionally, it discusses the "sharing of information with those responsible for Public Protection, Safety, or Public Health"[100] by allowing that "information retained by components may be disseminated to individuals in public or private entities only for

[98] Northern California Regional Intelligence Center, "Private Sector Partners," https://ncric.org/(X(1)S(ckgsc04y0xmtczcgbdbrwbpy))/default.aspx?menuitemid=105&menusubid=18&menugroup=NCRIC+Public+Home&AspxAutoDetectCookieSupport=1

[99] Northern California Regional Intelligence Center, State Threat Assessment System, *Information Privacy Policy*, 2014, https://ncric.org/html/CaliforniaSTTASPrivacyPolicy.pdf

[100] Ibid.

public protection, safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures"[101] The ACTIC maintains and trains on the privacy policy and also maintains and annually reviews a set of standing information needs, also known as a collection plan. The collection plan focuses on threats, hazards and issues. Threats include terrorism, special events, and some specific criminal acts that the fusion center collects information and intelligence on. Hazards include public health, natural events (e.g., fire, severe weather), and critical incident support. Issues involve strategic concerns of the partner agencies like gangs, weapons, narcotics, and crime trends. The ACTIC collection plan provides TLOs and ACTIC partners specific direction on what the fusion center is focusing its efforts and on what constituent entities to should report. Fusion centers can ask for liaisons or any reporting party to report suspicious information. Collection plans, like the ACTIC's, provide direction and guidance on what is considered suspicious to the fusion center and also lets the reporting party know what is being collected and analyzed by the center. Table 2 shows some comparisons between the four liaison officer programs.

Table 2. Liaison Officer Programs by Comparison

Liaison Officer Program Capabilities	ACTIC	NCRIC	CFIX	CIAC
Information Sharing and Exchange	√	√	√	√
On Scene Response	√			
Threat and Vulnerability Assessments	√			assist
Basic Liaison Officer Course	40 Hours	8 Hours	16 Hours	24 Hours

[101] Ibid., 11.

V. RECOMMENDATIONS AND CONCLUSION

Fusion centers pursue their individual goals and objectives. These goals and objectives may be addressed by taking one, two, or all three of the capacities of the ACTIC TLO program and using it as a conceptual model to replicate in part or as a whole to meet their needs. Nationally, fusion centers should move toward establishing a consistent and institutionalized relationship between the fusion center and its constituent agencies. There are models, including the models previously addressed in this thesis, from which urban areas and state fusion centers can take smart practices and then tailor their liaison officer program to meet the needs of the participant jurisdiction, the fusion center, and the federal government. These fusion center's state and local partners may be members of public safety, members of the military, emergency management, or members of the private sector. The capacity and capability of the liaison officer is only limited by the fusion centers commitment to expand on a baseline of capabilities to make the community safer.

The ACTIC TLO program unifies three separate capabilities. These capabilities are information and intelligence sharing, critical infrastructure protection, and on scene response. These specific capabilities continue to support the ACTIC and its partner jurisdictions as they address significant incidents across Arizona.

I recommend that the *Fusion Center Guidelines* broadly define a liaison officer program as a necessary component in state and major area fusion centers. This broad definition should mandate an information sharing network between the fusion center and its constituent entities, including partners from the public and private sector. I further recommend that the baseline capabilities for state and major urban area fusion centers be modified to make a liaison officer program a necessary component of achieving the baseline capabilities of a fusion center as assessed by the Department of Homeland Security.

Communities in the United States face a new generation of issues that must be addressed by their component agencies across the federalist landscape. The issues of

response, critical infrastructure, and trusted partnerships fall under an umbrella we now call homeland security. Addressing homeland security requires collaboration. Collaboration does not happen by accident. Hoping for collaboration at the scene of an incident is not a plan. If the word “hope” enters into a plan then there is no plan, there is simply hope.

The ACTIC TLO program has institutionalized public safety relationships. It has fostered a trusted partner relationship between individuals and their agencies that do not typically engage each other, other than at the scene of an extraordinary event. The ACTIC has been the unique environment that has allowed the distinctive network to have been created and matured.

The TLO program began with a concept and a core group of individuals who took the initiative and focused on the new generation of homeland security issues in Arizona. The ACTIC TLO model addresses many critical capabilities that are required of today’s fusion centers and may be a concept that other fusion centers can consider when as they attempt to build their capacity and capability to meet the needs of the homeland security enterprise.

Fusion centers across the country look to the ACTIC, the CIAC, the CFIX, and the NCRIC as examples of how multi layered and multijurisdictional relationships can be leveraged into a comprehensive and complex environment. These liaisons institutionalize a relationship between their agency, department, or entity with their fusion center. These programs are examples of how fusion centers have created their information sharing environments. The next step is to unify these efforts across the fusion center landscape.

The Department of Homeland security should add the requirement of a comprehensive liaison officer program to the fusion center baseline capabilities of each fusion that the Department of Homeland Security recognizes. This comprehensive program can be tailored to the needs of each of the fusion centers but at its core should have public safety representation from law enforcement, fire service, emergency medical, and public health. Fusion centers can add capabilities like conducting critical infrastructure assessments, responding to incidents, information collection, and others to

their program as they deem necessary. The key is institutionalizing the fusion centers relationships with their constituent partners thus ensuring information sharing.

DHS and the Department of Justice published the *Fusion Center Guidelines* in 2006,[102] and they published *Baseline Capabilities for State and Major Urban Area Fusion Centers* in 2008.[103] The documents focus on fusion centers achieving "baseline level of capability…"[104] Each document provides a vision of the elements that a fusion center should possess. There is little specific direction on how to achieve the vision. The ACTIC TLO Program embodies a majority of the envisioned capabilities listed in both documents.

The TLO Program addresses each of the following fusion center baseline capabilities for the ACTIC.

> 1. Intrastate Coordination—In developing and implementing all Fusion Process related plans and procedures, the center shall coordinate with other fusion centers (the designated state fusion center and/or any UASI fusion center(s)) within its state to identify the roles and responsibilities of each center in carrying out the Fusion Process (gathering, processing, analyzing, and disseminating of terrorism, homeland security, and law enforcement information) on a statewide basis.[105]

Participation in the TLO Program prevents jurisdictions from having to create their own fusion center. In addition, the TLOs from the states jurisdictions are trained and equipped the same.

> 2. Risk Assessment—Fusion centers shall conduct or contribute to a statewide and/ or regional risk assessment that identifies and prioritizes threats, vulnerabilities, and consequences at regular intervals.[106]

The TLOs are the trained and equipped professionals at fusion centers that conduct the assessments. The TLOs can use a computer that is linked with the ACTIC to enter the assessment into the current DHS system, and the TLOs can access the

---

[102] Global Justice Information Sharing Initiative. *Fusion Center Guidelines,* 3.

[103] DHS, and DOJ Bureau of Justice Assistance, *Baseline Capabilities*.

[104] Ibid., 10.

[105] Ibid., 12.

[106] Ibid.

assessment for incident commanders who respond to incidents where the assessment has been completed.

> 3. Information Requirements—The information requirements for the fusion center shall be defined, documented, updated regularly, and consistent with the center's goals and objectives as defined by the governance structure and reflect the risks identified in the statewide and/or regional risk assessment[107]

The TLOs are some of the contributors and agency representatives who are queried and surveyed on the risks and who provide the data concerning the risk assessment. The TLOs in Arizona are their jurisdictions representative to the ACTIC. The ACTIC conducts annual surveys on goals, priorities, and objectives of the fusion center. The fusion center, including the TLOs work with the DHS protective security advisor, reports officer, intelligence and analysis officer, and the FBI concerning statewide and regional threats including border related issues, special event and critical infrastructure.

> 4. Suspicious Activity Reporting (SAR)—Fusion centers shall develop, implement, and maintain a plan to support the establishment of a suspicious activity and incident reporting process for their geographic area of responsibility, in a manner consistent with the Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project. Specifically, centers shall have the ability to receive, process, document, analyze, and share SARs in a manner that complies with the ISE-SAR Functional Standard.[108]

The TLO are the operators and trainers for this program. They enter the SAR data or direct reporting parties to the data entry mechanism. In addition, TLOs respond to incidents and provide real time verifiable and credible information concerning active incidents in their respective jurisdictions.

> 5. Alerts, Warnings, and Notifications—Fusion centers shall ensure that alerts, warnings, and notifications are disseminated, as appropriate, to state, local, and tribal authorities; the private sector; and the general public.[109]

---

[107] Ibid., 13.

[108] Ibid.

[109] Ibid., 14.

The TLOs provide the mechanism where each member jurisdiction has a responsible party for accepting, reviewing, and addressing alerts, warnings, and notifications on behalf of their jurisdiction. The ACTIC relies on the TLOs to provide the statewide information sharing environment.

> 6. Situational Awareness Reporting—Fusion centers shall develop processes to manage the reporting to key officials and the public of information regarding significant events (local, regional, national, and international) that may influence state or local security conditions.[110]

TLOs are responsible and accountable to their home jurisdiction first, and they have an additional duty of engaging the fusion center concerning exceptional and special circumstances. The TLOs are also the professionals within an organization that the fusion center can reach out to and glean timely, credible, and accurate information. In addition, the TLO is the fusion center network that the ACTIC uses. A responsible party in each ACTIC partner jurisdiction across the state has been identified, trained, and vetted for this purpose.

> 7. Data Sources—Fusion centers shall identify and document data sources and repositories needed to conduct analysis based on the mission of the center, the findings of the Risk Assessment, and the center's defined Information Requirements.[111]

TLOs are the operators who have access to this data in repositories for their agencies across the state. The ACTIC has many data driven responsibilities, including facial recognition, INTERPOL center for Arizona, DHS risk assessments, special event threat mitigation video capabilities, and more.

The Maricopa County Sheriff's Office operates the facial recognition capability at the ACTIC. When there is a photograph of a suspect, the facial recognition unit can query the picture against millions of known images from a variety of databases. TLOs can leverage this capability when responding to incidents where suspects or victims are unknown, and there is a photograph. The unit requires an active investigation to query the database.

---

[110] Ibid.

[111] Ibid.

> 8. Coordination With Response and Recovery Officials—Fusion centers shall identify and coordinate with emergency managers and appropriate response and recovery personnel and operations centers to develop, implement, and maintain a plan and procedures to ensure a common understanding of roles and responsibilities and to ensure that intelligence and analysis capabilities can be leveraged to support emergency management operation activities, as appropriate, when events require such a response.[112]

TLOs respond to moderate and large scale (Tier I, II and III) incidents, and they provide a scalable asset that can be expanded to include missions supporting incident commanders on expanding incidents and emergency managers during mitigation and recovery efforts. National level exercise TOPOFF4 yielded a recommendation that TLOs be dispatched to EOCs in the affected jurisdictions along with the affected county and state EOC to facilitate information sharing and provide decision makers the intelligence and information that is necessary to respond to, address, mitigate, and recover from critical incidents.

> 9. Coordination With Private Sector and Critical Infrastructure and Key Resources (CI) Information Sharing—Fusion centers, in partnership with locally based federal authorities, shall develop, implement, and maintain a plan and procedures for sharing information with owners of CI and, in general, the private sector, in a coordinated manner.[113]

TLOs are the ACTIC's outreach to CI. They engage CI from the perspective of the local jurisdiction and the ACTIC. The TLOs work with the DHS protective security advisor to ensure there is a bridge between the national level governmental partners and the critical infrastructure partners that reside in the TLOs jurisdiction.

> 10. Exercises—Fusion centers should conduct or participate in another agency's scenario-based tabletop and live training exercises to regularly assess their capabilities.[114]

TLOs are operational assets assigned by their community as liaisons to the fusion center. Many are automatically dispatched to a standard list of calls and are requested to support any variety of incidents. They are actively engaged in the training and exercises

[112] Ibid.

[113] Ibid., 15.

[114] Ibid.

within their jurisdictions and are critical components of regional, statewide, and national level exercises, such as TOPOFF4, Coyote Crisis, Vigilant Guard for example. The TLOs provide the link between the incident management team, the fusion center, and the participating jurisdiction.

TLOs address many of the baselines concerning "information gathering/collection and recognition of indicators and warnings."[115]

> 1. Information-Gathering and Reporting Strategy—Fusion centers shall develop, implement, and maintain an information gathering and -reporting strategy that leverages existing capabilities and shall identify methods for communicating information requirements and the overall information-gathering strategy to partners, to include any applicable fusion liaison officers.

The TLOs are the backbone of this capability in Arizona, and they are provided the training and equipment to fulfill this role. Furthermore, TLOs respond to calls, report tips, and leads to the national suspicious activity reporting initiative and to the FBI through a system called e-Guardian. Moreover, the TLOs have a number of reporting mechanisms by which the reports can be made—through a web portal, by phone, or directly entered into the system with the use of a computer.

> 2. Feedback Mechanism—Fusion centers shall define and implement a feedback mechanism[116]

The TLO Program is the method that provides engagement and feedback from the jurisdiction and from the ACTIC. Survey is a mechanism that is used by the ACTIC. TLOs and other consumers are given the opportunity to address issues or concerns about ACTIC publications with the use of a survey tool that is hyperlinked to the end of each ACTIC intelligence publication. The ACTIC also conducts annual surveys of the TLOs for feedback and input concerning ongoing programs and future initiatives. The TLO Program hosts an annual conference where issues are addressed and relevant training is provided to address issues identified as the program receives feedback.

---

[115] Ibid., 16.

[116] Ibid.

> 3. Collection and Storage of Information—Fusion centers shall define the policies and processes and establish a mechanism for receiving, cataloging, and retaining information provided to the center.[117]

TLOs are signatories of non-disclosure agreements and are trained in the proper use of the collection and storage mechanisms of the ACTIC.

TLOs address many of the baselines concerning "process and collation of information."[118]

> Information Collation—Fusion center analysts shall use the necessary and available tools to process and collate information and intelligence to assist with accurate and timely analysis.[119]

The TLOs provide the ACTIC analysts the capability to engage and collect information from jurisdictional databases across the state through the use of a trusted network.

> 2. Levels of Confidence—Fusion centers shall liaise with partners to ensure that information collected is relevant, valid, and reliable.[120]

This is the intent of the TLO Program. Real-time, verifiable, and actionable information is exchanged throughout the state by the ACTIC and its TLOs.

TLOs address many of the baselines concerning "intelligence/information dissemination."[121]

> 1. Dissemination Plan—Fusion centers shall develop a high-level dissemination plan that documents the procedures and communication mechanisms for the timely dissemination of the center's various products to the core and ad hoc customers.[122]

The TLOs are a core capability for the fusion center and within a jurisdiction for dissemination. The TLO Program provides a vetted group of public safety partners across

---

[117] Ibid.

[118] Ibid., 17.

[119] Ibid.

[120] Ibid.

[121] Ibid., 18.

[122] Ibid.

Arizona. Each law enforcement agency, professional fire department, and sheriff's office has at least one and in most case many points of contact who are trained TLOs. One of the core missions that these individuals are trained in involves being their agencies point of contact for fusion center products. Furthermore, the TLOs responsibilities include digesting the fusion center products and further disseminating them to the operators and managers who require the information.

> 2. Reporting of Information to Other Centers—Fusion centers shall develop the processes and protocols for ensuring that relevant and vetted priority information is reported to fusion centers in other states and localities to support regional trends analysis.[123]

The TLO program is the mechanism that the ACTIC uses to identify relevant information and vet out priority information concerning incidents and events throughout Arizona. This information is translated into situational awareness bulletins, officer awareness bulletins, and similar documents for distribution to states, localities, and it supports regional trend analysis.

The ACTIC has a watch center that is staffed by ACTIC intelligence analysts and representatives from the partner agencies. The Watch Center is the hub for suspicious activity reporting in the state. Calls are answered 24 hours a day, seven days a week by ACTIC staff or the DPS duty officer. Suspicious activity reporting is documented in a database and the information is entered or forwarded to the appropriate federal state or local database. Examples of these databases include the DHS National Suspicious Activity Reporting database and the FBI e-Guardian system. As TLOs respond to incidents across Arizona, they notify and update the watch center of incidents. As incidents arise in jurisdictions, the watch center can contact the TLO and get a situational awareness briefing that can be shared with decision makers. As incidents expand, TLOs can work through the Watch Center to request ACTIC data (intelligence and information) and capabilities like HazMat, facial recognition, and computer forensics to name a few.

One example of the watch center's roles includes the method Arizona agencies use to address suspicious substances. Since the anthrax incidents of 2001 there have been

[123] Ibid.

public safety protocols in place in Arizona. The suspicious substance protocol addresses anthrax, ricin, or other suspicious substance calls for service across the state. The Arizona plan has matured over time. Incident responders determine if a suspicious substance is a possible threat or otherwise requires analysis by the state laboratory known as the Laboratory Response Network (LRN). The hazardous materials team members that are typically TLOs take possession of the substance and notify the watch center that they will be transporting the evidence to the LRN. The watch center provides a number specific tracking to the evidence. The law enforcement chain of custody is established concerning the item, which will be important for prosecution if the case is determined to be a criminal act. The LRN then notifies the watch center of the results of the tests. The watch center makes notifications to the partner jurisdictions.

> 3. Reporting of Information to Federal Partners—Fusion centers shall develop the processes and protocols, in coordination with the FBI and DHS Office of Intelligence and Analysis (I&A), for ensuring that relevant and vetted priority information is reported to the JTTF and other appropriate federal agencies to support its inclusion into national patterns and trends analysis.[124]

The TLOs report their jurisdictions SARs through the ACTIC. Additionally, the TLOs responsibility is to engage as their agencies representative to the ACTIC. TLOs in jurisdictions have federally-sponsored security clearances and can be briefed on cases on behalf of a jurisdiction or may be leveraged to support operations where participants need to be cleared. Tips and leads that are reported by the individual jurisdictions to the ACTIC are also entered into the FBI's e-Guardian system for accountability and follow up by the JTTF. Furthermore, the FBI and the JTTF use the ACTIC and the TLO program to distribute their regionally specific documents to the regions law enforcement and public safety agencies.

TLOs address many of the baselines concerning "reevaluation."[125]

[124] Ibid., 19.

[125] Ibid., 21.

> Performance Evaluation—Fusion centers shall develop and implement a plan to reevaluate the center's performance of the intelligence cycle on a regular basis.[126]

TLOs participate in a yearly ACTIC survey concerning intelligence, the collection plan, and the priorities of the ACTIC. Also, the TLO coordinator has a permanent seat on the ACTIC Intelligence subcommittee and participates in leveraging the TLOs to identify the information needs of their specific communities. When the specific needs of the partner jurisdictions change, the collection plan is changed to meet those needs. As members of the Intelligence Committee, the TLOs use a survey tool to reevaluate the intelligence cycle.

TLOs address many of the baselines concerning "management and administrative capabilities"[127]

> 1. Governance Structure—Fusion centers shall have a governance structure that provides appropriate representation for the jurisdictions and disciplines in the center's area of responsibility.[128]

The TLO program is the mechanism where individual jurisdictions engage with the fusion center. The jurisdiction is represented to the fusion center, and conversely, the fusion center is represented to the jurisdiction. Participating TLO jurisdictions have seats on the managing and executive boards of the ACTIC.

> Mission Statement—Fusion centers shall have a defined mission statement that is clear and concise and conveys the purpose, priority, and roles of the center.[129]

> According to Arizona Counter Terrorism Information Center:
>
> The mission of the Arizona Counter Terrorism Information Center is to protect the citizens and critical infrastructures of Arizona by enhancing and coordinating counter terrorism intelligence and other investigative

[126] Ibid.

[127] Ibid., 23.

[128] Ibid.

[129] Ibid., 24.

> support efforts among local, state and federal law enforcement agencies.[130]
>
> 3. Collaborative Environment—Fusion centers shall identify the organizations that represent their core (permanent) and ad hoc stakeholders and the roles and responsibilities of each stakeholder and develop mechanisms and processes to facilitate a collaborative environment with these stakeholders.[131]

The TLO program is the embodiment of this collaborative environment. It is the mechanism where jurisdictions can engage with the fusion center, public safety, critical infrastructure, and community partners to achieve the ACTICs mission.

> 4. Policies and Procedures Manual—Fusion centers shall develop a policies and procedures manual for center operations.[132]

The TLO program is incorporated into the ACTICs policies and the TLO Program maintains TLO training manual, TLO standing operating procedures, and TLO operations handbook for its participants.

> 5. Center Performance—Fusion centers shall define expectations, measure performance, and determine effectiveness of their operations.[133]

The TLO program supports this endeavor. Measuring expectations, performance measures and effectiveness of terrorism and crime prevention efforts is complex. The TLOs' activities provide for much of the measurable activity of the fusion center. Their performance measures include SAR documentation, e-Guardian entries, and subject matter expertise in critical areas.

Suspicious activity reporting by the community, public safety partners, and TLO partners exists at the ACTIC. The current system is an off the shelf product that had originally been built in support of the Silent Witness system. The ACTIC systems used to take in, document and assign suspicious activity reports have changed a number of times

---

[130] Arizona Counter Terrorism Information Center, "Mission / Vision," 2004, http://www.azactic.gov/About/Mission_Vision/ 2004

[131] DHS, and DOJ Bureau of Justice Assistance, *Baseline Capabilities*, 26.

[132] Ibid.

[133] Ibid.

since the ACTIC opened. When a suspicious activity report comes into the ACTIC it goes to the Watch Center. The Watch Center has contact with a TLO in each of the state highway patrol districts, each county sheriff's office and many police, fire, and EMS departments across the state.

> 6. Outreach—Fusion centers shall establish a policy to govern official outreach and communications with leaders and policymakers, the public sector, the private sector, the media, and citizens and develop a plan to enhance awareness of the fusion center's purpose, mission, and functions.[134]

The individual TLO is the face of the ACTIC in each home jurisdiction, with their home critical infrastructure and among the response community. The ACTIC houses Arizona's Community Liaison Officer Program (CLP). The mission of the CLP is to:

> provide a direct link between the state Counter Terrorism Center and the citizens, business community, and Tribal Nations in Arizona. Establishing and enhancing intelligence gathering and dissemination by any and all means available will make Arizona the safest and most prepared state in the nation.[135]

The Community Liaison Program (CLP) provides a link between Arizona's citizens, business, and tribal nations and the ACTIC. CLP's purpose is to make Arizona the most prepared state in the nation through information gathering and dissemination.[136]

The ACTIC has a fulltime community liaison program (CLP) officer, assigned from one of the ACTIC partner agencies, who manages the program and the ACTIC community outreach. The CLP officer is a graduate of the TLO basic school and presents the program to each basic TLO training session. This partnership incorporates a number of governmental agencies to unify community liaison initiatives, reduce duplication of effort, and increase membership. The unified program is called Arizona Partners for Arizona's Safety and Security (AZ PASS).

The ACTIC participates in AZ PASS along with the state's department of emergency management, Department of Homeland Security, Phoenix FBI Infraguard,

---

[134] Ibid., 26.

[135] Arizona Counter Terrorism Information Center, "Community Liaison Program (CLP)," 2015, http://www.azactic.gov/Community_Liaison/

[136] Ibid.

and private sector partners to foster an information sharing environment with participating businesses. PASS members are invited to participate in ACTIC programs concerning their particular critical infrastructure sector. The analysts at the ACTIC create products specifically for the AZ PASS community. These documents provide AZ PASS partners situational awareness and analysis on how trends may affect their community. Examples of AZ PASS situational awareness documents include computer hacking of the hospitality community or mass transit and public transportation security awareness.[137]

The TLO Program specifically addresses each of the following *Fusion Center Guidelines* for the ACTIC as published by DHS, DOJ, and the Global Information Sharing Initiative:

1. Adhere to the tenets contained in the *National Criminal Intelligence Sharing Plan* (NCISP) and other sector-specific information sharing plans, and perform all steps of the intelligence and fusion processes.
2. Collaboratively develop and embrace a mission statement, and identify goals for the fusion center.
3. Create a representative governance structure that includes law enforcement, public safety, and the private sector.
4. Create a collaborative environment for the sharing of intelligence and information among local, state, tribal, and federal law enforcement agencies, public safety agencies, and the private sector.
5. Utilize Memoranda of Understanding (MOUs), Non-Disclosure Agreements (NDAs), or other types of agency agreements, as appropriate.
6. Leverage the databases, systems, and networks available via participating entities to maximize information sharing.
7. Create an environment in which participants seamlessly communicate by leveraging existing systems and those currently under development, and allow for future connectivity to other local, state, tribal, and federal systems.
8. Develop, publish, and adhere to a privacy and civil liberties policy.
9. Ensure appropriate security measures are in place for the facility, data, and personnel.
10. Integrate technology, systems, and people.

[137] Ibid.

11. Achieve a diversified representation of personnel based on the needs and functions of the center.
12. Ensure personnel are properly trained.
13. Provide a multitiereed awareness and educational program to implement intelligence-led policing and the development and sharing of information.
14. Offer a variety of intelligence services and products to customers.
15. Develop, publish, and adhere to a policies and procedures manual.
16. Define expectations, measure performance, and determine effectiveness.
17. Establish and maintain the center based on funding availability and sustainability.
18. Develop and implement a communications plan among fusion center personnel; all law enforcement, public safety, and private sector agencies and entities involved; and the general public.[138]

A comprehensive TLO program fulfills many baseline capabilities for a fusion center, and it institutionalizes the relationships between the fusion center and its constituent agencies by satisfying many of the elements that make up the fusion center guidelines.[139] A comprehensive TLO program should be a requirement for any recognized state or major urban area fusion center that is recognized by the Department of Homeland Security.

[138] Global Justice Information Sharing Initiative. *Fusion Center Guidelines*, 5–7.

[139] Global Justice Information Sharing Initiative. *Fusion Center Guidelines*; DHS, and DOJ Bureau of Justice Assistance, *Baseline Capabilities*.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Central Florida Intelligence Exchange. *Intelligence Liaison Officer Program Concept of Operations*. Orlando, FL: Central Florida Intelligence Exchange, 2011.

Chen, Yi-Ru. "Tell Me What I Need to Know: What Mayors and Governors Want from Their Fusion Centers." Master's thesis, Naval Postgraduate School, 2009.

Colorado Information Analysis Center. *Terrorism Liaison Officer Handbook 2008*. Denver CO: Colorado Information Analysis Center, 2008.

Federal Emergency Management Agency. *Ready Business Mentoring Guide*. 2014. http://www.fema.gov/media-library-data/1392217307183-56ed30008abd809cac1a3027488a4c24/2014_business_user_guide.pdf

———. *Technical Assistance Catalog*. 2009. http://www.fema.gov/pdf/about/divisions/npd/npd_technical_assistance_catalog.pdf

Global Justice Information Sharing Initiative. *Fusion Center Guidelines*. Washingotn, DC: U.S. Department of Homeland Security, and U.S. Department of Justice, 2006. https://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf

Harwood, Matthew. "A Model of Intelligence Sharing." *Security Management*, April 1, 2012. https://sm.asisonline.org/Pages/A-Model-of-Intelligence-Sharing.aspx

Information Sharing Environment, and National Security Staff. *Strategic Implementation Plan for the National Strategy for Information Sharing and Safeguarding*. 2013. https://mise.mda.gov/drupal/sites/default/files/20140103%20Final%20NSISS%20Strategic%20Implementation%20Plan_0.pdf

Johnson, Bart R. "DHS Office of Intelligence and Analysis: Supporting the Front Lines of Homeland Security: Renewed Emphasis Designed to Improve Service to State and Major Urban Area Fusion Centers." *The Police Chief* 77, no. 2 (2010). http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=2011&issue_id=22010

Lowenthal, Mark M. *Intelligence from Secrets to Policy*. Los Angeles: Sage, 2012.

Lukin, Anthony. "Criminal Justice Terrorism Liaison Officer." California Emergency Management. August 22, 2011. Accessed January 20, 2012. http://www.calema.ca.gov/CSTI/Documents/Course%20Catalog/Terrorism%20Liaison%20Officer.pdf

Monaco, J. “Spying on First Amendment Activity: State-by-State.” American Civil Liberties Union. Accessed November 28, 2011. https://www.aclu.org/free-speech-technology-and-liberty/spy-files-spying-first-amendment-activity-state-state

McGhee, Sam. “Impacting the Evolution of Information Sharing in the Post-9-/11 United States.” *The Police Chief*, February 2015. http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display&article_id=3636&issue_id=22015

Napolitano, Janet. *Securing Arizona*: *A Roadmap for Arizona Homeland Security*. April 2003. http://azmemory.azlibrary.gov/cdm/ref/collection/statepubs/id/3089

National Commission on Terrorist Attacks upon the United States. *Final Report of the National Commission on Terrorist Attacks upon the United States*. New York: W. W. Norton, 2004.

National Fusion Center Partners. *Award of Excellence*. Washington, DC: National Fusion Center Partners, 2008.

National Network of Fusion Centers. *2014–2017 National Strategy for the National Network of Fusion Centers*. 2014. http://ise.gov/sites/default/files/National%20Strategy%20for%20the%20National%20Network%20of%20Fusion%20Centers%202014.pdf

Office of Intelligence and Analysis. *Office of Intelligence and Analysis Strategic Plan Fiscal Year 2011–Fiscal Year 2018*. Washington, DC: U.S. Department of Homeland Security, 2011. http://www.dhs.gov/xlibrary/assets/ia-fy2011-fy2018-strategic-plan.pdf

Peters, Katherine McIntire. “DHS-Supported Fusion Centers Raise Civil Liberties Concerns.” Government Executive. 2009. http://www.govexec.com/defense/2009/04/dhs-supported-fusion-centers-raise-civil-liberties-concerns/29076/

Phoenix Fire Department. *Strategic Plan 2014–2016*. https://www.phoenix.gov/firesite/Documents/strategicplan.pdf

Price, Michael. *National Security and Local Police*. Brennan Center For Justice. 2013. http://www.brennancenter.org/sites/default/files/publications/NationalSecurity_LocalPolice_web.pdf

Program Manager, Information Sharing Environment. *Information Sharing Environment, Annual Report to Congress*. June 2011. http://www.ise.gov/sites/default/files/ISE_Annual_Report_to_Congress_2011.pdf

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. https://www.hsdl.org/?view&did=16026

Salyers, Rickey L. and Troy Lutrick. “Best Defense.” *Fire Chief*, February 2011. 48–53. http://firechief.com/preparedness/firefighting_best_defense/

Saupp, Kevin. “Fusion Liaison Officer Programs: Effective Sharing of Information to Prevent Crime and Terrorism.” *The Police Chief Magazine*, February 2010. http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=2013&issue_id=22010

Simpson, Warren. *Dissemination Acknowledgement Form ACTIC Privacy and Procedures* Guide. Phoenix, AZ: Arizona Counter Terrorism Information Center 2010.

Stone, Adam. “National Fusion Center Model is Emerging.” *Emergency Management* (January 2015. http://www.emergencymgmt.com/safety/National-Fusion-Center-Model-Is-Emerging.html

U.S. Department of Homeland Security. “Fusion Center Locations and Contact Information.” January 2014. http://www.dhs.gov/fusion-center-locations-and-contact-information

———. *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection*. 2003. http://www.dhs.gov/homeland-security-presidential-directive-7#1

———. *Information Sharing Strategy*. Washington, DC: U.S. Department of Homeland Security, 2008). https://www.dhs.gov/xlibrary/assets/dhs_information_sharing_strategy.pdf

———. *National Network of Fusion Centers Fact Sheet*. August 6, 2014. http://www.dhs.gov/files/programs/gc_1296484657738.shtm

U.S. Department of Homeland Security, Office for Civil Rights and Civil Liberties. *Civil Liberties Impact Assessment for the State, Local and Regional Fusion Center Initiative*. 2008. https://www.dhs.gov/xlibrary/assets/crcl_civil_liberties_impact_assessment_12_11_08.pdf

U.S. Department of Homeland Security, and U.S. Department of Justice, Bureau of Justice Assistance. Baseline Capabilities for State and Major Urban Area Fusion Centers: A Supplement to the Fusion Center Guidelines. Supplement. Washington, DC: U.S. Department of Homeland Security, and Bureau of Justice Assistance, 2008. http://www.fema.gov/pdf/government/grant/2010/fy10_hsgp_fusion.pdf

U.S. Department of Justice. *The Attorney General's Report on Criminal History Background Checks*. 2006. http://www.bjs.gov/content/pub/pdf/ag_bgchecks_report.pdf

———. *Fact Sheet: 2009 National Fusion Center Conference*. Washington, DC: Federal Information & News Dispatch, Inc., 2009.

White House. *Sharing Information with State, Local, and Tribal Governments*. Washington, DC: White House, 2007. http://georgewbush-whitehouse.archives.gov/nsc/infosharing/

Yin, Robert K. *Applications of Case Study Research*. Thousand Oaks, CA: Sage, 2009.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California