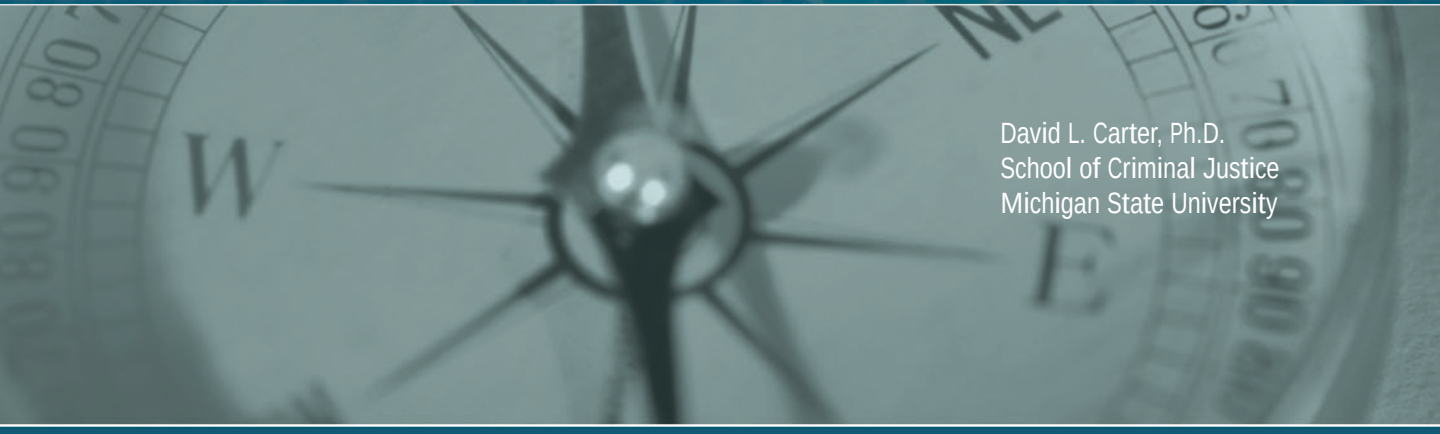
Law Enforcement Intelligence:

A Guide for State, Local, and Tribal Law Enforcement Agencies



David L. Carter, Ph.D.
School of Criminal Justice
Michigan State University

Law Enforcement Intelligence:

A Guide for State, Local, and Tribal Law Enforcement Agencies

November 2004
David L. Carter, Ph.D.

This project was supported by Cooperative Agreement #2003-CK-WX-0455 by the U.S. Department of Justice Office of Community Oriented Policing Services. Points of view or opinions contained in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice or Michigan State University.

Preface

The world of law enforcement intelligence has changed dramatically since September 11, 2001. State, local, and tribal law enforcement agencies have been tasked with a variety of new responsibilities; intelligence is just one. In addition, the intelligence discipline has evolved significantly in recent years. As these various trends have merged, increasing numbers of American law enforcement agencies have begun to explore, and sometimes embrace, the intelligence function. This guide is intended to help them in this process.

The guide is directed primarily toward state, local, and tribal law enforcement agencies of all sizes that need to develop or reinvigorate their intelligence function. Rather than being a manual to teach a person how to be an intelligence analyst, it is directed toward that manager, supervisor, or officer who is assigned to create an intelligence function. It is intended to provide ideas, definitions, concepts, policies, and resources. It is a primer-a place to start on a new managerial journey.

Every effort was made to incorporate the state of the art in law enforcement intelligence: Intelligence-Led Policing, the National Criminal Intelligence Sharing Plan, the FBI Intelligence Program, the array of new intelligence activities occurring in the Department of Homeland Security, community policing, and various other significant developments in the reengineered arena of intelligence.

A number of groups have provided important leadership in this field and afforded me opportunities to learn from their initiatives and experiences. These include the Global Intelligence Working Group (GIWG), Major City

Chiefs' Intelligence Commanders, High-Intensity Drug Trafficking Areas (HIDTA), Counterdrug Intelligence Executive Secretariat (CDX), the Counterterrorism Training Working Group, and the International Association of Intelligence Analysts (IALEIA). In particular, I also would like to thank the COPS Office, FBI, and Bureau of Justice Assistance.

Many people assisted me in this project. First and foremost are the members of my Advisory Board (listed in Appendix A). I appreciate your time, contributions, and expertise. You have added significant value to this work. I particularly thank Doug Bodrero, Eileen Garry, Carl Peed, Maureen Baginski, Tim Healy, Louis Quijas, and Bob Casey for their efforts.

My sincere appreciation also goes to Dr. Andra Katz-Bannister of the Wichita State University Regional Community Policing Institute (RCPI) who gave me constant feedback and support, Dr. Barry Zulauf at the Drug Enforcement Administration (DEA), who always manages to pull off the impossible, Merle Manzi, most recently of the Federal Law Enforcement Training Center (FLETC), who did a yeoman's job of reviewing and editing the manuscript in the waning hours of the deadline, and my Michigan State doctoral assistant, Jason Ingram, who assisted in many of the details and research needed for this project. My thanks also go to my COPS Project Monitor Michael Seelman who provided support and facilitation to get the project completed. Finally, I thank my wife Karen, and children Hilary, Jeremy, and Lauren who put up with the time I worked on this and other projects – you are always in my thoughts.

David L. Carter, Ph.D.
Michigan State University

Executive Summary

New expectations and responsibilities are being placed on law enforcement agencies of all sizes to develop an intelligence capacity as part of a cohesive national strategy to protect the United States from terrorism and the deleterious effects of transjurisdictional organized crime. As part of this trend, particularly after the events of September 11, 2001, unprecedented initiatives have been undertaken to reengineer the law enforcement intelligence function.

Adhering to National Standards

This guide is intended to provide fundamental information about the contemporary law enforcement intelligence function in its application to state, local, and tribal law enforcement (SLTLE) agencies. The guide embodies the Intelligence-Led Policing philosophy, demonstrating how it complements community policing already in use by American law enforcement. It also embodies the principles, ideology, and standards of both the National Criminal Intelligence Sharing Plan and the Global Justice Information Sharing Initiative. It reflects current issues of law, particularly with regard to intelligence records systems (as per 28 CFR, Part 23) and liability issues.

Definitions and Perspective

At the outset, this guide defines and illustrates law enforcement intelligence with respect to its current application to SLTLE. Because of different jurisdictional responsibilities, federal law enforcement agencies use slightly different definitions. These differences are explained and illustrated to enhance information sharing and ensure clear communications between federal and nonfederal law enforcement. Because of global terrorism, the presence of SLTLE officers on Joint Terrorism Task Forces (JTTF) and a more integrated role between the FBI and SLTLE, discussion is provided on the meaning and implications of national security intelligence as it relates to nonfederal law enforcement. To add perspective, the guide provides a brief history of law enforcement intelligence. Significant legal and policy implications have evolved through

This guide is intended to provide fundamental information about the contemporary law enforcement intelligence function in its application to state, local, and tribal law enforcement (SLTLE) agencies.

Moreover, critical issues are addressed ranging from ethics to responsibilities of line officers to the community's role in the intelligence function.

this comparatively short history, including perspectives from the 9/11 Commission. They are summarized at the end of Chapter 3 as lessons learned and framed as a checklist for policies and procedures that affect many aspects of the intelligence function.

To add perspective, the guide provides a brief history of law enforcement intelligence. There are significant legal and policy implications that have evolved through this comparatively short history, including perspectives from the 9/11 Commission. These are summarized at the end of Chapter 3 as "lessons learned." The "lessons" have been framed essentially as a checklist for policies and procedures that affect many aspects of the intelligence function.

Intelligence-Led Policing

The concept of Intelligence-Led Policing is explained from an operational perspective, illustrating its interrelationship with community policing and CompStat. Moreover, critical issues are addressed ranging from ethics to responsibilities of line officers to the community's role in the intelligence function. This discussion builds on the previous chapters to provide a perspective of intelligence that is "organic" to the law enforcement agency; that is, intelligence is part of the fabric of decision making that can have department-wide implications.

Intelligence Processes and Products

Based on the foundation that has been built, the guide explains current accepted practice of turning "information" into "intelligence." The intelligence cycle and analytic process are explained in summary form to provide the reader with an understanding of the processes. It is important for executives and managers to understand the language and protocols to effectively communicate with analysts and manage the intelligence function.

A discussion of information technology provides some insights into software requirements, networking issues, resources, security issues, and the dynamics associated with open-source information and intelligence.

This is followed by a discussion of intelligence products, the different types of intelligence analysis, and how these products are used for both operations and management. Finally, dissemination or information sharing-is discussed, particularly in light of the National Criminal Intelligence Sharing Plan.

Management and Human Resources

Readers of this guide will be experienced in management issues; hence, these sections focus on facets of management unique to law enforcement intelligence. Defining the mission, policy issues, and methods for staying current on trends and practices are addressed, paying particular attention to intelligence file guidelines and ensuring accountability of the intelligence function. As illustrated in the brief history of law enforcement intelligence, these two issues have been paramount, particularly as related to civil lawsuits. The importance of 28 CFR, Part 23, ***Guidelines for Criminal Intelligence Records Systems***, is stressed and model intelligence file guidelines prepared by the Law Enforcement Intelligence Unit (LEIU) are included in the appendices. Also included as an appendix is a comprehensive management audit checklist that touches on virtually all aspects of the intelligence function.

With respect to human resources, staffing is discussed, with particular emphasis on the need for professional intelligence analysts. In addition, intelligence training is examined and concludes with a summary of sources and contact information. These facets of management are consistent with the recommendations of the National Criminal Intelligence Sharing Plan.

Networks and Systems

In today's digital world, the heart of effective information sharing is an understanding of the various communications networks available to law enforcement – some are evolving as this is written. The guide presents information about critical secure networks and how law enforcement officers can gain access to the networks. An important recommendation is that all law enforcement agencies should have access to a secure

Defining the mission, policy issues, and methods for staying current on trends and practices are addressed, paying particular attention to intelligence file guidelines and ensuring accountability of the intelligence function.

Another significant change in law enforcement intelligence has been "intelligence requirements" produced by the FBI Intelligence Program.

communications system that is based on Internet protocols (IP). Intelligence products and advisories from federal agencies- the FBI and Department of Homeland Security (DHS) in particular – essentially rely on a secure IP system. The issues and processes are discussed in detail.

Intelligence Requirements and Threat Assessment

Another significant change in law enforcement intelligence has been "intelligence requirements" produced by the FBI Intelligence Program. Defining intelligence requirements adds dimensions of specificity and consistency to intelligence processes that previously had not existed. The guide describes the concept and processes in detail. Inherently related to defining intelligence requirements is understanding the threats posed in a jurisdiction. Indeed, the intelligence process is threat-driven with the intent of preventing a terrorist act or stopping a criminal enterprise and, therefore, the guide provides a threat assessment model.

Federal Law Enforcement Intelligence

The penultimate chapter describes federal law enforcement programs and products that SLTLE agencies should be aware of. Because of some confusion on the issue, the chapter begins with a discussion of classified information to clarify some confusion on the issue and provides information on how SLTLE officers can apply for security clearances. Based on the need for information security, the chapter also discusses declassified information for law enforcement, specifically related to the Sensitive But Unclassified (SBU) designation, the FBI Law Enforcement Sensitive (LES) designation, and the DHS For Official Use Only (FOUO) designation.

Building on the classification and information security issues, the guide discusses and illustrates the FBI Office of Intelligence products, FBI counterterrorism programs, and multi-agency initiatives–specifically the Terrorism Threat Integration Center (TTIC) and the Terrorist Screening Center (TSC). Equally prominent in the discussion are the intelligence products and advisories produced by the DHS. The FBI and DHS have established a productive working relationship on intelligence matters, embracing the need to be inclusive with state, local, and tribal law enforcement agencies for two-way information sharing.

Intelligence products and services as well as contact information also are provided for the Drug Enforcement Administration (DEA), El Paso Intelligence Center (EPIC), National Drug Pointer Index (NDPIX), National Drug Intelligence Center (NDIC), High-Intensity Drug Trafficking Areas (HIDTA), Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), the Financial Crimes Enforcement Network (FinCEN), and the High Risk Money Laundering and Related Financial Crimes Areas (HIFCA).

Summary

The intent of this guide is to aid state, local, and tribal law enforcement agencies to develop an intelligence capacity or enhance their current one. To maximize effectiveness, the standards used in the preparation of this guide were to ensure that it is contemporary, informative, prescriptive, and resource rich.

Summary of New Initiatives

- Development of the FBI Intelligence Program with its new emphasis on intelligence requirements, new intelligence products, and creation of the Field Intelligence Group (FIG) in every FBI Field Office as the primary intelligence contact point among state, local, and tribal law enforcement and the FBI.
- Development of new FBI counterterrorism initiatives and programs.
- New intelligence products from the Department of Homeland Security (DHS) as well as a substantive input role of raw information into the DHS intelligence cycle by state, local, and tribal law enforcement agencies.
- Expansion and articulation of the Intelligence-Led Policing concept.
- Implementation of the National Criminal Intelligence Sharing Plan.
- Creation of a wide variety of initiatives and standards as a result of the Global Intelligence Working Group (GIWG) of the Global Justice Information Sharing Initiative.
- Renewed vigor toward the adoption of 28 CFR Part 23, ***Guidelines for Criminal Intelligence Records Systems***, by law enforcement agencies that are not required to adhere to the regulation.
- Secure connections for email exchange, access to advisories, reports, and information exchange, as well as integration and streamlining the use of Law Enforcement Online (LEO), Regional Information Sharing Systems' RISS.net, and creation of the Anti-Terrorism Information Exchange (ATIX).
- New operational expectations and training opportunities for intelligence analysts, law enforcement executives, managers, and line officers.

Challenges to be Faced by Law Enforcement Executives

- Recognize that every law enforcement agency – regardless of size or location – has a stake in this global law enforcement intelligence initiative and, as such, must develop some form of an intelligence capacity in order to be an effective consumer of intelligence products.
- Develop a culture of collection among officers to most effectively gather information for use in the intelligence cycle.
- Operationally integrate Intelligence-Led Policing into the police organization.
- Recognize that increased information sharing at and between law enforcement at all levels of government requires new commitments by law enforcement executives and managers.
- Increase information sharing, as appropriate, with the broader public safety and private security sectors.
- Protect data and records along with rigid accountability of the intelligence function.
- Keep law enforcement intelligence and national security intelligence separate, particularly with respect to state and local officers on Joint Terrorism Task Forces.
- Broader scrutiny of intelligence records and practices by civil rights groups.
- Routinely use intelligence to make better tactical and strategic decisions.
- Increase regionalization in all aspects of the intelligence function as an ongoing initiative of law enforcement agencies at all levels of government.
- Ensure that non-law enforcement government officials and the community understand what law enforcement intelligence is and the importance of their role in the intelligence function.

Table of Contents

CHAPTER 1: INTRODUCTION 1

Perspective 3

CHAPTER 2: UNDERSTANDING CONTEMPORARY LAW ENFORCEMENT INTELLIGENCE: CONCEPT AND DEFINITION 5

Defining Intelligence 9

Definitions and Context 11

National Security Intelligence 14

CONCLUSION 17

CHAPTER 3: A BRIEF HISTORY OF LAW ENFORCEMENT INTELLIGENCE: PAST PRACTICE AND RECOMMENDATIONS FOR CHANGE 19

Law Enforcement Intelligence: The Years of Evolution 22

Early Intelligence Recommendations 26

Intelligence Recommendations in the Era of Public Investigations 27

Law Enforcement Intelligence at the State, Local, and Tribal Levels 29

Recent Developments: Law Enforcement Intelligence and the 9/11 Commission 33

LESSONS LEARNED 35

CHAPTER 4: INTELLIGENCE-LED POLICING: THE INTEGRATION OF COMMUNITY POLICING AND LAW ENFORCEMENT INTELLIGENCE 37

Intelligence-Led Policing 41

Ethical Issues 43

The Similarity to CompStat 43

The Flow of Illicit Commodities 45

Public Education 46

Civil Rights Issues 48

Community Members as Law Enforcement Volunteers 50

CONCLUSION 51

CHAPTER 5: THE INTELLIGENCE PROCESS 55

The Intelligence Cycle 63

INFORMATION MANAGEMENT AND INTELLIGENCE PROCESSES 64

Software to Aid the Intelligence Process 66

Information Technology Management 67

Information Technology Resources 70

Open-Source Information and Intelligence 70

CONCLUSION 74

CHAPTER 6: LAW ENFORCEMENT INTELLIGENCE CLASSIFICATIONS, PRODUCTS, AND DISSEMINATION 77
Intelligence Based on the Nature of Analysis 80
Intelligence Products 80
Operational ("non-product") Intelligence 81
Intelligence Based on the Orientation of the Analysis 83
DISSEMINATION 85
National Criminal Intelligence Sharing Plan 86
CONCLUSION 90
CHAPTER 7: MANAGING THE INTELLIGENCE FUNCTION 91
Establishing an Organizational Framework 95
"Chartering" an Intelligence Unit 97
IACP Model Policy on Criminal Intelligence 99
Adhering to 28 CFR Part 23 100
Auditing the Intelligence Function 100
Establishing and Managing Partnerships 101
Sources for Intelligence Management and Resource Trends 103
CONCLUSION 105
CHAPTER 8: HUMAN RESOURCE ISSUES 107
STAFFING 110
The Intelligence Analyst 110
TRAINING 111
Categories of Currently Available Intelligence Training Programs 115
Federal Bureau of Investigation College of Analytic Studies 115
Drug Enforcement Administration (DEA) 116
Federal Law Enforcement Training Center (FLETC) 116
General Counterdrug Intelligence Plan (GCIP) 118
IALEIA Foundations of Intelligence Analysis Training (FIAT) 118
Other Programs and Training Resources 118
INTELLIGENCE COURSES IN HIGHER EDUCATION 119
CONCLUSION 121
CHAPTER 9: NETWORKS AND SYSTEMS 123
Regional Information Sharing System (RISS) 126
Anti-Terrorism Information Exchange (ATIX) 128
Law Enforcement Online (LEO) 130
Law Enforcement Intelligence Unit (LEIU) 132
Information Sharing 133

Joint Regional Information Exchange System (JREIS) 133
Homeland Security Information Network (HSIN) 134
National Law Enforcement Telecommunications System (NLETS) 136
Accelerated Information Sharing for Law Enforcement (AISLE) 137
International Criminal Police Organization (INTERPOL) 137
Law Enforcement Information Sharing Program 139
REGIONAL INTELLIGENCE CENTERS 140
CONCLUSION 143
CHAPTER 10: INTELLIGENCE REQUIREMENTS AND THREAT ASSESSMENT 145
Filling Gaps/Fulfilling Requirements 148
Threat Assessments 150
FBI Intelligence Requirements Templates 152
CONCLUSION 153
CHAPTER 11: FEDERAL LAW ENFORCEMENT INTELLIGENCE 159
Classified Information 162
Sensitive But Unclassified (SBU) Information 164
DHS For Official Use Only (FOUO) Information 166
FEDERAL INTELLIGENCE PRODUCTS 166
FBI Office of Intelligence 167
FBI Counterterrorism 169
Specialized Counterterrorism Units 169
FBI Information Sharing and Operational Coordination Initiatives 170
Terrorism Threat Integration Center (TTIC) 170
Terrorist Screening Center 171
Consolidated Terrorist Screening Database 172
Department of Homeland Security 173
Intelligence Analysis and Alerts 173
Critical Infrastructure Protection 174
Cyber Security 174
Indications and Warning Advisories 175
Drug Enforcement Administration 180
Intelligence Products 181
El Paso Intelligence Center (EPIC) 182
National Drug Pointer Index (NDPIX) and National Virtual Pointer System (NVPS) 183
National Drug Intelligence Center (NDIC) 185
Intelligence Products 186

High-Intensity Drug Trafficking Areas (HIDTA) Regional Intelligence Centers .186
Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) 187
Financial Crimes Enforcement Network (FinCEN) 189
High Risk Money Laundering and Related Financial Crimes Areas (HIFCA) . . .191
Gateway 192
CONCLUSION 192
CHAPTER 12: SUMMARY, CONCLUSIONS, AND NEXT STEPS 195
IMPLEMENTING CHANGE: THE R-CUBED APPROACH 199
Reassessing 200
Refocusing 201
Reallocating 201
CONCLUSION 202
Appendices 203
A Advisory Board 204
B Law Enforcement Intelligence Unit (LEIU) File Guidelines 208
C Intelligence Unit Management Audit 224
D 28 CFR Part 23 248
E FBI Security Clearance Guidelines 264
F Biography of David L. Carter, Ph.D. 270
G Intelligence Unit Management Audit (Tear-Out Section) 274

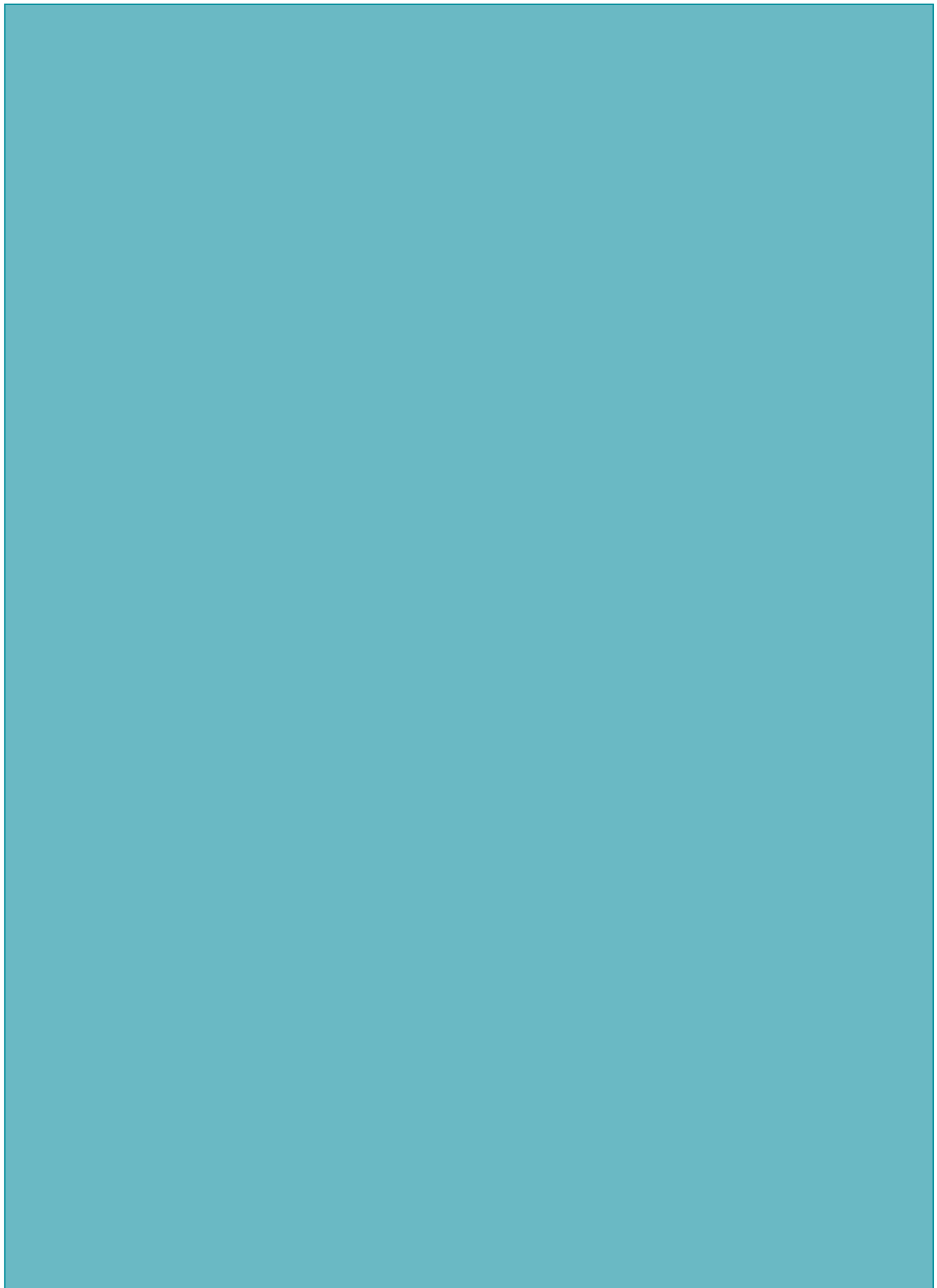
List of Figures

1-1 Diverse Information Collected for Intelligence Analysis 10
1-2 Comparative Illustrations of Information and Intelligence 11
1-3 Intelligence Community 15
4-1 Comparison of CompStat and Intelligence-Led Policing 43
4-2 Examples of Topics in Public Education Program 49
4-3 Examples of Actions the Public Can Take 49
4-4 Austin, Texas Police Department Civil Defense Battalion 52
5-1 Crime Triangle 59
5-2 Link Diagram Illustration 61
5-3 Commodity Flow Chart Illustration 62
5-4 Intelligence Cycle 64
5-5 FBI Intelligence Cycle Definitions and Processes 65
5-6 Illustration of Descriptive Map – Hate Groups in the U.S. 67
5-7 Illustrations of I2 Analysis Screens 68
5-8 Illustration of Open-Source News Stories on RISS ATIX 75
6-1 Fact Sheet – National Criminal Intelligence Sharing Plan 88
7-1 Sample Mission Statement and Goals of an LEI Unit 98
7-2 Sample Provisions for a Partnership Agreement 103
8-1 Intelligence Training Categories and Descriptions 114
9-1 Anti-Terrorism Information Exchange (ATIX) Welcome Screen 130
9-2 System Integration – HSIN Operations and Intelligence Integration 136
9-3 INTERPOL Notices 139
9-4 Law Enforcement Intelligence Network (Iowa) 141
9-5 Georgia Information Sharing and Analysis Center 142
10-1 Traditional Collection vs. Requirements-Based Collection 149
10-2 Threat Assessment Model for SLTLE 151
10-3 Intelligence Information Needs Template 154
10-4 "Baseline" Intelligence Information Needs Template 155
11-1 DHS and Intelligence and Threat Assessment Processes 176
11-2 DHS Operations Morning Brief 176
11-3 DHS Information Bulletin 177
11-4 DHS Physical Advisory 178
11-5 DHS Cyber Advisory 179

Introduction

1

CHAPTER ONE



Introduction

Every law enforcement agency in the United States, regardless of agency size, must have the capacity to understand the implications of information collection, analysis, and intelligence sharing. Each agency must have an organized mechanism to receive and manage intelligence as well as a mechanism to report and share critical information with other law enforcement agencies. In addition, it is essential that law enforcement agencies develop lines of communication and information-sharing protocols with the private sector, particularly those related to the critical infrastructure, as well as with those private entities that are potential targets of terrorists and criminal enterprises.

Not every agency has the staff or resources to create a formal intelligence unit, nor is it necessary in smaller agencies. Even without an intelligence unit, a law enforcement organization must have the ability to effectively consume the information and intelligence products being shared by a wide range of organizations at all levels of government. State, local, and tribal law enforcement (SLTLE) will be its most effective when a single source in every agency is the conduit of critical information, whether it is the Terrorist Intelligence Unit of the Los Angeles Police Department, the sole intelligence analyst of the Lansing, Michigan Police Department, or the patrol sergeant who understands the language of intelligence and is the information sharing contact point in the Mercedes, Texas Police Department. Hence, each law enforcement agency must have an understanding of its intelligence management capabilities regardless of its size or organizational structure.

This document will provide common language and processes to develop and employ an intelligence capacity in SLTLE agencies across the United States as well as articulate a uniform understanding of concepts, issues, and terminology for law enforcement intelligence (LEI). While terrorism issues are currently most pervasive in the current discussion of LEI, the principles of intelligence discussed in this document apply beyond terrorism and include organized crime and entrepreneurial crime of all forms. Drug trafficking and the associated crime of money laundering, for example, continue to be a significant challenge for law enforcement. Transnational computer crime, particularly Internet fraud, identity theft cartels, and global black marketeering of stolen and counterfeit goods, are entrepreneurial crime problems that are increasingly being relegated to SLTLE agencies to investigate simply because of the volume of criminal incidents. Similarly, local law enforcement is being increasingly drawn into human trafficking and illegal immigration enterprises and the often-associated crimes related to counterfeiting of official documents, such as passports, visas, driver's licenses, Social Security cards, and credit cards. Even the trafficking of arts and antiquities has increased, often bringing a new profile of criminal into the realm of entrepreneurial crime. All require an intelligence capacity for SLTLE, as does the continuation of historical organized crime activities such as auto theft, cargo theft, and virtually any other scheme that can produce profit for an organized criminal entity.

To be effective, the law enforcement community must interpret intelligence-related language in a consistent manner. In addition, common standards, policies, and practices will help expedite intelligence sharing while at the same time protecting the privacy of citizens and preserving hard-won community policing relationships.

Perspective

At the outset, law enforcement officers must understand the concept of LEI, its distinction from National Security Intelligence (NSI) and the potential problems an SLTLE agency can face when the two types of intelligence overlap. A law enforcement executive must understand what is meant by an "intelligence function" and how that function can be fulfilled

In addition, common STANDARDS, POLICIES, and PRACTICES will help EXPEDITE intelligence sharing while at the same time PROTECTING THE PRIVACY of citizens and preserving hard-won community policing RELATIONSHIPS.

through the use of different organizational models. Related executive decisions focus on staffing, particularly when there are fiscal limitations. What kinds of information does the law enforcement agency need (e.g., intelligence requirements) from the federal government to most effectively counter terrorism? How are those needs determined? How is the information requested? When and in what form will the information be received? Will a security clearance be needed to review the information that an executive requests? These are critical questions of a police executive.

From a policy and process perspective, what is meant by intelligence sharing? What information can be collected? What information can be kept in files? How long may it be kept in files? When does a person

transcend the threshold of exercising his or her rights to posing a threat to community safety? What resources exist to aid an SLTLE agency in accomplishing its intelligence goals? How can the entire law enforcement agency be integrated into the intelligence function? If a law enforcement organization is to be effective, the answers to these questions must be a product of written policy.

The intent of this document is to provide answers – or at least alternatives – to these questions. To begin the process, every law enforcement administrator must recognize that intelligence and information sharing can be effective in preventing terrorism and organized crime. To realize these ends, however, the intelligence process for law enforcement at all levels of government requires the following:

- Reengineering some of the organization's structure and processes
- Developing a shared vision of the terrorist or criminal threat
- Establishing a commitment to participate and follow through with threat information
- Overcoming the conceptual difficulty of intelligence processes that some personnel find difficult to grasp
- Committing resources, time, and energy from an agency to the intelligence function
- Embracing and using contemporary technology, including electronic access to information and an electronic communications capability through a secure connection
- Having proactive people using creative thought to identify "what we don't know" about terrorism and international organized crime
- Requiring a law enforcement agency to think globally and act locally
- Patience.