Protecting Your Community From Terrorism:

Strategies for Local Law Enforcement

Volume 4: The Production and Sharing of Intelligence

COPS
COMMUNITY ORIENTED POLICING SERVICES
U.S. DEPARTMENT OF JUSTICE

POLICE EXECUTIVE RESEARCH FORUM

Protecting Your Community From Terrorism: The Strategies for Local Law Enforcement Series

Vol. 4: The Production and Sharing of Intelligence

Stephan A. Loyka, Donald A. Faggiani, and Clifford Karchmer

with

Maureen Baginski
Daniel Bibel
Melvin Carraway
Stuart Kirby
Ritchie A. Martinez
Steve Sellers
John Sullivan

COPS
COMMUNITY ORIENTED POLICING SERVICES
U.S. DEPARTMENT OF JUSTICE

Police Executive Research Forum

This project, conducted by the Police Executive Research Forum (PERF), was supported by Cooperative Agreement No.2002-HS-WX-K001 with the U.S. Department of Justice Office of Community Oriented Policing Services. Points of views or opinions contained in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice or the members of PERF.

The opinions expressed reflect the general consensus of executive session attendees. However, not every view or statement presented in this report can necessarily be attributed to each participant.

The websites and sources that are cited provide useful information at the time of this writing, but the authors do not endorse any information of the sponsor organization or other information on the websites.

Police Executive Research Forum
Washington, DC 20036
United States of America
February 2005

ISBN 1-878734-87-3
Library of Congress Number 2005901063

Photos courtesy of (from top to bottom): Arlington County Police Department (1-3)
Federal Emergency Management Association (4)
PERF (5)

Cover Design by David Edelson, PERF

Interior Design based on a layout by Elliot Thomas Grant, etg Design

Contents

Chapters

Appendices

Acknowledgments

We would like to express our gratitude to the many individuals who contributed to this white paper. Any value it has is largely a result of their vision and commitment to improving how law enforcement entities gather and share information while continuing to support the tenets of community policing.

This white paper is the result of the guidance and support of the paticipants at the fourth executive session (in a series of five) made possible by the U.S. Department of Justice Office of Community Oriented Policing Services (COPS). We are grateful to Director Carl R. Peed for his continued recognition of the importance of these sessions and for his leadership. The successes of the sessions and the resulting white papers related to community policing in a security-conscious world are due in large part to the hard work, determination, and patience of Project Monitor Amy Schapiro.

We also are grateful to the following contributors: Executive Assistant Director, Maureen Baginski, Office of Intelligence, Federal Bureau of Investigation; Daniel Bibel, Program Director, Crime Reporting Unit, Massachusetts State Police; Melvin Carraway, Superintendent, Indiana State Police and Chairman of the Global Advisory Committee; Ritchie Martinez, Criminal Intelligence Analyst Supervisor, Arizona Department of Public Safety and former President of the International Association of Law Enforcement Intelligence Analysts; Major Steve Sellers, Commander, Criminal Investigations Bureau, Fairfax County (VA) Police Department; and John Sullivan, Sergeant, Los Angeles County Sheriff's Department.

Representatives from local, state, and federal law enforcement agencies participated in the session, and we thank them for their thoughtful and candid discussions about intelligence-led policing and the need for greater sharing of information in the face of the terrorist threat. A special thanks is due to Maureen Baginski, not only for her written contribution mentioned earlier, but also for her thorough and well-received presentation at the session. We also thank Deputy Attorney General of the United States James Comey for taking the time out of his busy schedule to discuss the pressing legal issues facing law enforcement agencies since September 11, 2001.

Several members of the PERF staff deserve our recognition. Executive Director Chuck Wexler was instrumental in getting the representatives from the various agencies to the same table as well as in facilitating the session. We thank Project Director Heather Davies for planning the session, taking notes, and providing critical feedback on this white paper. Research Assistant/Event Planner Anna Berke managed the complicated logistics of the two-day event. Lorie

Fridell, Director of Research provided significant comments on the development of this paper. David Edelson, working under a demanding schedule, did an outstanding job completing the layout and design of this white paper. Special thanks go to Barbara de Boinville and Martha Plotkin for their editing skills.

We gratefully acknowledge those of you in law enforcement—at every level of government—who work to keep us safe from terrorism. We hope this paper provides useful resources to assist you in your efforts.

Foreword

More than 30 years ago, crime-fighting techniques shifted from the traditional model of policing in the 1960s to the community policing principles of the 1970s. At that time the law enforcement profession witnessed a major change in how it combated crime. Police departments across the country began to work more closely with the communities they served in an effort to open lines of communication and generate information that could address the root causes of crime. These same community policing principles greatly contribute to law enforcement's counterterrorism efforts today. Facing a global threat of terrorism and another possible attack on U.S. soil, law enforcement agencies again are witnessing a major modification in how they deploy and utilize resources to fight both crime and terrorism. Local and state police, as first responders and as investigators, are working with their federal counterparts to create information-sharing initiatives that will enable all law enforcement agencies to help detect, prevent, and respond to a terrorist threat or attack.

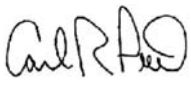
There are about 18,500 federal, state, local, and tribal law enforcement agencies in the United States, and each one has different operating procedures, service demands, and communities and infrastructures to protect. In the face of an ever-growing terrorist threat with potential ties to traditional crimes, such as drug trafficking and forgery, law enforcement agencies across the country are advancing intelligence-led policing as a principal philosophy. This intricate and analytical form of law enforcement is increasingly becoming viewed as necessary in the aftermath of the September 11, 2001 terrorist attacks. Agencies are recognizing that they need to be involved in developing reliable intelligence and need to work together to share that intelligence to achieve common goals. But budget constraints, technology deficiencies, inadequate training, and differing expectations can hinder a department's ability to meet the security needs of the community. That is why the federal branches of law enforcement and their local and state counterparts are working with new resolve to create resourceful and effective partnerships based on producing and sharing information and intelligence.

A crucial first step in this process is identifying and understanding the terrorist threat. When a threat is defined, an agency can better detail its needs and expectations, allowing for a structure

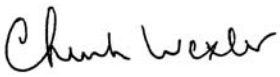
conducive to the exchange of information. Police chief executives in this country—now engaged in community policing—should understand the importance of working with their communities to produce information that can lead to solid intelligence. These local law enforcement officials, schooled in the fundamentals of community problem solving, are vital assets to the federal agencies tasked with the lead role in investigating terrorism. But the long-standing "wall" that has divided and hindered relationships between agencies at the federal, state, and local levels, particularly when it comes to intelligence, must be dismantled.

The Police Executive Research Forum (PERF), with funding from the U.S. Department of Justice Office of Community Oriented Policing Services (COPS), is making progress toward bridging these divisions. PERF has convened a series of forums for law enforcement leaders, antiterrorism experts, and policymakers to examine and discuss the best ways to share information and intelligence in a security-conscious world. This white paper is the result of the fourth executive session, which brought together counterterrorism experts from the Department of Homeland Security; the U.S. Secret Service; the Department of Justice; the Federal Bureau of Investigation; the Central Intelligence Agency; the Bureau of Alcohol, Tobacco, Firearms and Explosives; the National Security Agency; the Drug Enforcement Administration; National Oceanic and Atmospheric Association and state, county and local law enforcement officials. The white paper examines the challenges and concerns of the respective agencies as well as the progress they have made toward creating an integrated intelligence-sharing system. Conducted as an open forum for participants to share their ideas, the session provided insight on their approaches to such issues as how law enforcement executives develop intelligence functions within their departments, the difference between "information" and "intelligence," the move toward intelligence-led policing, and successful models that can be replicated across the country.

The COPS Office and PERF are pleased to facilitate these forums and to present concrete strategies that can help law enforcement agencies share information and integrate community policing and intelligence-led policing principles into their day-to-day operations.



Carl R. Peed
Director, COPS



Chuck Wexler
Executive Director, PERF

CHAPTER ONE

INTRODUCTION

SINCE THE ATTACKS OF SEPTEMBER 11, 2001, THE UNITED STATES HAS MADE significant strides toward strengthening homeland defense, improving emergency response, and reducing community fear. Agencies at the federal, state, and local levels are beginning to create positive working relationships with each other, and to integrate their strategies for responding to the threat of terrorism. They are recognizing not only the importance, but also the need for enhanced vertical and horizontal communications.

Law enforcement agencies have historically been charged with preserving the safety and security of the public. Regrettably, this mission is no longer limited to traditional crime—the prevention and deterrence of another terrorist attack on American soil have become a crucial part of this mission, leaving law enforcement agencies at every level of government responsible for restoring and maintaining a public sense of security.

How can law enforcement fulfill this new obligation successfully? What is the key to maximizing the probability of success in thwarting the next terrorist attack? The answer lies in the ability to know as much as possible about the threat in order to respond accordingly and efficiently. The answer is the use of reliable intelligence.

Identifying when, where, and how a terrorist attack will happen is tremendously difficult at best, yet this knowledge could save hundreds or maybe thousands of American lives. The most effective weapon in the war on terrorism is intelligence—the detailed analysis, evaluation, and interpretation of information. And the nucleus of this weapon is information collected and shared by federal, state, and local law enforcement agencies. Intelligence begins as bits of raw information or data. Information becomes intelligence when it is organized, analyzed, and interpreted with a specific focus. Without intelligence, agencies may be less than prepared to make the strategic and tactical decisions necessary to prevent and respond to critical incidents. This concept applies to both criminal and terrorist investigations.

The primary challenge for local law enforcement is understanding and then utilizing intelligence in a community policing context. Before information becomes intelligence, numerous questions must be answered. What information should be collected? How will it be analyzed and by whom? What information must be shared and what information must be kept confidential? How can information on individuals be collected without jeopardizing their rights as American citizens? These are just some of the issues that must

be addressed before good information can become useful intelligence. Yet the preceding questions cannot be answered apart from an examination of intelligence analysis itself. It is only with a clear comprehension of the analytic process that one can fully explore the subsequent collection and sharing aspects of the intelligence function. Identifying the central elements of a successful intelligence function will enable law enforcement agencies to generate practical solutions to the aforementioned challenges, establish rewarding intelligence functions specific to their needs, develop protocols for working with the Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS) and other federal agencies and eliminate barriers to sharing intelligence.

The Project: Community Policing in a Security-Conscious World

Since 2002, the Police Executive Research Forum (PERF),[1] with support from the U.S. Department of Justice Office of Community Oriented Policing Services (COPS), has conducted a project entitled "Community Policing in a Security-Conscious World." Together PERF and the COPS Office have convened a series of executive sessions for law enforcement chief executives, other policing professionals, government policymakers, and other stakeholders to explore, debate, and exchange information. These sessions provide law enforcement practitioners with opportunities to share and develop effective strategies for addressing terrorism while continuing to advance community policing. After the sessions, white papers on the findings are widely disseminated to law enforcement personnel and decision makers at all levels of government.

The first executive session was held on November 7–8, 2002, in Washington, D.C., and resulted in a white paper entitled *Protecting Your Community from Terrorism: Strategies for Local Law Enforcement, Volume 1: Local-Federal Partnerships*. The second volume, entitled *Working with Diverse Communities*, was the result of the second executive session held on June 5–6, 2003, in Chicago, IL. The third volume, *Preparing for and Responding to Bioterrorism*, was the result of the third executive session held in Los Angeles, CA, on July 24–25, 2003. (These documents are available for free download at www.policeforum.org or www.cops.usdoj.gov.) Following this white paper, the fifth volume will focus on law enforcement's partnership with the DHS. A sixth white paper, funded by the National Institute of Justice, is also planned on partnering to prepare for and respond to critical incidents.

The Executive Session on Intelligence and Information Sharing

On December 16–17, 2003, in Washington, D.C., PERF convened the fourth executive session of federal, state, and local law enforcement officials, intelligence experts, and academics from the intelligence and criminal justice fields. (See Appendix A for a list of participants and observers.) Moderated by Chuck Wexler, PERF's executive director, the session fostered a lively examination of strategies

[1] PERF, a nonprofit membership organization of progressive policing professionals, is dedicated to advancing law enforcement services to all communities through innovation and national leadership. Its members represent jurisdictions serving more than half of the nation's population, and the organization provides training, technical assistance, research, publications, and other services to its members and the profession. More information about PERF can be found at its website, www.policeforum.org.

for effectively integrating intelligence and information sharing with community policing. The discussion was particularly fruitful because participants had been asked, before the session, to find out what their intelligence officers and analysts considered to be the most pressing concerns related to information sharing. The primary discussion focused on the myriad challenges to effective intelligence collection and information sharing that plague local-federal partnerships, yet the session affirmed how important it is for law enforcement agencies to have an intelligence function for both criminal and terrorist investigations.

In addition to the difficulty of meeting local intelligence demands, participants discussed elements of effective intelligence units in jurisdictions such as Los Angeles and New York. Emphasis was placed on the factors that constitute productive intelligence and the manner in which multi-agency, multijurisdictional partnerships are cultivated. The session also included a critical assessment of available information-sharing resources.

The White Paper

This white paper, the fourth in the series, summarizes the comments of participants at the executive session on intelligence and information sharing. Volume One in the series, *Local-Federal Partnerships*, briefly explored the need for greater sharing of intelligence by agencies, organizational impediments to effective intelligence sharing, and local agencies' concerns about turf battles and security clearances. This paper builds upon that early discussion, stresses the importance of the intelligence function, and provides recommendations to law enforcement agencies for establishing a successful intelligence function. The goal of this white paper is to help local law enforcement agencies and others in the field identify the means and merits of producing and sharing solid intelligence and to provide recommendations for preventing future terrorist attacks through progressive, analytic policing techniques. After all, prevention starts first and foremost at the local level. This document is not meant to recommend a plan for the transformation of the federal intelligence community, nor does it outline a long-range plan the likes of those being formulated by other federal agencies. Rather it is a framework in which to consider more immediate actions that can be taken by state and local agencies and to focus on remaining challenges.

This volume is divided into four substantive chapters: What is Intelligence?, Intelligence-Led Policing, Developing a Successful Intelligence Function, and Recommendations. The chapters include several sidebar pieces written by executive session participants or law enforcement practitioners that provide more detailed accounts of selected programs or points of view.

CHAPTER TWO

WHAT IS INTELLIGENCE?

Intelligence and information are not the same—a distinction explored later in the chapter. First, one must understand the common illusions surrounding intelligence. These misconceptions are a proper starting point because they were discussed and, it is hoped, dispelled during the course of the executive session.

Illusions and Intelligence

It has become widely accepted that information sharing among government agencies and between levels of government is essential to preventing another catastrophic attack like that of September 11, 2001. Yet, a misconception persists on the part of the public, lawmakers, and even some in the law enforcement and intelligence communities that information sharing alone will be the miracle counterterrorism solution. Information sharing is critical for homeland security. It makes prevention possible by enabling a better national and local understanding of threats. Indeed, information sharing moves usable information gathered by federal, state, and local agencies to the national level and back down again. But the key to successful information sharing is that the information is usable. In order to enable this exchange, it is important that all the parties collaborating in the production and sharing processes be on the same page, conceptually as well as technologically.

Maureen Baginski, executive assistant director for the Office of Intelligence at the FBI, opened the executive session stressing many of these issues. Baginski oversees the collection, analysis, and dissemination of intelligence throughout the FBI and is responsible for integrating the intelligence function into all FBI investigative operations. She also serves as the primary FBI contact for the dissemination of information to (and receipt of information from) the intelligence community, state and local law enforcement agencies, and other government agencies, both national and international. The intelligence community is defined as "a federation of fifteen executive branch agencies and organizations that conduct intelligence activities necessary for the conduct of foreign relations and protection of national security."[2] Those agencies include the intelligence elements of the Army, Navy, Marine Corps, and Air Force; the Central Intelligence Agency; the Defense Intelligence Agency; the Department of Homeland Security; the Department of Energy; the Federal Bureau of Investigation; the National Geospatial-Intelligence Agency (formerly the National Imagery and Mapping Agency); the National Reconnaissance Office; the National Secu-

[2] See the Intelligence Community website at www.intelligence.gov.

rity Agency; the Department of the Treasury; the Department of State; and the Coast Guard.

The lead intelligence officer for the FBI, Baginski set the tone for the session in her discourse. Her remarks highlighted the urgent need to dispel the myths surrounding intelligence. For too long, the intelligence and law enforcement communities have had an uneven and at times antagonistic relationship fostered in part by such misconceptions. This was evident in the candid confessions of Baginski and several other law enforcement professionals in attendance. Commenting on her more than 25 years of experience working for the National Security Agency, Baginski acknowledged the intelligence community's view of law enforcement as an unknown, and those at the session who had made a career in law enforcement cited similar skepticism with respect to the intelligence community.

The reasons for any doubts or misinterpretations are understandable. The two communities differ in their core responsibilities and objectives, not to mention in their expectations regarding information acquisition and management. Moreover, the contemporary cultures of the two communities were shaped by very different experiences. The intelligence community evolved from a Cold War mentality—an approach rooted in rigid command and control and orchestrated behind a veil of secrecy. As participants at the executive session pointed out, the law enforcement community has unfortunately been beset by scandals as a result of improper and overreaching domestic intelligence activities. As a result, the distance between the law enforcement and intelligence communities widened further. But this relationship is necessarily changed by the nature of the threat we now face. The responsibilities and expectations placed on the law enforcement and intelligence communities correspond and even intersect today.

> ***"The important question is why agencies need to generate an intelligence function. The answer is to enable better, more informed decision making."***
>
> ***—Melvin Carraway, Superintendent, Indiana State Police***

Toward the end of her address, Baginski posed the question to law enforcement officials in attendance, "What worries you most?" She immediately followed that inquiry with two more questions. "What do you know about that threat? And, more importantly, what don't you know about that threat?" The simple questions she raised highlight the need for and value of intelligence as a tool for making sound decisions.

Intelligence as a Tool for Making Decisions

Intelligence is not something that is only collected by covert agents attempting to subvert another government or organization, or even prevent attacks on our own government. This view is antiquated and no longer valid. The truth is, the collection and analysis of intelligence is no longer limited to government agencies. Today intelligence functions are widespread. The desire to execute insightful, calculated decisions transcends mission, sector, or industry. Most large organizations need a formal capacity to determine whether threats in their respective environments should become the subjects of executive policy consideration. Corpora-

tions seeking to maintain or increase their market share collect information on market fluctuations, consumer trends, and their competitors. They do so to achieve their desired goal through informed decision making. Herbert Meyer, a former administrator in U.S. intelligence, concisely delineates what executive session participants were trying to convey about the meaning of intelligence today:

> Intelligence has broadened to become organized information. More precisely, intelligence has come to mean information that has not only been selected and collected, but also analyzed, evaluated and distributed to meet the unique policymaking needs of one particular enterprise. It is this transformation of what has been collected into finished, polished, forward-looking analytic products designed to meet the unique policymaking needs of one enterprise—and the organizational effort required to do it—that marks the difference between what intelligence used to be and what it has become (Meyer 1987).

Physicians are trained to diagnose a patient before initiating a medical intervention. They gather information in order to improve their chances of properly diagnosing and curing a problem. So should law enforcement design and conduct their operations blindly? The answer is plainly, no. Executive session participants—federal, state, and local officials alike—agreed that the indispensable reward of intelligence analysis is an improved, informed decision-making process. Like other professionals, law enforcement executives need information that will not only facilitate the development of effective responses, but also enable their proper execution and provide a measurement of success. Law enforcement intelligence ultimately supports three specific types of decision making—strategic, operational, and tactical.[3] Tactical decisions—like those made regarding specific crime-fighting measures—are critically important.

Intelligence as a Tool for Fighting Crime

During the two-day session, some questioned whether attention was being disproportionately directed at Islamic extremism, neglecting traditional crime responsibilities—and homegrown terrorist threats. Other participants drew the discussion back to the nexus that exists between traditional crime and terrorism. They cited fraudulent identifications, trafficking in illegal merchandise, and drug sales as means to terrorists' ends. The "ends" or goals are simple—kill, destroy, and disrupt. But the complexities of the new threat necessitate a fundamental change in law enforcement priorities—not simply toward terrorism but toward an intelligence-based approach.

For law enforcement, intelligence constitutes an actionable inference or a set of related inferences derived from some form of inductive or deductive logic. By combining information, analysis, and interpretation, intelligence helps to document a threat, ascertain its probability of occurring, and define a responsive course of action, all in a timely manner. Good information, analyzed and evaluated in a timely manner, can provide the details necessary for developing the most efficient and productive strategies for disrupting a drug or crime syndicate, preventing a terrorist attack, or addressing any number of evolving crime prob-

[3] See Carter 2002 for a discussion of the types of decision making supported by intelligence.

lems. In a country fighting terrorism, intelligence provides a means to unravel and intercept terrorist plots or to define countermoves. In the world of law enforcement today, intelligence is good crime analysis applied in a new context.

Executive session participants mentioned COMPSTAT[4] as a good example of how law enforcement can turn information into one form of intelligence for fighting crime. The COMPSTAT process, developed and first implemented in the New York City Police Department (NYPD) in 1994, collects and analyzes crime data.[5] This "intelligence-led" strategy enabled the policymakers in New York City to position key resources where they would have the greatest impact. The result was a relatively quick and dramatic reduction in violent and drug-related crimes.

> ***"Terrorism can and does manifest itself in traditional criminal activity."***
>
> ***—Melvin Carraway, Superintendent, Indiana State Police***

[4] For more information on the COMPSTAT process at the NYPD and crime mapping as a law enforcement tool, see the NYPD website at http://www.ci.nyc.ny.us/html/nypd/html/chfdept/chief-of-department.html and the National Institute of Justice website at http://www.ojp.usdoj.gov/nij/maps/pubs.html. For additional information on regional crime mapping and case studies on how mapping has been successfully applied, see LaVigne and Wartell (1998, 2000, 2001).
[5] See Steinert-Threlkeld (2002).

A MODEL OF FEDERAL, STATE, AND LOCAL INFORMATION SHARING

by Major Steve Sellers, Commander, Criminal Investigations Bureau, Fairfax County (VA) Police Department

Shortly after September 11, 2001, the Fairfax County Police Department realized the importance of establishing a Criminal Intelligence Unit (CIU) to address not only traditional criminal intelligence, but also the real possibility of domestic and international terrorists in our midst. Fairfax County, a diverse jurisdiction of over one million residents, lies just west of Washington, D.C., and is home to the Central Intelligence Agency, near the Pentagon, and close to many other sensitive agencies seen as potential targets. Immediately upon establishment of the CIU, the department strengthened relationships with its federal partners in the intelligence field. Fortunately, many of these relationships were already solid because of previous joint criminal investigations and the close proximity of the department to the nation's capital. However, the international or foreign intelligence arena was relatively new to the agency, and required additional collaborative efforts. All per-

sonnel selected for the CIU were handpicked for their experience, interpersonal skills, and ability to establish and maintain effective working relationships.

One of the first steps taken by the department was to shift the administrative control of detectives assigned to the Joint Terrorism Taskforce (JTTF) from the Major Crimes Division to the CIU. This change established the first link to federal intelligence resources and eventually led to new ties to experts in the field. Second, the department broadened its relationships with other federal agencies like the U.S. Attorneys Office, Immigration and Customs Enforcement at the Department of Homeland Security, the Central Intelligence Agency, the Department of State, the Social Security Administration, and various military intelligence installations. Eventually, these collaborations yielded joint investigative work. Through their work together on criminal cases of common interest, detectives, federal agents, and analysts developed trust. Strong working relationships between federal, state, and local authorities in the world of intelligence are paramount to effective information sharing. The walls of mistrust must be systematically broken down. In the end, effective communication depends on the people who are selected to participate and lead our intelligence efforts.

Once the issue of trust was addressed, the CIU members applied for federal top-secret clearances. Although not necessarily required for police intelligence functions, top-secret clearances reduce the complexities inherent in sharing classified information. Clearances generally took anywhere from 12–16 months to obtain.

The same commitment to relationship-building also applies to community involvement. Many years ago the Fairfax County Police Department established the Auxiliary Police Officer Program and later the Volunteer in Police Services (VIPS) program. Both programs draw upon Fairfax County citizens interested in giving back to the community by volunteering their time with the department. Some members of the Auxiliary Police and VIPS programs were already actively engaged in full-time intelligence jobs with a variety of federal agencies. Shortly after September 11, 2001, the CIU drew upon this pool of experienced intelligence professionals and reassigned them to the CIU. In addition, the VIPS coordinator conducted an active recruitment effort to seek more experts in the field. Today, the CIU has 19 active VIPS officers and 14 auxiliary police officers. Most of them have extensive intelligence experience and appropriate security clearances. The use of experienced police volunteers not only extended the department's capabilities and staffing, it also opened doors to multiple federal agencies and fostered communication.

The next step toward improved information sharing was the integration of operational functions. Federal partners from the Secret Service and FBI were invited to move into the department's intelligence office. Integration of daily activities (working in the same office) resulted in mutual trust and an environment open to sharing information. Later, a more developed plan of integration emerged with the newly established National Capital Regional Intelligence Center (NCRIC). The NCRIC, managed by the Fairfax County Police Department and funded by the FBI,

draws upon multiple federal, state, and local law enforcement and intelligence organizations to work under one roof. The NCRIC outlined plans to incorporate a Watch Desk, an operational component, and an analysis component staffed by multiple agencies. This system of integration ensures adequate information sharing within the entire Washington, D.C., metropolitan area.

Effective and timely information sharing is the responsibility of law enforcement leaders. They must be judicious in determining who will operate the intelligence function within their agencies. Information sharing occurs faster and more efficiently at the supervisory and line levels. Some police leaders are quick to blame federal administrators for failing to share important information. In many cases, however, the fault may lie within the department and its own selection of personnel to perform the intelligence function. Trust is forged at the supervisory and line levels when law enforcement and federal agencies integrate operations and work together on a daily basis. These steps have helped to ensure an effective and efficient information-sharing model for the Fairfax County Police Department.

The Difference between "Information" and "Intelligence"

David Carter, a professor of criminal justice at Michigan State University and an observer at the executive session, has written extensively with colleagues on the merits of law enforcement intelligence, defining it as "...the product of an analytic process that provides an integrated perspective [about] disparate information about crime, crime trends, crime and security threats, and conditions associated with criminality" (Carter and Holden 2002). He makes an important distinction between information and intelligence: "In the purest sense, [the term] intelligence information is an inaccuracy since information is raw data and intelligence is the output of the analytic process" (Carter 2002).[6]

Throughout the executive session, some participants used the terms "information" and "intelligence" interchangeably. It is a misconception to view intelligence as simply pieces of information about people, places, or events that may or may not hold some significance in determining criminality. One of the objectives of the executive session was to ensure these terms were used properly so all participants would have a common understanding. By insisting on this distinction early on, the moderator succeeded in promoting a more focused and accurate dialogue.

Meyer's (1987) intelligence model outlines four stages of the intelligence process: determining requirements based on a comprehensive threat assessment, collecting relevant and usable information, analyzing the data and developing an appropriate response, and finally, assessing the

[6] Carter and Holden (2002) and Carter (2004) are also sources for more information on how local law enforcement can apply intelligence and community policing principles in furtherance of homeland security goals.

effectiveness of the intelligence and decision-making processes. Some analysts believe that this process can best be understood as a linear progression. The first two stages are processes concerned with information, while the last two stages are processes based on intelligence and rooted in analysis. In the middle of this continuum, would be a brick wall with a window for passing the end product of the information processes to the beginning of the intelligence process. This would be the only point where the two processes meet, according to this theory. Ideally this process should be cyclical though, with the end intelligence product in turn influencing what is being collected next.

Information is essentially raw data, either qualitative or quantitative. There may be some analysis involved, but it is generally of a descriptive nature. In law enforcement, the information is what a crime analyst might use to identify, for example, a drug hot spot. Reports of drug use or sales in a specific area would be the information gathered, but when scrutinized and examined against the spatial analysis of multiple reports, the information becomes more revealing. The investigator may then take the analysis from the crime analyst and use it in conjunction with other information—witness statements, personal experience, or knowledge from those dealing with other drug markets—and apply it to a case or another specific threat. Competent analysis organizes and interprets the data in a framework determined by intelligence requirements or specific gaps in knowledge. Only after bringing all the information and analysis available together does the investigator have the "intelligence" to make an interpretive decision about a strategic, tactical, or operational plan of action.

Executive session participants agreed that intelligence is key to discovering what is unknown about an identified threat. But in order to generate reliable intelligence and produce results that are applicable to that specific problem, the information feeding the analytic process must be collected in a manner consistent with an individual's or agency's needs. In other words, beginning with quality information is paramount to achieving a successful end product. As will be explained later, executive session participants emphasized that departments cannot establish a successful intelligence function without promoting quality collection, and quality collection is driven by an agency's particular needs or requirements for information.

> ***"Requirement-driven collection is the key to success."***
>
> ***—Barbara Cart, Executive Assistant, Homeland Security Office, National Security Agency***

Each stage of this process may require separate technology, personnel, training, and educational commitments. Assessing what needs to be known and defining the techniques for collecting these data can rely on a process that is very different from that used for transforming the information into a finished product and providing policymakers with the findings. On the surface, the technology used to archive, transfer, and process the information and intelligence may seem similar and banal—a simple computer terminal, for instance. However, below the surface, different software, manuals, and paperwork can be driving the effort. More importantly, in front of that terminal there may be analysts with different training and skill sets than the information collectors.

Executive session participants noted that the awareness of the distinction between "information" and "intelligence" shed light on the misconception that information sharing will enable an immediate resolution to problems of crime and security. Participants also agreed that whether the information is efficacious in resolving the problems of crime and security depends on its quality.

Types of Intelligence[7]

Much of the confusion about the meaning of the term "intelligence" can be attributed in part to the absence of a clear delineation between national security intelligence and law enforcement intelligence.

Participants agreed that national security intelligence is what typically comes to mind when a person hears the term "intelligence." This type of intelligence is focused on identifying and neutralizing external threats posed by foreign powers, organizations, or now transnational actors like terrorists. They seek to undermine or disrupt the social, political, and economic relationship between the United States and the rest of the world. Historically, utilizing and producing this intelligence have been the responsibility of organizations like the Central Intelligence Agency, the National Security Agency, and the Defense Intelligence Agency. The FBI has important national security intelligence responsibilities stemming from jurisdiction over espionage and counterintelligence and, more recently, terrorism.

Strategic intelligence provides detailed information on the overview of criminal activity, groups, and threats, enabling broader departmental policy planning and resource allocation. Ongoing strategic intelligence keeps officials alert to threats and potential crimes. The information gathered, analyzed, and disseminated helps police understand the structure, characteristics, motivations, and philosophy related to specific intelligence targets. Strategic intelligence is what most agencies lack. Participants noted, however, that operational and tactical intelligence, without strategic intelligence to put it in an overarching plan or context, is not as productive as it could be.

Operational intelligence is the type used most often by law enforcement agencies. It guides operational decisions about how to maintain public safety. Operational intelligence can justify monitoring individuals who may pose a threat to public safety, but care should be exercised to avoid overstepping domestic surveillance restrictions and other intelligence-gathering limitations. Executive session participants suggested that this can be accomplished through clearly defined policies and procedures set forth by agency executives. (The Department of Justice guidelines established by the Code of Federal Regulations [specifically, 28 CFR 23 et seq.] were drafted to accomplish just that. They carefully proscribe what information cannot be collected.)[8] Policymakers need to become familiar with the laws governing domestic surveillance and intelligence gathering—most notably the USA PATRIOT Act and a presidential directive, Executive Order 123333. These authorities expand the role and capacity of law enforcement to gather information and intelligence. The potential con-

[7] Definitions of strategic, operational, and tactical intelligence are based largely on the work of David Carter (2002; 2004) and Carter and Holden (2002).

[8] For more information on 28 CFR, see the General Printing Office website, www.gpoaccess.gov, or the FBI website, www.fbi.gov.

cerns about privacy and individual rights surrounding domestic surveillance and other intelligence gathering, as well as the bad taste left by several law enforcement agencies' misjudgments in the past few decades, have made some departments wary. Executive session participants, however, warned their colleagues against discounting the value of operational intelligence and choosing not to actively pursue their other inteligence functions because of the potential legal ramifications, and because it is still an essential tool for maintaining community security.

Tactical intelligence is used in either the formulation of an ongoing criminal investigation or in threat mitigation during a crisis situation. This is the type of intelligence involved in what police commonly refer to as "raid planning." Tactical intelligence is most often gathered as a case-building instrument, yet in a crisis situation it can offer insight concerning the nature of both the threat and the target. Tactical intelligence also helps police effectively manage a response. In the case of a precise terrorist threat to an identifiable target it can help police move decisively to prevent the attack.

While the distinction between national security intelligence and law enforcement intelligence was discussed among participants at the executive session, they recognized the increasing overlap in the new dynamic that our nation faces following the attacks of September 11, 2001. The proliferation of threats that transcend national borders and conventional tactics (for example, suicide bombers and chemical attacks) understandably muddy the terminology. There is a clear nexus between the two forms of intelligence in dealing with terrorists living and breaking the law in our own cities, towns, and counties. It is perhaps most evident now that traditional criminal enterprises that engage in such activities as drug trafficking and money laundering in the United States are funding international crimes committed by multinational organizations. Recently, individuals engaged in cigarette smuggling on a massive scale to raise funds for a terrorist organization were prosecuted. As this example shows, intelligence that improves national security is intelligence that improves law enforcement efforts, and vice versa.

DATA QUALITY AND USABILITY

by Daniel Bibel, Program Director, Crime Reporting Unit, Massachusetts State Police

The following quote from the website of the West Midlands Police Department in the United Kingdom provides a good introduction to the topic of data quality and usability:

> Management of data requires time, authority, resources and expertise to complete the tasks necessary to help ensure that...data (and the information extracted from it) is of

such quality as to make it reliable, trusted by those who use it, effective in...policing... and looked upon as a priceless asset rather than an administrative burden.[9]

Police administrators are data consumers, just like the administrators and managers in any organization. In order to make rational decisions, plan strategies, and assess outcomes, they need to have timely, accurate, reliable, and valid data. Whether crime is up or down, and no matter how many calls for service come in, decisions need to be made concerning all the elements that make up an executive's business practice. These decisions relate to employee scheduling, routine maintenance of vehicles, and budgeting, in addition to things commonly understood to be police matters. Whether these decisions are effective will be determined in large part by the data used to make them.

Data are part of the basic building blocks of an information system, but data alone ("raw data") are not enough for the police executive. To enable effective decision-making, data must be combined with value and meaning in order to transform it into actionable knowledge. The quality of our results (output) depends in great measure on the quality of our data (input). "The integrity and reliability of data-based analysis and reporting depend, in large part, on the quality of the underlying data." (Whitaker n.d.)

There are a number of internal checks on the quality of data. These checks are generated, maintained, and used within an agency. On a very basic level, the data must "fit" the requirements of the data systems in use. Standard codes or abbreviations are used for certain data elements. Most computer systems have built-in checks to eliminate the entry of totally incorrect data. For example, a number cannot be entered in a computer field that requires a letter, and a street address that does not exist within a jurisdiction cannot be entered into a computer-aided dispatch system.

In the best situation, the data within the agency will be used creatively and productively for administrative, operational, or tactical purposes. The more the data are used, the better the quality of the data should become, as errors in coding or content are detected and corrected. This feedback loop is a necessary component of any system for collecting quality data. Although software can perform some level of error checking, the knowledge of an experienced individual is essential in quality control. The process of case review is therefore critically important in a quality data system. Data may still be "wrong" (that is, it may be incomplete or missing), but the data can nonetheless be useful within a department. Officers in an agency may understand where to go when dispatched to "Red's Garage," even without a specific street address given. The age, race, or sex of a particular person may be missing in a report, but the person could be well known to the department. Variations in spelling may be acceptable, since everyone "knows" what is being referenced. As long as the mistakes or errors are consistent, the data may be meaningful and useful.

[9] See www.west-midlands.police.uk/

The use of data for intelligence and information sharing creates a new set of issues and concerns. An agency may have reasonable data quality standards (and have a good understanding of the limitations of its own data), but when the agency's data must be shared with a group of agencies, questions about the reliability and accuracy of the shared data elements often arise. So-called "cooperative information systems" demand greater scrutiny from all the agencies involved.

Eck (2002) describes five potential sources of error in crime data: citizen reporting differences, agency recording variations, event classification, inconsistent descriptive information, and geocoding accuracy. Citizen reporting differences may be outside the control of agency management, but each of the other factors should be managed by the agency.[10] Donald Faggiani, Dan Bibel, and Diana Brensilber (2001) mention a sixth source of error, the department's lack of appreciation for the utility of their data. Without this understanding of and appreciation for the value of data, it is unclear whether the resources needed to provide quality data will be made available.

Each of these factors will have an impact on the reliability and validity of an individual police department's data. When several police agencies attempt to merge their data, the cumulative error rate will be much greater. It may be assumed that all agencies use the same coding system for data elements, or that a standardized look-up table exists to map the different values. Similar data elements, however, may not have the same meaning or significance. Different agencies may have different standards for reporting or processing events. One department may enter only the most serious offense in an incident, while an adjoining department enters all offenses. The case review process may be expedited in Department A while Department B delays 24 hours before sign-off. In another set of agencies, citizens come forward to report a high percentage of all offenses, whereas a neighboring department with poor community relations receives a much smaller proportion of offense reports. In any one of these examples, the potential for cooperative information sharing will be greatly reduced. Agencies must be aware of this, and continue to move the intelligence function along accordingly.

---

[10] Even citizen reporting behavior may well be within the control of police if efforts are made to improve police-community relations and to encourage crime reporting.

CHAPTER THREE

INTELLIGENCE-LED POLICING

It was commonly accepted among the executive session participants that local law enforcement agencies need help in reengineering their intelligence function. Discussions focused on what was lacking at various agencies, whether it was resources, technology, or qualified personnel. Some participants contended that these were secondary issues. The more central issue was the need to foster a more analytic approach to policing—an approach driven by intelligence.

National Criminal Intelligence Sharing Plan

In March 2002, law enforcement executives and intelligence experts attending the International Association of Chiefs of Police (IACP) Criminal Intelligence Sharing Summit, funded by the Office of Community Oriented Policing Services (COPS), called for the creation of a coordinated criminal intelligence council to develop a national criminal intelligence sharing plan. In response to this need, the Global Justice Information Sharing Initiative (Global),[11] a federal advisory committee of the U.S. Department of Justice, formed the Global Intelligence Working Group (GIWG) funded by the Office of Justice Programs (OJP) to act as an interim council to coordinate intelligence and information sharing recommendations. The GIWG, the IACP and OJP incorporated best practices and recommendations from across the country into the National Criminal Intelligence Sharing Plan (NCISP). The NCISP is the result of participation and feedback from local, state, tribal, and federal law enforcement. The plan contains model policies and standards for leveraging existing infrastructures for sharing criminal intelligence across all levels of government. It provides a cohesive vision and practical solutions to improve law enforcement's ability to detect threats and protect communities. The chairman of the Global Advisory Committee at this writing is Superintendent Melvin Carraway of the Indiana State Police. At the executive session, he played an instrumental role by informing the group about the NCISP, which has been endorsed by the U.S. Department of Justice, the Department of Homeland Security, and myriad law enforcement groups. A core recommendation of the Plan is the promotion of *intelligence-led policing*.

[11] For more information on the National Criminal Intelligence Sharing Plan and the 2002 International Association of Chiefs of Police Summit that initiated the effort, see http://it.ojp.gov//topic.jsp?topic_id=8 or the IACP website at www.theiacp.org.

GLOBAL JUSTICE INFORMATION SHARING INITIATIVE

by Melvin Carraway, Superintendent, Indiana State Police

Local law enforcement is still defining its role in addressing the ongoing terrorist threat. While some new approaches, technologies, and skills are needed, police professionals have a solid foundation in community policing, problem solving, and innovative crime control. The focus of law enforcement is and always will be crime-based. Law enforcement in America is adept at preventing crime and disorder, addressing citizens' fears and needs, uncovering leads, interviewing suspects and witnesses, reviewing evidence, gathering statements, and finding patterns. Police will draw on these skills to collect and analyze new or different types of intelligence in light of the terrorist threat. Managers and policy makers must reinforce the premise that good police work can uncover all types of crime patterns—including terrorism. The key to their success will be providing them with the information and intelligence—as well as the means to share what they observe with others engaged in counterterrorism—they need to detect terrorist activity.

Community policing has promoted interagency trust, partnerships, and the value of information. Daily newspaper headlines attest to the effectiveness of local law enforcement community policing efforts in both mitigating and providing solutions to problems, preventing crime and violent acts, and helping to instill a sense of security within communities. The necessary evolution of community policing following the attacks of September 11, 2001 inevitably leads to preventing and responding to the effects of terrorism. Strengthening citizen partnerships with patrol officers and using their information to detect and arrest those who would harm our communities is a natural outgrowth of community policing. We must utilize the combined efforts of all public safety agencies' resources and build on their community policing successes to prevent another terrorist act from taking place. Agencies must assess their deficiencies in information sharing, the incompatibilities of information sharing technologies, and the inconsistencies of procedures and policies that prevent the effective sharing of information and intelligence.

With these tenets as a framework, a new initiative has been underway to improve information and intelligence sharing between federal, state, local, and tribal agencies engaged in counterterrorism. GLOBAL, the "group of groups," represents more than 30 justice-related organizations. We have been laying the foundation for an environment where trust is cultivated and technology is enhanced to aid all members of the justice community. The National Criminal Intelligence Sharing Plan (NCISP) highlights actions and recommendations that federal, local, state, and tribal law enforcement agencies can follow to implement successful information and intelligence sharing approaches. A community of law enforcement experts from operations, training, analysis, policy, and security participated in the development of its recommendations.

Law enforcement agencies, regardless of size, should adopt the minimum standards of intelligence-led policing outlined in the NCISP. The standards focus on the intelligence process and include elements such as the mission of the function, management and supervision, personnel selection, training, security, privacy rights, development and dissemination of intelligence products, and accountability measures.

GLOBAL has published several products recently that advance and reinforce the need for information sharing standards. These publications include security practices, justice information privacy guidelines, and the Global Justice Extensible Markup Language (XML) Data Model (Global JXDM).

The Global JXDM is an XML standard designed specifically for criminal justice information exchanges, providing law enforcement, other public safety agencies, prosecutors, public defenders, and other judicial entities with a common language to effectively share data and information in a timely manner. The Global JXDM is designed to increase the ability of justice and public safety communities to share information at all levels, laying the foundation for local, state, and national justice interoperability. The Global JXDM is a comprehensive product that includes a data model, a data dictionary, and an XML schema. Through the use of a shared vocabulary that is understood system-to-system, Global JXDM enables access from multiple sources and reuse in multiple applications. As of October 2004, more than 50 law enforcement and justice-related projects have been implemented using the Global JXDM, demonstrating its flexibility and stability.

The justice community is moving toward interoperability and enhanced intelligence production and information sharing, and Global continues to do its part. For more information regarding the Global Justice Information Sharing Initiative, please visit the U.S. Department of Justice Office of Justice Programs website at www.it.ojp.gov/index.jsp.

The Philosophy of Intelligence-Led Policing

Intelligence-led policing is based on a common understanding of intelligence and its usefulness. At the executive session, Superintendent Carraway noted the NCISP recommends a standardized definition of intelligence-led policing. The Plan defines it as "the collection and analysis of information to produce an intelligence end-product designed to inform police decision making at both the tactical and strategic levels." The NCISP adds that for intelligence-led policing to be effective, it must become an "integral part of an agency's philosophy." Intelligence-led policing is a management orientation in which intelligence serves as a guide to operations, rather than the reverse. Managers must be prepared to deviate from traditional policing philosophies—a move to action rather than reaction. They must understand and trust that operations can and should be driven by intelligence. Intelligence-led policing is innovative and, by some standards, even radical. Above all, it requires commitment.

DEFINING WHAT WORKS: A CASE STUDY FROM THE UNITED KINGDOM IN INTELLIGENCE-LED POLICING

by Stuart Kirby, Detective Chief Superintendent, HQ Crime and Operations Division, Lancashire Constabulary

Situated in the Northwest of England, the Lancashire Constabulary, an agency of 5,600 staff (3,600 sworn), initiated intelligence-led policing in the early 1990s when examination revealed indiscriminate use of resources did little to improve public confidence or to reduce and detect crime and disorder. The Constabulary seized the opportunity to be one of the lead forces in the countrywide implementation of the UK National Intelligence Model (NIM). It predicted that the uniform implementation of an evaluated intelligence process would be significant, not only across its own operational areas but also when dealing with other police forces.

Initially the Constabulary had to ensure they complied with the NIM requirement to put critical personnel in place, such as analysts, researchers, and intelligence officers. Similarly, systems and technical capacity were enhanced to collate intelligence from a variety of sources. Here the Constabulary developed "Sleuth," a data warehousing system, which presents such timely information as known individuals (arrests and intelligence), recorded crime, recorded incidents, forensic information, domestic violence data and statistics, missing individuals, and other high-interest people—tailored to individual area or officer needs.

Although the NIM process works at level 3 (national issues), the Constabulary employs the model predominantly at level 2 (cross-border issues within the Constabulary or between neighboring forces); and level 1 (local neighborhood level). At each level a strategic assessment is completed, which sets out current and emerging crime and disorder issues. These assessments are presented and discussed at a Strategic Tasking and Co-ordinating Group (STCG) meeting. At the Constabulary level (level 2) STCG, Chief Constable Paul Stephenson meets with other Chief Officers, Divisional (local) Commanders, and heads of administrative departments to agree on a control strategy, which in effect are the priorities for the force. Similarly Divisional Commanders, influenced by these priorities, meet with their own senior management team and set the local (level 1) priorities. While these meetings set, monitor, and review the strategic agenda, they are supported by a Tactical Tasking and Co-ordinating meeting group who decide the best methods for implementing the STCG's wishes. At all of these meetings actions are carefully recorded and allocated to specific individuals who are required to return and report on them.

An illustration is perhaps the best way to show how the process works. During 2001, while reviewing operational performance at the force monthly STCG, a Divisional Commander explained that a number of persistent offenders were driven to steal by their cocaine addiction, creating a new hot spot. As there appeared some consensus on the increased availability of the drug, Chief Con-

stable Paul Stephenson commissioned a problem profile on the issue. The problem profile,[12] together with target profile,[13] tactical assessment,[14] and strategic assessment[15] (mentioned earlier) are the four most relied upon of the analytical products described by the NIM. Once the problem profile was commissioned, HQ Intelligence staff set the data collection plan requiring local intelligence units to supply information on such issues as amount and type of drug seizures, locations, offenders and victims. The collection plan also requested that personnel interview persistent offenders to understand their lifestyle, and contact other partners (i.e., health and drug professionals) for their perspective.

The completed "problem profile" was presented at a later STCG meeting and as a result class A drugs and drug-related criminality were made a priority of the control strategy. Prompted by the NIM, the Lancashire Constabulary then devised its strategic response in three areas: further intelligence gathering, enforcement, and prevention.

In relation to enforcement, Operation Nimrod, a systematic and targeted test purchase operation was formed to focus on open drug markets. From 2002–2004, this has resulted in the execution of 4,000 warrants, the seizure of £500,000 worth of drugs and 400+ offenders sentenced collectively to more than 1,000 years in prison. The consistency of the model also allowed improved regional and national collaboration, which resulted in interagency enforcement activity on trafficking routes. Other tactical activity also supported these strategic responses. Target profiles were commissioned at levels 1 and 2, to deal with problem individuals, while daily Tasking and Coordinating meetings focused patrol and specialist staff at a local level on priority areas.

Meanwhile the preventive effort concentrated on Operation Tower, an assertive program targeting persistent offenders. Such offenders are approached and offered support in terms of drug treatment, accommodation, and employment. However, should they slip back into the drug abuse that generates their offending, they are targeted for enforcement. The project, at this writing, involves 271 persistent offenders of which 175 are currently in treatment. A results analysis conducted by academics has shown it having a significant impact on reducing crime.

---

[12] Problem profiles are assessments that focus on specific crime trends or incident hotspots. A problem profile generally includes a detailed analysis of the problem or threat, and recommendations for intelligence, prevention, enforcement, or partnership activity.

[13] Much like problem profiles, target profiles are made to gain a greater understanding of specific threats. In this case the threat is a specific person(s) or criminal network.

[14] Tactical assessments involve the collection of diverse data in order to monitor and identify crime trends. The product is forward-looking, but provides an analysis of current operational threats, assessed against the anticipated priorities set out in the strategic assessment and control strategy.

[15] Strategic assessments take into account the agency's needs related to enforcement and prevention activity, and assist in defining a control strategy. The assessment uses crime data, as well as public perception and satisfaction surveys, and health, welfare, and education data to determine both agency and community priorities along with intelligence, prevention, and enforcement needs.

The Constabulary is committed to a problem-oriented approach in order to deliver sustainable solutions to crime and disorder issues. The NIM provides a clear process to highlight priorities, understand problems, set cohesive strategies, and monitor both implementation as well as the results delivered. It also provides the framework to involve partner agencies in understanding and responding to these issues.

A number of executive session participants made strong arguments that many law enforcement agencies have been practicing intelligence-led policing in their jurisdictions for some time. The growth of technology in the 1980s and 1990s moved many departments from pin maps and paper files to GIS and crime analysis. In addition, some participants stated that just because a local law enforcement agency does not refer to an intelligence function does not mean that it is not engaged in collection and analysis efforts.[16] Indeed, local law enforcement uses intelligence in order to cultivate leads, build investigations, and implement strategies for dealing with specific problems. Although, efforts to extend their analysis beyond their border or regions has been more of a challenge.

The well-known COMPSTAT program, begun by the NYPD, has used statistical analysis in the development of effective tactical decisions and resource allocations. The COMPSTAT program has also relied on follow-up and accountability assessments to steer policy decisions. COMPSTAT is only one example of a tool that facilitates intelligence-led policing. Another approach is a program for High Intensity Drug Trafficking Areas (HIDTAs).[17] The Office of National Drug Control Policy guidelines that mandate regional drug threat assessments, and stipulate that strategies for combating those threats be implemented based on the assessment, follow a similar targeting strategy for addressing crime threats and security problems. In addition to these and other mechanisms for advancing intelligence-led policing, there are other successful approaches to addressing crime, citizen fear, and the terrorist threat—most notably, community policing.

Community Policing and Intelligence-Led Policing

The community policing philosophy promotes and supports organizational strategies to address the causes and reduce the fear of crime and social disorder through problem-solving tactics and police-community partnerships. The community policing model balances reactive responses to calls for service with proactive problem-solving centered on the causes of crime and disorder. Developing police-community partnerships, improving communications with the public, reducing fears, and taking a scientific approach to problem solving are actions that directly support intelligence-led policing. Proactive, problem-oriented policing also requires an analytic capacity necessary for both information collection and intelligence

[16] Maureen Baginski reminded participants of this truth in her address to the executive session.
[17] More information on the HIDTA program can be found on page 38 of this document and at http://www.whitehousedrugpolicy.gov/hidta/index.html and at www.nhac.org.

analysis. The ultimate objective of problem-oriented policing is the development of a more detailed understanding of and effective response to specifically identified problems.

Specifically, problem-oriented policing is based on the SARA model—scanning for, analyzing, responding to, and assessing problems.[18] Officers are encouraged to scan for and then prioritize problems based on community and other stakeholder information and data on a set of incidents. Officers then attempt to define the source of a problem. The problem, rather than the incident, becomes the primary focus of police work. Systematic collection and analysis of information about the specific problem or threat follow. These first two steps in the SARA model exemplify the proactive approach of intelligence-led policing. The third and fourth steps in the SARA model—response and assessment—are also an integral part of intelligence-led policing, especially with regard to the use of tactical intelligence. Officers tailor their approach to the situation based on analysis and circumstance. They then evaluate their efforts to determine whether they have been effective, efficient, or to map further analysis or action.

The Community Policing Consortium has created a technical assistance program designed to support law enforcement executives with organizational change.[19] Specifically, the program is intended to help police leaders think strategically about innovative approaches to criminal intelligence within the framework of community policing. (See Appendix B for a summary table from the facilitator's blueprint entitled, *A Guide to Incorporating the Intelligence Function into Community Policing*.) Executive session participants familiar with the initiative recognized it as an important means to reconcile or integrate intelligence work and community policing. The program also stresses the importance of safeguards to protect constitutional rights and the role of front-line police officers as well as managers in applying community policing principles to their critical responsibilities.

> ***"Community policing officers are close to and know their communities, and not through clandestine operations, but through trust and relationships that have been cultivated over time."***
>
> ***—Peter Modaferri, Chief of Detectives, Rockland County, NY, District Attorney's Office***

The core of the program is a symposium for chief executives of law enforcement agencies where they have an opportunity to engage in the free exchange of ideas about community policing principles and criminal intelligence in an interactive format that targets specific, relevant issues and moves the profession forward.

---

[18] For more information on the SARA model, see http://www.lancashire.police.uk/problemsolving.html or *Problem-Solving Tips: A Guide to Reducing Crime and Disorder Through Problem-Solving Partnerships* available through the U.S. Department of Justice Office of Community Oriented Policing Services.

[19] The program was designed by PERF Deputy Director Drew Diamond in coordination with the Community Policing Consortium. The Consortium is funded by the COPS Office and composed of the following five policing organizations: Police Executive Research Forum, International Association of Chiefs of Police, National Organization of Black Law Enforcement Executives, National Sheriffs' Association, and Police Foundation. For more information on the Consortium, this program, and the training blueprint see www.communitypolicing.org, or contact the Consortium office at (800) 833-3085.

Throughout the two-day executive session, the one theme that underscored most of the discussions was the uncertainty over how to sustain a community policing philosophy in this new paradigm. For well over a decade, community oriented policing has helped to guide and change the role of American law enforcement within the communities they serve. Local law enforcement participants at the executive session expressed their commitment to community-oriented policing and to problem solving. The relationship between local law enforcement agencies and the communities they serve is a valuable tool in fighting crime and addressing the terrorist threat. The information flow between the cop on the street and the members of the community is a vital resource for identifying neighborhood problems, reporting suspicious activity, and providing a context for intelligence analysis. The level of trust that exists between local police and residents will influence the value of the information police receive about all potential threats to community safety, and illustrates the important contribution of community policing to the intelligence process.

Starting at the Street Level

The adage that the analyst is only as good as the data he or she receives was frequently repeated during the session. Community policing can be an important mechanism for strengthening communications and investigations that yield quality data. Executive session participants maintained that if intelligence-led policing was going to take hold, it would need to build on the successes of community oriented policing and start with the conversion of the individual officers at the street level. While executive session discussion topics covered everything from improving intelligence resources to technology, the need to begin by training the line officer in awareness and collection was continually emphasized.

With the real-life demands on police resources, it is largely up to line officers to do the information collecting. If line officers were provided better training in collection—as well as the basic principles of analysis—an agency could enhance quality collection. After all, intelligence work begins at the street level.

THE NEED FOR TRAINED AND ACCREDITED ANALYSTS OF CRIMINAL INTELLIGENCE

by Ritchie A. Martinez, Certified Criminal Analyst; Arizona Department of Public Safety Criminal Intelligence Analyst Supervisor; Former President, International Association of Law Enforcement Intelligence Analysts[20]

The role of the law enforcement criminal intelligence analyst evolved during the 1970s. At first only a few agencies had full-time intelligence analysts, and most of them were used to support organized crime (OC) investigations. Agencies with OC or general criminal intelligence units predominately used sworn police officers to perform analytical duties. Police civilian personnel (that is, nonsworn/commissioned personnel) were rarely hired for those trusted positions or given opportunities to attend the very limited training available. Since then the challenge of multijurisdictional and global crimes has produced changes in the thinking of police executives. Today they recognize the value of managing and analyzing information, and intelligence analysts are used at all levels in criminal justice agencies.

Properly used and trained intelligence analysts are a valuable expert resource for agency executives. This is especially important today when information must be routinely and urgently analyzed to prevent local crime and maintain our nation's security. Well-trained intelligence analysts contribute by

- Reducing the civil rights and privacy pitfalls that intelligence units can encounter as a result of collecting, storing, and sharing criminal information/intelligence;
- Implementing knowledge-based networks and computerized systems;
- Applying analytic methods for complex operational, tactical, and strategic criminal investigations; and
- Managing, assessing, and analyzing information through special computerized analytic tools and the application of critical thinking skills.

The increased utilization of intelligence analysts has generated the need for training and accreditation. Whether performed by sworn or civilian personnel, criminal intelligence analysis is now widely accepted as a specialized function requiring professional skills. Our national counterdrug efforts and the current counterterrorism crisis have heightened this awareness. Like many responses to a crisis, the rapid acquisition of analysts has created gaps in the development of analytic training standards (the National Criminal Intelligence Sharing Plan did approve intelligence

[20] Ritchie A. Martinez was serving as President of the International Association of Law Enforcement Intelligence Analysts (IALEIA) at the time of the executive session.

training standards in June 2004) and proper roles for the analyst. Police executives must plan how to meet the needs of working analysts, and intelligence analysts must examine their competencies to ensure they meet the expectations of their professional body. The training and eventual certification of intelligence analysts must be a mutually shared goal for agency executives and analysts.

No standardized intelligence training for basic academy police recruits exists at the state and local level yet. Federal agencies (the Federal Bureau of Investigation and the Drug Enforcement Administration) have limited programs. Most providers of training represent the commercial, governmental, and professional associations. While all training providers deliver excellent products, the providers do not coordinate their efforts, and they do not provide a logical progression to learning core analytical competencies. Consequently, the current training creates gaps in knowledge for some existing analysts and prevents some new career analysts from learning the fundamentals of criminal intelligence analysis. The training shortcomings are as short-sighted as having academies omit how to write reports on criminal charges from police officers' training information. Core principles are essential for developing a sound foundation for analytical thinking. Like police officers, analysts need to achieve competency through the practice of efforts that meet common standards. The law enforcement intelligence community has begun to develop those standards. Two programs—former President Clinton's Executive Mandate 2000, General Counterdrug Intelligence Plan (GCIP), and the U.S. Department of Justice Global Justice Information Sharing Initiative: National Criminal Intelligence Sharing Plan (NCISP)—have identified intelligence analyst issues that must be addressed and have made specific recommendations.

The NCSIP tasked the International Association of Law Enforcement Intelligence Analysts (IALEIA) with developing analytic standards. These standards are pending approval. In addition to IALEIA, which has been advancing the science and art of intelligence since 1981, the Law Enforcement Intelligence Unit (LEIU) and the Society of Certified Criminal Analysts (SCCA) have developed standards for intelligence unit personnel. All of these groups are responding to national initiatives and working to develop and implement programs. SCCA has been certifying professional law enforcement, military, and corporate/industry security analysts since 1990.

The training of intelligence analysts has made progress. Training is better today, and it is positioned to improve. The challenge will be to orchestrate the efforts of these and other groups, and work closely with professional organizations that have been vested in the law enforcement criminal intelligence field for years.

Core Minimum Criminal Intelligence Training Standards

Part of the key to developing standards for intelligence-led policing is ensuring that all levels of law enforcement are provided with the appropriate training on what criminal intelligence is and how it should be collected, analyzed, and shared. The National Criminal Intelligence Sharing Plan (NCISP) recommended the development of minimum training standards for all affected levels of law enforcement personnel. The Global Intelligence Working Group (GIWG) has collaborated with a subgroup of DOJ's Counter-Terrorism Training Working Group (CTTWG) to develop minimum training standards for the six training classifications outlined in the NCISP. Currently a national Criminal Intelligence Training Coordination Strategy (CITCS) is being implemented by the GIWG that will develop minimum training standards for the following five training classifications (Intellicenge Analyst and Inelligence Collectors are treated as one classifcation by GIWG despite being separate in NCISP):

- Intelligence Analyst
- Intelligence Manager
- Law Enforcement Executive
- General Law Enforcement Officer (Basic Recruit and In-Service)
- Train-the-Trainer

The CITCS recommendations include minimum standards for training, time allotments for each element, as well as suggested curricula, training delivery methods, and materials. The purpose of these standards is to provide a blueprint for training facilities, law enforcement agencies, and personnel. These are not mandated standards, but rather a guide for agencies and organizations to develop and/or enhance their intelligence function through consistent, quality training.

The GIWG and the Criminal Intelligence Coordinating Council (CICC), a Council established by the U.S. Attorney General to implement the NCISP, has also been working with the International Association of Law Enforcement Intelligence Analysts (IALEIA) to develop Law Enforcement Analytical Standards. Input for the standards was obtained through a number of meetings, IALEIA's web site, and the GIWG and CICC membership, as well as many other agencies and individuals. IALEIA and Global are cosponsoring the production of booklets on Law Enforcement Analytical Standards for future distribution and use by the law enforcement and intelligence communities.

CHAPTER FOUR

DEVELOPING A SUCCESSFUL INTELLIGENCE FUNCTION

Executive session participants emphasized that before information and intelligence sharing systems can be established, important decisions—and changes—must be made by each agency regarding personnel, technology, organizational structures, and strategies, policies, and procedures for handling the collection, storage, and sharing of quality data. Change management is an important concept. Properly managed change involves an organization-wide commitment to reform, a clear communication of that vision, and the identification of concrete steps to effect positive change.

Meeting the Commitment

Participants at the session noted that in order to advance intelligence-led policing, ensure solid intelligence production, and facilitate the exchange of valuable, focused, and actionable intelligence, law enforcement agencies will need to change the manner in which they regularly function. This transition goes beyond deciding to openly share routinely collected information with other law enforcement agencies, and includes sharing the burden of information analysis, and in turn the manufacture of effective intelligence. This responsibility requires devoting personnel and resources to both collection and analysis.

Working together, state and local law enforcement agencies need to develop, where possible, cadres of intelligence and analytic experts who are professionally trained and educated. The few national-level analytic training programs—public and private—should be complemented by specialized in-service programs offered by state and regional law enforcement academies. In this way, the need for multitudes of trained analysts will be met more readily. State and regional academies are closer than national groups or third party contractors to the range of specific threats faced by local communities, yet they still can be grounded in a national framework.

Participants noted that even agencies that employ analysts or that operate an intelligence unit, may not always benefit from their existence. Too often intelligence units are plagued by passivity. Too many intelligence units simply respond to information requests and do not have a prescribed responsibility to perform some type of analysis.

Achieving a Shared View of the Threat

In her opening address to session participants, Maureen Baginski stressed how crucial it is for the law enforcement community—from federal to local agencies—to develop a "shared view of the threat." Before attempting to determine where, when, or how the next threat will present itself, law enforcement agencies need to understand the nature of the possible threats and the requisite features of the collection process that are likely to ensure that the right information is collected. Executive Assistant Director Baginski believes federal authorities should meet periodically with police to exchange views on perceived threats and collectively work on identifying priorities. The lack of a common understanding of the threats facing the United States is at odds with the urgent need to get decision-makers the information they require. The threats facing U.S. communities today are not limited, of course, to international terrorism but include criminal networks as well as local, "home grown" hate groups. If officers gained a shared understanding of the various threats and related concerns then they may be able to produce new insights of value in this newly expanded area of responsibility—intelligence production. These principles are consistent with the goals of targeted, problem-oriented policing encouraged by the community policing model.

Identifying intelligence collection requirements is critical to effective threat mitigation. These requirements help police collect what they need and avoid unnecessary commitments of time and resources to collecting information that may never prove to be useful. An up-front, and sustained effort to collect more targeted information can help avoid problems endemic to other intelligence efforts where the separation of useful information from useless information occurs late in the process—leading to inefficiency or even legal difficulties. In fact, one of the goals of the Office of Intelligence at the FBI is the development of a framework for ordering intelligence priorities.

> ***"Intelligence analysts are only as good as the information they receive from the collector. We must build the intelligence function from the ground up, beginning with the rank-and-file officer."***
>
> ***—Maureen Baginski, Executive Assistant Director, Office of Intelligence, Federal Bureau of Investigation***

Identifying knowledge gaps in federal and local law enforcement agencies in particular, and establishing the intelligence needs of both would enable a more efficient exchange of data and/or intelligence. Threat-based collection would help avoid the problems that information and intelligence gathering created in the 1970s. During that time, some law enforcement agencies collected an overabundance of information on individuals without a clear goal of an end product in mind—and even without an explicit connection to criminal activity. So more than 30 years later, collecting, archiving, and sharing information can recreate that controversy unless law enforcement agencies can find a better way to identify the critical threat basis of the information to be collected and determine how long it should be kept

before it is purged. Whether or not an agency has the resources to establish its own intelligence function, it must issue guidelines for officers on collection techniques and targets. Each piece of information needs to be assessed for its validity and reliability in understanding threats, identifying suspects, and developing cases that can be prosecuted.

Helping Officers Identify, Collect, and Use Information

The advancement of intelligence-led policing begins with a full understanding of the legitimacy of the intelligence function. Executive session participants agreed that the underlying goal of intelligence-led policing is to increase the quantity and quality of usable information. Better information will certainly improve the intelligence being developed by local, state, tribal, and federal law enforcement agencies. But the ability to produce and share intelligence is dependent on the standards set forth for collection, analysis, and dissemination of the information or intelligence. Intelligence-led policing is going to be successful only if the information the police get is credible and interpreted correctly. Therefore, developing standard, integrated data systems, documenting the standardization, as well as implementing and evaluating these standards in more than 18,000 state, local, and tribal law enforcement agencies are essential tasks.

> ***"We need a generation of police officers who know how to identify, collect, and use information before we can ensure legitimately productive information sharing."***
>
> ***—Peter Modaferri, Chief of Detectives, Rockland County, NY, District Attorney's Office***

Fostering the Analytic Process

Executive session participants conceded that not all agencies are able to allocate the same resources to developing an independent intelligence function. In agencies without the capacity or staffing levels to support a corps of analysts, personnel in intelligence and specialized enforcement units need to develop skills in organizing and analyzing their own information—in effect becoming their own analysts. An impressive array of intelligence exploitation and data mining tools is available in software platforms and can be maintained on desktop and other portable computers. (Many agencies are acquiring these systems now with terrorism prevention grants from the Office of Domestic Preparedness and other grant programs.)[21] Fortunately, these products are becoming more affordable as agencies are becoming increasingly concerned with tightening budgets and overextended resources. Federal agencies, such as DHS, can provide valuable assistance to local and state enforcement agencies by offering evaluative assessments of these programs in order to support a more knowledgeable procurement process.

Federal agencies are providing assistance with regards to training as well. Technology is really secondary to the cultivated abilities of a fully

[21] For more information regarding grant opportunities, see the ODP website at http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0356.xml.

"Not everyone will be able to deploy the same resources, but there are some fundamental training techniques that an agency can strive towards implementing; domestic and international best practices they can learn from; and analytical standards they can identify that will enable the agency as a whole to be more prepared."

—Ritchie A. Martinez, Criminal Intelligence Analyst Supervisor, Arizona Department of Public Safety

trained and experienced analyst. The intelligence analytic training program now being piloted at the Federal Law Enforcement Training Center (FLETC) on behalf of state and local enforcement agencies is a positive beginning.[22] Executive session participants agreed that analysts and officers alike must be well versed in the analytic process that supports intelligence production. Still, understanding analysis is not a trivial matter. Analysis is a practice rooted in cognitive mental processes—not exclusively dictated by specific methods or techniques. Once apprised of a subject or threat, the analyst, or the officer in many cases, must know what to look for next and infer a reasoned conclusion.

This is a difficult practice to cultivate through training. Particular variables—unrelated to the actual focus of the analysis—affect the analytic process. This is important for managers developing an intelligence function, or improving the intelligence process within their department, to understand. By distilling a list of the variables that affect analytic reasoning, it may be possible to move the tradecraft of intelligence analysis closer to a science.[23]

Systemic Variables

Systemic variables are those that affect both the intelligence organization and the analytic environment. The managerial structure, management practice, working culture, taboos, and organizational demographics are all variables that affect organizational behavior, as well as individual work habits or practices. Systemic variables also incorporate outside influences, such as consumers' needs, time and political constraints, as well as security issues.

"We need to train law enforcement in analytic tradecraft."

—Maureen Baginski, Executive Assistant Director, Office of Intelligence, FBI

[22] For more information on funding and training programs see the FLETC website at www.fletc.gov, the training section of the IALEIA website at www.ialeia.org/training, or the Office of Justice Program Information Technology Initiatives website at http://it.ojp.gov/index.jsp.

[23] Rob Johnston has explored these variables for the CIA in his work, Developing a Taxonomy of Intelligence Analysis Variables.For a more detailed discussion of theories on refining intelligence analysis to a science, as well as more on the following variables, see a CIA document written by Johnston (2003) or http://cia.gov/csi/studies/vol47no3/article05.html.

Systematic Variables

Systematic variables are those that affect the process of analysis itself. They include specific requirements of users; how the information is acquired, stored, and reported; the reliability or validity of the data; and most importantly any organizationally prescribed methods for processing the information and making decisions based upon the analysis.

Idiosyncratic Variables

Variables that affect the individual and his or her analytic performance are considered to be idiosyncratic variables. They influence the mindset and personal approach of the analyst or officer. This mental paradigm reflects the cultural, linguistic, and socioeconomic background of the individual, including any biases, decision-making styles, or reactions to different stressors. These variables also encompass education, training, and the willingness and ability to apply experience or skill sets to the task at hand.

Communication Variables

Finally, the variables that affect interaction within and between groups are vital to understanding the intelligence function. Communication variables include formal and informal exchanges within and among organizations, and between individuals and networks that are a part of the intelligence cycle.

The analytic process, rather than an exact science, is a tradecraft. It mirrors the practice of medicine in that tools and techniques support a diagnosis, yet in the end it is the personal judgment of the practitioner that integrates the art and the science to produce an informed and effective course of action.

Some executive session participants discussed an ideal paradigm in which every agency would be able to fully staff its own intelligence unit. A manager could then deploy analysts to the field to assist in quality data collection. Other participants warned against this type of thinking.

> ***"Developing an intelligence function is about experimentation, prioritization, and responsiveness."***
>
> ***—John P. Sullivan, Sergeant, Los Angeles County Sheriff's Department***

In fact, a very vocal group of local law enforcement executives expressed concern about individual agencies—particularly small and medium-sized agencies—developing their own intelligence units, for fear they would create a greater abundance of counterproductive stovepipes of unexploited information. It was suggested by these same participants that networks, such as the Joint Terrorism Task Forces (JTTFs), the FBI Law Enforcement Online (LEO), and Regional Information Sharing Systems (RISSnet), simply be utilized more effectively rather than create new production and sharing mechanisms. Several participants called for more regional coordination, and proposed that larger agencies with the capacity and established infrastructure to assist smaller agencies or partners do so through joint intelligence partnerships.

Tools for Intelligence Sharing

As participants discussed, not every agency is capable of developing a full-fledged intelligence unit. These agencies need to find a way to share information and obtain intelligence through other channels. And those that are capable of employing intelligence analysts or officers still need to be able to interface with other groups in order to ascertain outside intelligence, as well as communicate their own intelligence products. Session participants made the recommendation that state and local agencies should use the LEO and RISSnet networks—discussed in more detail below—to their fullest potential. These forums facilitate the critical exchange of information while national standards for collecting, archiving, and sharing data are developed. Several executive session participants suggested that state and local representatives also contact their regional FBI Field Intelligence Groups (FIGs) as a means to develop relationships that would facilitate the effective exchange of critical information.

MOVING INTELLIGENCE SHARING FORWARD

by Maureen Baginski, Executive Assistant Director (EAD), Office of Intelligence, Federal Bureau of Investigation

The Threat

Today, our adversaries are nation states, militaries, and shadowy criminal and criminal-like organizations that would do us harm. These adversaries represent complex challenges; they are networked together by information technology systems that allow them to have a shared view of their objectives, a clear understanding of their roles in carrying out those objectives, and very tight decision loops in taking action. To defeat these adversaries and prevent the harm they would do, we must get inside and ahead of their decision loops. Intelligence information and information technology systems that allow maximum sharing of intelligence information are core weapons in our battle with this new adversary. It takes a network to defeat a networked adversary.

Intelligence is best defined as vital information about those who would do us harm. The only measure of the value of intelligence is whether or not it helps a decision maker make a better decision. The decision makers are those charged with protecting our nation, and there are many, ranging from the President to the patrolman. For that reason, intelligence producers must not base their intelligence products on what they know or what they think is interesting, but rather on what their decision makers must know to make better decisions. The goal of intelligence cannot be to get the decision makers' attention; it must be to inform their decisions. This means first and fore-

most that intelligence producers must invest more time and energy in understanding the needs of intelligence users. Only then will we create a network capable of defeating our adversaries.

The Intelligence Cycle

The Intelligence Cycle (below) is key to creating that network:

In a threat driven environment, **Intelligence Requirements** drive investigations. Requirements are identified information needs - what we must know to safeguard the nation. Intelligence requirements are established by the Director of Central Intelligence according to guidance received from the President and the National and Homeland Security Advisors. Requirements are developed based on critical information required to protect the United States from national security and criminal threats. The Attorney General and the Director of the FBI participate in the formulation of national intelligence requirements.

Planning and Direction is the second step of the intelligence cycle. It is the management of the entire effort, to respond to intelligence needs up to and including delivering an intelligence product to the decision maker. It also drives new requirements based on feedback from decision-makers. As the EAD for Intelligence, I lead the intelligence planning and direction function for the FBI.

Collection is the gathering of raw information based on requirements. Activities such as interviews, technical and physical surveillances, human source operation, searches, and liaison relationships result in the collection of intelligence. The FBI has a very robust collection capability because of our investigative mission. We must now share the vast amount of intelligence that we collect on a daily basis with our partners who need it to make decisions.

Another part of the intelligence cycle is **Processing and Exploitation**. This involves converting the vast amount of information collected to a form usable for analysis. This is done in a variety of methods including decryption, language translations, and data reduction. Processing includes the entering of raw data into databases where it can be exploited for use in the analysis process.

Analysis and Production is the conversion of raw information into intelligence. It includes integrating, evaluating, and analyzing available data and preparing intelligence products. This is a vital piece of the cycle as it is the "value added" portion of the process. Talented and knowledgeable FBI personnel integrate, evaluate, and put into context raw information and draw conclusions about

its implications. This is a vital part of transforming "information" into "intelligence" which then can be used to make decisions.

Dissemination, the last step, which directly responds to the first, is the distribution of raw or finished intelligence to the decision makers whose needs initiated the intelligence requirements. The FBI disseminates information in three standard formats: Intelligence Information Reports, FBI Intelligence Bulletins, and FBI Intelligence Assessments.

As you can see, the Intelligence Cycle is just that, a continuing cycle, which overlaps and drives each of its functions and in turn, drives the investigative mission. This cycle or process is used across all programs—Counterterrorism, Counterintelligence, Cyber, and Criminal—to counter all threats.

Field Intelligence Groups

The FBI's intelligence capabilities are dispersed across the country and overseas. It is in the field that the majority of our intelligence information is collected and produced. For that reason, a vital part of the FBI's enhanced intelligence capability is the creation of the Field Intelligence Groups or FIGs. The FIGs are comprised of agents and analysts who are charged with directing intelligence production operations in the field and ensuring that the sum total of FBI investigative product is reviewed for intelligence value and shared according to processes established by the Office of Intelligence.

The FIGs provide an independent intelligence requirements and collection function; supervise and oversee effective standards for the intelligence analyst and agent workforce; and provide planning and direction to all other parts of the intelligence cycle. The FIGs contribute to the FBI's overall intelligence cycle, which is focused on answering the questions and getting the answers to the right people. The FIGs serve as the Bureau's primary interface for receiving and disseminating information, including threat and violent act warning information, with the Intelligence Community; federal, state, local, and tribal law enforcement; and other government agencies. The FIGs oversee the transformation of the collected information into intelligence that we can share with ourselves and our partners, in a timely and consistent manner.

The Intelligence Cadre

The heart and soul of any intelligence program is its people. It is important to note that the intelligence cadre is not limited to intelligence analysts, but also includes agents, language analysts, surveillance specialists, and others. It takes all of these specialists to perform quality intelligence production at the FBI.

To that end, we now have standardized the Intelligence Analyst position descriptions, created one skill community for Intelligence Analysts (whether in the field or FBI headquarters), and standardized the Intelligence Analyst promotion procedures and criteria. There are three distinct

work roles for Intelligence Analysts at the FBI—operations specialists, reports officers, and all-source analysts. All FBI Intelligence Analysts will be certified in each work role to ensure maximum flexibility in deploying our analytic workforce. The Training Division and the Office of Intelligence are currently developing courses for agents, analysts, and law enforcement officers, to better prepare and educate our personnel regarding the integration of intelligence and law enforcement operations, and information sharing initiatives. We are in the process of hiring Intelligence Analysts, developing a certification process for our intelligence professionals, and standardizing our dissemination of intelligence to our partners.

The Intelligence Program and Information Sharing

At the FBI we will share information as the rule and withhold only by exception, both within the FBI and with our outside partners. The first question we ask ourselves is "who else needs to have this information?" We have worked with the GLOBAL Intelligence Working Group on the National Criminal Intelligence Sharing Plan and are committed to its model for intelligence and information sharing. The FBI is also committed to providing those information technology systems that assist law enforcement—from the National Crime Information Center, the Integrated Automated Fingerprint Identification System, and the Interstate Identification Index, to Law Enforcement Online.

Because defending the nation is a team effort, we will always "write to share." We recognize and take seriously our responsibility to the nation, the Intelligence Community, and our federal, state, local, and tribal law enforcement partners to disseminate information, and we do it as an inherent part of our mission. The time when any one of us can act on our own to defeat our adversaries is gone. We must rely on each other for what each brings to the table, whether it is manpower, technology, or expertise. We must work together in seamless coordination and create the networks that together will defeat our adversaries.

Regional Information Sharing System (RISS)

The Regional Information Sharing System (RISS), which was created by Congress in 1974, links law enforcement agencies throughout the nation by providing secure communications, information sharing resources, and investigative support to combat multijurisdictional crime and terrorist threats. RISS is a national program supported by six centers that operate in specific geographic regions, serving the unique needs of law enforcement in each of those regions while fostering information sharing among all levels of law enforcement across the country.

The Regional Information Sharing System secure intranet, or RISSnet, is the intranet-based means for participating law enforcement agencies to share criminal intelligence information. Funded by the U.S. Department of Justice,

and membership dues, RISSnet provides detailed information on an offender's criminal activity (addresses, phone numbers, weapons used, and other information useful to law enforcement). RISSnet began with only the six regional projects—each with a separate data system that could be accessed by all members. Revised in the mid-1990s, RISSnet is now a secure, firewall-protected wide-area network (WAN). This new system enables better access to the information across all participating agencies. RISS now serves more than 7,000 local, state, federal, and tribal law enforcement member agencies in all 50 states, the District of Columbia, U.S. territories, Australia, Canada, and England.

Law Enforcement Online (LEO)

Introduced by the FBI in 1995, the Law Enforcement Online (LEO) system is a communications and information service for law enforcement agencies. At this writing, approximately 40,000 users have access to the LEO system through the Internet. Those who have an established account with the FBI can access the system from any Internet connection in the world. According to the FBI, LEO is intended to provide a state-of-the-art communication mechanism to link all levels of law enforcement throughout the United States. Both the LEO and RISS programs urge state and local agencies to post important information which could be useful in identifying multijurisdictional criminals and help to further these investigations. The systems also provide secure e-mail as a common tool for communications between agencies regardless of geographic location or level of government. And LEO is also used as a vehicle to educate officers on the best technologies and practices in all areas of law enforcement.

The FBI has also developed a 24-hour *Counterterrorism Watch Center*, to serve as the FBI's focal point for all incoming terrorist threats.

High Intensity Drug Trafficking Areas (HIDTA)

The High Intensity Drug Trafficking Area (HIDTA) program focuses resources and personnel in the areas of the country most vulnerable to drug trafficking, and helps federal, state, and local law enforcement agencies solve problems through teamwork and information sharing. Authorized by the Anti-Drug Abuse Act of 1988, the HIDTA program is administered by the Office of National Drug Control Policy. The HIDTA program began with five areas in 1990 and has since grown to 31 areas across the United States. The areas selected for the program are major centers of illegal drug production, manufacturing, importation, or distribution. These areas are also major distribution points for narcotics trafficking. They are particularly dangerous because of their potential to expand the illegal drug markets to other areas.

Intelligence Fusion Centers

Executive session participants discussed the recent surge of interest in regional and multiagency intelligence fusion centers. One example is the Joint Terrorism Task Force (JTTF). The JTTFs are designed to involve local agencies in the work being conducted by federal agencies like the FBI, through information sharing and collaboration in counterterrorism efforts. Participants recommended they be expanded to have a greater role and capacity for intelligence gathering and analysis beyond case-specific investigations. Other intelligence fusion centers are compacts of local and

state enforcement agencies specializing in such efforts as antiterrorism or narcotics enforcement.[24] Agencies that participate in intelligence fusion centers need evaluative tools to determine whether the centers are operating as efficiently as they might be, and whether certain fusion arrangements as federal-local collaborations are more cost-effective in certain situations than other arrangements, such as local-county networks. At the time of this writing, there is no widespread acceptance of a prescribed framework to determine how either a local intelligence or regional fusion center should be established, and correspondingly, there is no evaluative scheme to compare the structure and organizational components of different kinds of fusion centers to assess efficiency.[25] The possibility that even a minority of such centers may be operating at sub-optimal levels, in contrast to their potential, is reason enough to begin to develop guidelines for steering a definitive movement towards collaboration.

> ***"We should be wary about each agency creating its own intelligence unit. It could result in simply creating more silos of information that are unconnected to a meaningful network."***
>
> ***—Charles Ramsey, Chief of Police, Metropolitan (DC) Police Department***

Safeguards for Balancing Empowerments with Restraints

Any initiative to upgrade the local intelligence function must be advanced by the executive. Questions of beginning or expanding an intelligence collection effort, setting up or enhancing a dedicated unit, training and equipping personnel, and bounding the initiative with legal safeguards all require attention at the highest command level.

The Global Intelligence Working Group realized the need for police chiefs and sheriffs to assume an active leadership role. The Criminal Intelligence Training Coordination Strategy Working Group, coordinated by the U.S. Department of Justice Office of Justice Programs, raised the issue as a priority in its [draft] document, "*Core Criminal Intelligence Training Standards.*" Specifically, the group recommends a four-hour block of training to raise the awareness of law enforcement executives to new requirements and opportunities in intelligence administration. The purpose is to educate executives on the basic purpose and role of the intelligence process in law enforcement, and to appreciate their expanded range of responsibilities as leaders under the U.S. Department of Justice adoption of the National Criminal Intelligence Sharing Plan.

Vehicles for delivering the executive-level orientation await finalization, but recommendations include the U.S. Attorneys' Law Enforcement Coordination Committees (LECCs), state Peace Officers Standards and Training (POST) programs, and the

[24] The Terrorism Early Warning Group (TEW) in Fairfax County, Virginia is an example of such a fusion center. The TEW group is highlighted in the sidebar discussion that follows this section.
[25] Carter (2004) discusses creating and managing an intelligence function, as well as collaborating with federal and regional agencies to facilitate intelligence production and sharing.

FBI National Academy. Depending on the receptivity of police executives to the program and the prospect that a four-hour session may leave unanswered questions, session participants recommend establishing a police chiefs and sheriffs advisory group to explore ongoing educational requirements for agency executives. Among other challenges, the executive advisory group could address the continuing need to find resources to sustain the upgraded intelligence effort, approaches for enhancing automated analysis of information, assessment of compliance with 28 CFR Part 23 and other legal controls on information dissemination and use, and other questions that will surely arise as intelligence becomes a more active and central process within law enforcement. The 28 CFR Part 23 provisions regulate the collections and storage of intelligence information on various individuals when agencies are using federal funds to operate intelligence systems. Whether units are utilizing open sources or confidential sources, a criminal predicate must exist if an agency is going to collect information on an individual or group of individuals.

Executive session participants stressed that law enforcement managers should implement specific guidelines to ensure a successful intelligence function. Concerns about data integrity and civil liberties must be addressed. Executive session observer David Carter (2002) has suggested that agencies adopt the following:

- A fair use policy to articulate the types of crimes to be included in the system, who has access to the system, and who "owns" the data in the system
- A quality assurance policy to document the validity, reliability, and materiality of the data, as well as who has the authority to enter data and alter the information
- A recision of any "Third Party Rules" to forbid the recipient of intelligence products from disseminating it to a third party
- Accountability controls to govern all information security and provide audit trails for all information
- An inspectorate to monitor processes and controls and to handle allegations or concerns about security breeches and inappropriate dissemination
- A compliance mechanism to ensure that all federal and state laws are abided by with respect to the submission and distribution of information and to manage Freedom of Information Act or Open Records inquiries.

Many of these guidelines are also covered in the U.S. Department of Justice guidelines on interjurisdictional information-sharing systems and can be found in 28 CFR 23 et seq.[26] IALEIA's Law Enforcement Intelligence Unit (LEIU) has developed information-sharing guidelines that can provide assistance in establishing an intelligence capacity, and the Criminal Intelligence Coordinating Council, a steering council working in association with the Global group, is also developing standards for regional intelligence centers—including guidance on the development of memoranda of understanding between crossjurisdictional entities.[27]

[26] Presently they apply to systems funded by the U.S. Department of Justice and to networks funded under the Crime Control Act. HIDTA has voluntarily adopted them as a positive standard, but various systems funded by the Department of Homeland Security and by the Office of Domestic Preparedness mandated to conform to the 28 CFR provisions covering accountability and requiring that information systems be tied to explicit criminal activity.

[27] For more guidance on developing and implementing standards for an information-sharing capacity, see the Law Enforcement Intelligence Unit website at www.leiu-homepage.org/main.cgi.

THE TERRORISM EARLY WARNING (TEW) GROUP: MULTILATERAL INTELLIGENCE FUSION AND INFORMATION SHARING

by Sergeant John P. Sullivan,
Los Angeles County Sheriff's Department

The Terrorism Early Warning (TEW) Group in Los Angeles was established in 1996 as an interagency information sharing and analysis function designed to serve the information needs of local, state, and federal agencies involved in all phases of homeland security operations.

The TEW Model

The TEW is a multilateral, multijurisdictional, and multidisciplinary effort. It integrates law enforcement, fire, health, and emergency management agencies to address the intelligence needs for combating terrorism and protecting critical infrastructure. The TEW goes beyond criminal intelligence fusion and analysis. It results in "all source/all phase" fusion. In other words, it integrates all the information necessary for achieving a situational understanding at all phases of operations (before, during, and after an incident).

The TEW in Los Angeles includes a multidisciplinary fusion center staffed by "core agencies" including the Los Angeles County Sheriff's Department, Los Angeles Police Department, Los Angeles Division of the FBI, Los Angeles Fire Department, Los Angeles County Fire Department, and Los Angeles County Health Department. The TEW also receives support from state agencies and independent police, fire, and health agencies in Los Angeles County. The core agencies contribute permanent and surge staff, forward all potential terrorist criminal leads and pre-incident indicators to the TEW for assessment, and participate in joint training and exercises to facilitate TEW operations. In addition, each agency (and stations or units at larger agencies) have established Terrorism Liaison Officers (TLOs) to enhance two-way information exchange between the TEW and cooperating agencies. The TEW works in cooperation with Joint Terrorism Task Forces and other investigative agencies to improve prevention and response and to ensure an appropriate exchange of information between investigative and response entities.

TEW Organization

As depicted in Figure 1, the TEW is organized into six mutually supportive cells. The responsibilities of each cell are described below:

- The Unified Command cell provides direction, sets intelligence requirements, and interacts with the incident command entities.
- The Analysis/Synthesis cell coordinates net assessment activities and develops the collection plan. (It requests information be sought by the various net assessment elements and develops

the results of all the cells' analysis into actionable intelligence products, including advisories, alerts, warnings, and mission folders to assist response.)

- The Consequence Management cell assesses the law enforcement, fire, and health consequences of the event.
- The Investigative Liaison cell coordinates with criminal investigative entities and the traditional intelligence community.
- The Epidemiological Intelligence (Epi-Intel) cell is responsible for real-time disease surveillance and coordination with the disease investigation.
- The Forensic Intelligence Support cell exploits a range of technical means to support the TEW fusion process. These include chemical, biological, radiological, and nuclear explosives (CBRNE) reconnaissance, the use of sensors and detectors, and geospatial tools (such as mapping, imagery, and GIS products).

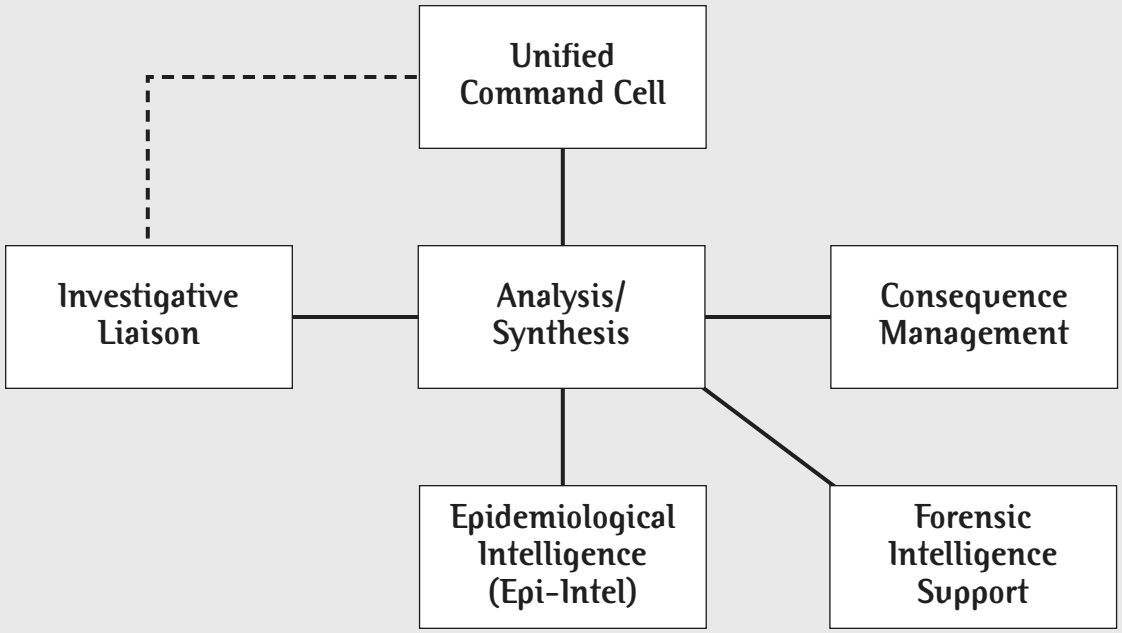


Fig. 1. TEW Net Assessment Organization

The Terrorism Early Warning (TEW) Group model is designed for both "first responder" agencies and "follow-on" response agencies, as a cooperative vehicle for obtaining and assessing the information and intelligence needed for an effective homeland security response. It establishes a high degree of interoperability among levels of responders (local, state, federal), disciplines (law enforcement, fire service, public health and medical), and civil and military agencies. This model demonstrates that intelligence is an important element in forging an interagency response.

CHAPTER FIVE

RECOMMENDATIONS

Since September 11, 2001, the challenge of reshaping the law enforcement intelligence function in the United States, and more specifically of advancing intelligence-led policing, has been much more daunting than it might appear. As noted by participants at the executive session on Intelligence and Information Sharing, this endeavor extends far beyond creating interoperable technologies for sharing data. In the fight against terrorism, as in the fight against crime in our communities, success depends on building a foundation of shared understandings, shared expectations, and shared goals. This challenge of intragovernmental intelligence cooperation is certainly formidable, but it is a challenge that must be met collectively because, as Americans and as law enforcement practitioners, we face together the consequences of this threat. Therefore, we must find ways of developing a common perception of the threats to our communities and our country so that we can act in concert. Establishing these commonalities will then enable governmental and law enforcement agencies at every level to develop the mechanisms needed to meet the threats successfully.

The executive session provided a forum for federal, state, and local law enforcement practitioners and members of the intelligence community to discuss their concerns and hopes with regard to the future of intelligence and information sharing. The open and spirited dialogue proved informative. Participants discussed not only the need for a shift in policy toward intelligence-led policing but also threat-specific policing practices. Once established, the shift in philosophy should provide a framework for the swift implementation of collection, analysis, dissemination, and technology standards for the law enforcement and intelligence communities. The recommendations below reflect the themes and suggestions presented and discussed throughout the executive session. The list is not exhaustive, but hopefully provides a firm foundation for successful intelligence and information sharing. The recommendations are grouped by theme.

Defining the Terms

➔ Law enforcement managers must understand the term "intelligence." Its meaning is not limited to clandestine operations in the national security context. Intelligence helps organizations develop an accurate picture of their respective environments and make informed decisions.

➔ Analysts and officers alike must emphasize the distinction between "information" and "intelligence." Intelligence combines information, analysis, and interpretation to produce inferences about a specific problem or threat.

Moving Toward Intelligence-Led Policing

➔ Law enforcement executives must assess how they currently use intelligence, and whether they need to reengineer their structure, personnel, and resources to support an intelligence-led policing philosophy.

➔ The law enforcement profession should recognize the need for better analytic capabilities in the policing profession. To help guide the movement toward intelligence-led policing, leaders of state and local agencies in the United States should examine models from other countries as well as identify best practices nationwide.

➔ State and local law enforcement agencies should recognize the value of the concepts outlined in the National Criminal Intelligence Sharing Plan (NCISP) and begin to work at following the guidelines set forth by the Plan.[28]

➔ Following the recommendations in the NCISP, law enforcement agencies must work together to develop a common understanding of criminal intelligence and its usefulness in combating both traditional crime and terrorism-related offenses.

➔ In their efforts to improve intelligence and information sharing, state and local police executives should examine the FBI and other federal efforts to reorganize the nation's intelligence mechanisms and functions. Some suggested they should stress state and local participation in formulizing counterterrorism efforts and implement the relevant findings of the National Commission on Terrorist Attacks Upon the United States (9/11 Commission).[29]

➔ Issues related to standardizing data systems, documenting criteria, and implementing and evaluating the standards must be resolved. There are more than 18,000 state, local, and tribal law enforcement agencies in the United States, and in order to guarantee the success of intelligence-led policing initiatives, greater agreement on these issues must be reached.

➔ Federal entities are encouraged to continue their efforts to translate threats they are aware of into what it means for particular jurisdictions. At the same time, local law enforcement needs to enhance how it relays operative information up to the federal levels (i.e., evidence from identity theft cases, fraudulent documents, and more).

[28] For more information on NCISP and to obtain a digital copy, see http://it.ojp.gov/documents/ncisp/.
[29] For more information see www.fbi.gov/publications.htm and www.9-11commission.gov/.

Understanding Community Policing and Intelligence-Led Policing

➔ In the past 30 years law enforcement executives have increasingly embraced the philosophy of community policing. Today they must work to redefine the role of community policing within an intelligence-led policing environment. Federal agencies should consider developing both overview and prescriptive materials on intelligence-led policing.

Meeting the Need for Analysts

➔ To implement intelligence-led policing, state, local, and tribal law enforcement agencies need intelligence analytic experts who are professionally trained and educated. The few national-level analytic training programs—whether federal or private—should be complemented by specialized in-service programs at state and regional law enforcement academies.

➔ For agencies without the capacity or staffing levels to support a corps of analysts, their personnel in intelligence and specialized enforcement units need to access appropriate resources or develop skills to organize and analyze their own information. Intelligence exploitation and data mining tools are available in software platforms, and they can be maintained on desktop and other portable computers. New grants from the Department of Homeland Security are available to make many of these programs more affordable for state and local enforcement agencies.

➔ Just as the Office of Community Oriented Policing Services put more officers on the streets in the 1990s, we need resources that will enable the addition of qualified analysts to the ranks of federal, state, local, and tribal entities. This includes the development and training of a new generation of analysts, so that agencies are not vying for the services of a limited pool of career intelligence analysts.

Assessing Intelligence Fusion Centers

➔ There has been a recent surge of interest in intelligence fusion centers. These are regional, multi-agency centers that promote information sharing. Some centers involve federal-local partnerships and others are based on compacts between local and state enforcement agencies specializing in antiterrorism or narcotics enforcement. Evaluative tools are needed to determine whether participation in these centers is efficient and cost-effective in certain situations for law enforcement agencies. For example, agencies need to assess the efficacy of federal-local versus local-county fusion arrangements with respect to specific needs and capabilities.

➔ More efforts should be focused on regional intelligence planning, whether for collection, analysis, needs assessments, or grant applications.

➔ State and local agencies are encouraged to contact the local field office of the FBI and to develop working relationships with the Field Intelligence Groups within those offices.

➔ At the present time, there are no nationally accepted evaluative schemes for prescribing how either a local intelligence or regional fusion center should be established. Therefore, we have no corresponding ability to compare the structure and organization of different kinds of fusion centers. The possibility that even a few centers may be operating below their potential is reason

enough to begin to search for evaluative programs that can guide the future of a national movement in this direction.

Making the Most of Existing Resources

➔ Local law enforcement agencies, whether or not they participate in regional fusion centers or maintain an established intelligence function, are encouraged to seek out and fully utilize established mechanisms for sharing information such as LEO, RISS, as well as other regional task forces. FBI field offices and state homeland security offices continue to be important points of contact for local officials.

➔ Smaller agencies without the capacity to create or maintain an effective intelligence function are encouraged to partner with larger agencies in their region with an established intelligence mechanism or that possess the necessary resources to create a productive intelligence unit.

➔ More attention must be paid to identifying and disseminating best practices. These should include how best to include private sector and university security entities.

➔ There is a need to standardize the classification systems of the various intelligence agencies. Currently, what may be classified at one level may not be classified at another in a different government agency.

Balancing Empowerments with Restraints

➔ Law enforcement must be fully aware of federal constraints and safeguards—specifically, 28 CFR 23 et seq.— and understand when they should be applied.

➔ A curriculum stressing the new requirements and opportunities for law enforcement executives in the field of intelligence administration should be implemented through a variety of vehicles to ensure nationwide consistency in understanding.

➔ Law enforcement executives and public information officers (PIOs) should be provided background and talking points on the merits of local intelligence units, as well as information to help dispel or refute misconceptions on the part of the public and media, for use in interviews or public discussion forums. This background should include details of how the agency plans to protect the civil liberties and privacy of the community it serves.

The highlighted recommendations from this white paper cover a wide range of issues for law enforcement and other government agencies as they begin to formulate and advance their intelligence functions. The text offers more detailed suggestions that can be tailored to the unique needs of a department. In all, and the issues discussed within are meant as a starting point for further discussions on the future of producing and sharing intelligence.

APPENDIX A

PARTICIPANTS AND OBSERVERS

Participants[30]

Maureen Baginski
Executive Assistant Director
Office of Intelligence
Federal Bureau of Investigation
Washington, D.C.

Jack Barrett
Commander
Superintendent of Detectives
Metropolitan Police Department
Washington, D.C.

Daniel Bibel
Program Manager
Crime Reporting Unit
Massachusetts State Police
Framingham, Massachusetts

Victor Brito
Captain
Special Investigations Division
Metropolitan Police Department
Washington, D.C.

Charles Brueggemann
Deputy Director
Illinois State Police
Springfield, Illinois

Melvin Carraway
Superintendent
Indiana State Police
Indianapolis, Indiana
Chairman
Global Advisory Committee
Global Justice Information Sharing Initiative
Office of Justice Programs
U.S. Department of Justice

Barbara Cart
Executive Assistant
Homeland Security Support Office
National Security Agency
Fort Meade, Maryland

David Cohen
Deputy Commissioner for Intelligence
New York City Police Department
New York, New York

James Comey
Deputy Attorney General
U.S. Department of Justice
Washington, D.C.

Hank Crumpton
Chief of Natural Resources Division
Central Intelligence Agency
Washington, D.C.

Deborah Daniels
Assistant Attorney General
U.S. Department of Justice
Office of Justice Programs
Washington, D.C.

Edward Flynn
Secretary of Public Safety
Massachusetts Executive Office for Public Safety
Boston, Massachusetts

[30] Participants ranks and agency affiliations are listed as of the time of the executive session.

Joshua Filler
Director
Office of State and Local Government Coordination
Department of Homeland Security
Washington, D.C.

Polly Hanson
Chief of Police
Metro Transit Police Department
Washington, D.C.

Willie Hulon
Special Agent in Charge
Detroit Field Office
Federal Bureau of Investigation
Detroit, Michigan

Ron Iden
Assistant Director in Charge
Los Angeles Field Office
Federal Bureau of Investigation
Los Angeles, California

Robert Jordan
Special Agent in Charge
Portland Field Office
Federal Bureau of Investigation
Portland, Oregon

Kathleen Keirnan
Assistant Director
Office of Strategic Intelligence and Information
Bureau of Alcohol, Tobacco, Firearms, and Explosives
Washington, D.C.

Ronald Louie
Chief of Police
Hillsboro Police Department
Hillsboro, Oregon

Thomas Manger
Chief of Police
Fairfax County Police Department
Fairfax, Virginia

Ritchie A. Martinez
Criminal Intelligence Analyst Supervisor
Arizona Department of Public Safety
Tucson, Arizona
President
International Association of Law Enforcement Intelligence Analysts

Michael Mason
Assistant Director in Charge
Washington Headquarters
Federal Bureau of Investigation
Washington, D.C.

Peter Modafferi
Chief of Detectives
Rockland County District Attorney's Office
New City, New York

Daniel Oates
Chief of Police
Ann Arbor Police Department
Ann Arbor, Michigan

Robert K. Olson
Former Chief of Police
Minneapolis Police Department
Minneapolis, Minnesota

Carl Peed
Director
Office of Community Oriented Policing Services
U.S. Department of Justice
Washington, D.C.

D. Strebel Pierce
Special Agent in Charge
Minneapolis Field Office
Federal Bureau of Investigation
Minneapolis, Minnesota

Charles Prouty
Executive Assistant Director
Washington Headquarters
Federal Bureau of Investigation
Washington, D.C.

Louis Quijas
Director
Office of Law Enforcement Coordination
Federal Bureau of Investigation
Washington, D.C.

Charles Ramsey
Chief of Police
Metropolitan Police Department
Washington, D.C.

Mike Rolince
Acting Assistant Director
Federal Bureau of Investigation
Washington, D.C.

M. Douglas Scott
Chief of Police
Arlington County Police Department
Arlington, Virginia

Mark Spurrier
Deputy Chief
Office of Enforcement
National Oceanic and Atmospheric Administration
Silver Spring, Maryland

Michael Stenger
Special Agent in Charge
U.S. Secret Service
Washington, D.C.

John P. Sullivan
Sergeant
Los Angeles County Sheriff's Department
Monterey Park, California

Karen Tandy
Administrator
U.S. Drug Enforcement Agency
Arlington, Virginia

Bill Young
Sheriff
Las Vegas Metropolitan Police Deptartment
Las Vegas, Nevada

Observers[31]

Jim Burch
Associate Deputy Director of Policy
Bureau of Justice Assistance
U.S. Department of Justice
Washington, D.C.

David L. Carter
Professor
School of Criminal Justice
Michigan State University
East Lansing, Michigan

Robert Casey, Jr.
Deputy Director
Office of Intelligence
Federal Bureau of Investigation
Washington, D.C.

G. David Curry
Professor
Criminology and Criminal Justice
University of Missouri - St. Louis
St. Louis, Missouri

Mike Duffy
Deputy Chief Information Officer
U.S. Department of Justice
Washington, D.C.

Steven M. Edwards
Senior Policy Advisor for Law Enforcement
Bureau of Justice Assistance
U.S. Department of Justice
Washington, D.C.

[31] Observers' ranks and agency affiliations are listed as of the time of the executive session.

Robert Fox
Lieutenant
Intelligence Investigations Section
Analysis Unit
Major Crimes Division
Los Angeles Police Department
Los Angeles, California

Steven H. Gurley
Special Agent in Charge
Los Angeles Field Office
Federal Bureau of Investigation
Los Angeles, California

Greg Harris
Principal Deputy Director
Office of Intergovernmental and Public Liaison
U.S. Department of Justice
Washington, D.C.

Dennis Kenney
Professor
John Jay College
City University of New York
Policy Lab
Washington, D.C.

David Klinger
Professor of Criminology and Criminal Justice
University of Missouri - St. Louis
St. Louis, Missouri

Steve Mastrofski
Director
Department of Justice
George Mason University
Manassas, Virginia

Pat McCreary
Senior Policy Advisor
Bureau of Justice Assistance
U.S. Department of Justice
Washington, D.C.

Lois Felson Mock
Senior Social Science Analyst
National Institute of Justice
U.S. Department of Justice
Washington, D.C.

Ronald Parthemore
Law Enforcement Liaison
Office of State and Local Government Coordination
Department of Homeland Security
Washington, D.C.

Steven Pomerantz
Executive Director
Center for Criminal Justice Technology
Mitretek Systems
Falls Church, Virginia

Sue Reingold
Infrastructure Protection & Information Analyst
Office of State and Local Government Coordination
Department of Homeland Security
Washington, D.C.

Diego Rodriguez
Special Agent/Unit Chief
Federal Bureau of Investigation
Washington, D.C.

Raul Roldan
Section Chief
Federal Bureau of Investigation
Quantico, Virginia

Ellen Scrivner
Law Enforcement Consultant
Washington, D.C.

Kathleen Timmons
Special Assistant to the Assistant Director
Federal Bureau of Investigation
Washington, D.C.

Office of Community Oriented Policing Services Staff
1100 Vermont Avenue, NW
Washington, DC 20530
Phone: 1-800-421-6770
Fax: 202-616-2914
Website: www.cops.usdoj.gov

Beverly Alford
Assistant Director

Pam Cammarata
Deputy Director

Robert Chapman
Senior Social Science Analyst

Mary Hyland
Deputy Chief of Staff

Frank Mathers
Grant Monitoring Specialist

Laurel Matthews
Special Assistant

Gilbert Moore
Public Affairs Specialist

Timothy Quinn
Chief of Staff

Amy Schapiro
Senior Social Science Analyst

Michael Seelman
Senior Social Science Analyst

Police Executive Research Forum Staff
1120 Connecticut Avenue, NW, Suite 930
Washington, DC 20036
Phone: 202-466-7820
Fax: 202-466-7826
Website: www.policeforum.org

Anna Berke
Conference Coordinator

Corina Solé Brito
Research Associate

Terry Chowanec
Senior Associate

Heather Davies
Research Associate

Don Faggiani
Senior Research Associate

Lorie Fridell
Director of Research

Alex Hayes
Research Assistant

Clifford Karchmer
Director of Program Development

Bruce Kubu
Research Associate

Steve Loyka
Legislative Research Assistant

Stacy Osnick Milligan
Research Associate

Rebecca Neuburger
Membership/Marketing Coordinator

Martha Plotkin
Communications Director

Chuck Wexler
Executive Director

APPENDIX B

A GUIDE TO INCORPORATING THE INTELLIGENCE FUNCTION INTO COMMUNITY POLICING

A Guide to Incorporating the Intelligence Function into Community Policing[32]				
Planning and Implementation	**Step 1**	**Step 2**	**Step 3**	**Step 4**
1-1. Assessment: Perform workforce and community analysis	Analyze current intelligence efforts	Conduct internal (agency) environmental scan of current use of community in intelligence function	Conduct external (community) environmental scan of current use of community in intelligence function	
1-2. Political Support: Develop internal agency support and community support	Determine the political (both internal and external) stakeholders	Develop support from internal and external stakeholders	Promote community involvement in intelligence function	
1-3. Community Outreach: Educate the public about the plan—solicit input and feedback	Educate community	Develop material	Organize focus groups	Develop strategies to include stakeholders in the outreach effort
1-4. Agency Directives: Look for needed changes or additions	Encourage stakeholders to recommend or implement any changes in policies	Review policies and procedures for consistency with community policing principles		
1-5. Resource Considerations: Evaluate resources needed	Identify potential costs of implementing changes as recommended by the community with regard to the intelligence function	Review current technology related to the intelligence function and determine future needs	Identify funding sources	Prioritize and allocate resources; develop a budget
1-6. Training Needs: Assess the need for new skills /additional training	Identify training priorities	Develop a training strategy that involves the community in the intelligence function	Deliver the training	
1-7. Employee-Labor Relations Build support in the workforce	Engage the union (stakeholders) at the onset of the process	Develop consensus among formal and informal leadership in organization	Develop communication strategies to promote "buy in"	Establish a credible program that ensures open and honest ("above-board") communication

[32] Taken from the Community Policing Consortium's Executive Training Curriculum. (Minor editorial changes were made to this table by the authors.)

APPENDIX C

INTELLIGENCE TRAINING AND COUNTERTERRORISM FUNDING RESOURCES[33]

Intelligence Training Resources

Bureau of Justice Assistance Law Enforcement Training Database
http://bjatraining.aspensys.com/

Counter-Terrorism Training and Resources for Law Enforcement
http://www.counterterrorismtraining.gov/tta/index.html

Federal Law Enforcement Training Center (FLETC)
http://www.fletc.gov/trng.htm

Institute for Intergovernmental Research (IIR)
http://www.iir.com/

28 CFR Part 23 Training
http://www.iir.com/28cfr/Training.htm

State and Local Anti-Terrorism Training (SLATT)
http://www.iir.com/slatt/

National White Collar Crime Center (NW3C)
http://www.nw3c.org/training_courses.html

Regional Information Sharing Systems (RISS) Services and Training
http://www.iir.com/RISS/RISS_services.htm

Funding Resources

The Catalog of Federal Domestic Assistance (CFDA)
U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405
http://www.cfda.gov

Counter-Terrorism Training and Resources for Law Enforcement
http://www.counterterrorismtraining.gov/fund/index.html

Federal Grant Opportunities
Phone: (301) 589-1017
http://www.fedgrants.gov/

FirstGov
U.S. General Services Administration
1800 F Street, NW, Washington, DC 20405
Phone: (800) FED-INFO
http://www.firstgov.gov/Government/State_Local/Grants.shtml

Grants.Gov
HHH Building, Room 739F
200 Independence Avenue, SW
Washington, DC 20201
Phone (800) 518-4726
http://www.grants.gov/

[33] This list of resources was compiled by the Criminal Intelligence Training Coordination Strategy (CITCS) Working Group, working in association with the Global Initiative and the Bureau of Justice Assistance.

U.S. Department of Homeland Security (DHS)
Washington, DC 20528
http://www.dhs.gov/dhspublic/display?theme=38&content=3419

U.S. Department of Homeland Security, Office of Domestic Preparedness (ODP)
810 Seventh Street, NW
Washington, DC 20531
Phone: (800) 368-6498
http://www.ojp.usdoj.gov/odp/grants_goals.htm

U.S. Department of Justice, Bureau of Justice Assistance (BJA)
810 Seventh Street NW, Fourth Floor
Washington, DC 20531
Phone: (202) 616-6500
http://www.ojp.usdoj.gov/BJA/

U.S. Department of Justice, National Institute of Justice (NIJ)
810 Seventh Street, NW
Washington, DC 20531
Phone: (202) 307-2942
http://www.ojp.usdoj.gov/nij/funding.htm

U.S. Department of Justice Office of Community Oriented Policing Services (COPS)
1100 Vermont Avenue, NW
Washington, DC 20530
Phone: (800) 421-6770 or (202) 307-1480
http://www.cops.usdoj.gov/

U.S. Department of Justice, Office of Justice Programs
810 Seventh Street, NW, Room 5400
Washington, DC 20531
Phone: (202) 307-0790
http://www.ojp.usdoj.gov/fundopps.htm

REFERENCES

Carter, David L. 2004. *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*. Washington, D.C.: U.S. Department of Justice Office of Community Oriented Policing Services.

———. *Law Enforcement Intelligence: A Primer*. East Lansing, MI: Michigan State University, School of Criminal Justice.

Carter, David L. and Richard Holden. 2002. "Homeland Security and Local Law Enforcement: Practical Applications of Intelligence and Community Policing." *Local Government Police Management* (4th ed.) Washington, D.C.: International City Management.

Criminal Intelligence Training Coordination Strategy Working Group (DRAFT). 2004. *Core Criminal Intelligence Training Standards for United States Law Enforcement and Other Criminal Justice Agencies: Findings and Recommendations*. Washington, D.C.: Bureau of Justice Assistance.

Eck, John. 2002. *Overcoming the Barriers: Crime Mapping in the 21st Century*. Washington, D.C.: Police Foundation.

Faggiani, Donald, Daniel Bibel, and Diana Brensilber. 2001. "Regional Problem Solving Using the National Incident Based Reporting System." In Reuland, Melissa, Corina Brito and Lisa Carroll, eds., *Solving Crime and Disorder Problems*. Washington, D.C.: Police Executive Research Forum.

Global Intelligence Working Group (GIWG). 2004. *National Criminal Intelligence Sharing Plan*. Washington, D.C. U.S. Department of Justice, Office of Justice Programs. Available online at http://it.ojp.gov/topic.jsp?topic_id=103.

Johnston, Rob. 2003. "Developing a Taxonomy of Intelligence Analysis Variables." *Journal of Intelligence*, Vol. 47, No. 3.

LaVigne, Nancy and Julie Wartell. 1998. *Crime Mapping Case Studies: Successes in the Field*. Washington, D.C.: Police Executive Research Forum.

———. 2000. *Crime Mapping Case Studies: Successes in the Field, Volume 2*. Washington, D.C.: Police Executive Research Forum.

———. 2001. *Mapping Across Boundaries: Regional Crime Analysis*. Washington, D.C.: Police Executive Research Forum.

Meyer, H.E. 1987. *Real World Intelligence*. New York: Grove Weidenfeld.

Steinert-Threlkeld, Tom. 2002. "CompStat: From Humble Beginnings." *Baseline Magazine: The Project Management Center*. 9 September. (www.baselinemag.com).

Office of Community Oriented Policing Services. 2002. *Problem-Solving Tips: A Guide to Reducing Crime and Disorder Through Problem-Solving Partnerships*. Washington, D.C.: U.S. Department of Justice.

Whitaker, Janet. n.d. "Understanding NIBRS Data Quality." *Justice Research and Statistics Association Resource Center*. Washington, D.C. (www.jrsa.org).

About the Authors

Stephan A. Loyka,
Research Assistant/Legislative Specialist,
Police Executive Research Forum

Steve Loyka joined the PERF legislative affairs staff in 2003 after spending a year with the U.S. Senate Small Business Committee. Loyka has since taken on collaborative roles in the research and management services departments at PERF, contributing to several projects including this white paper series. He has represented PERF at forums dealing with homeland security and information-sharing issues. Recently, he participated in a working group on the need to create a training curriculum on criminal intelligence sharing for law enforcement executives. Loyka holds a bachelor of arts degree in political science from the Johns Hopkins University, and he will receive his master's degree in government and homeland security studies also from the Johns Hopkins University in early 2005.

Donald Faggiani, Senior Research Associate,
Police Executive Research Forum

Donald Faggiani, before returning to PERF, served as the executive director of the Wyoming Statistical Analysis Center for Rural Policy Studies at the University of Wyoming. He was also the director of the Virginia Statistical Analysis Center. He holds a doctoral degree in public policy analysis from the University of Illinois at Chicago and has been an adjunct faculty member of the University of Wyoming Criminal Justice Department.

Faggiani has worked extensively with the FBI's National Incident-Based Reporting System (NIBRS) and is recognized as one of the leaders in research using incident-based police data systems. He is one of the few researchers in the country to incorporate NIBRS with GIS and mapping for research purposes. Faggiani has been appointed to the FBI's Policy Advisory Council overseeing the development of a National Data Exchange Program for aiding law enforcement in their fight against terrorism.

He is also the project director for PERF's project on Protecting America's Ports: Assessing Coordination between Law Enforcement and Industrial Security, funded by the National Institute of Justice.

Clifford Karchmer,
Director of Program Development,
Police Executive Research Forum

Clifford Karchmer is responsible for expanding program opportunities at PERF in the areas of criminal justice and homeland security. He also has day-to-day management responsibilities for PERF programs with the Office of Justice Programs and Office of Domestic Preparedness. Examples include the Bureau of Justice Assistance (BJA) Police-Medical Collaboration Project, the BJA Homicide Investigative and Model Witness Security projects, the Office of Juvenile Justice and Delinquency Prevention (OJJDP) National Underage Drinking Program technical assistance, and the National Institute of Justice study of model police executive strategies to facilitate large budgetary acquisitions. He directs an ODP initiative to develop executive-

oriented guides on preparedness topics ranging from bioterrorism to unified incident management

Karchmer has been involved in a variety of research, strategy development, technical assistance, and training projects concerned with domestic and international dimensions of narcotics trafficking activity, money laundering and white-collar crime, asset forfeiture, homicide, and witness intimidation, and counterterrorism. He was honored with a Public Service Innovators' award by the John F. Kennedy School of Government at Harvard University for his work in developing a collaborative initiative between law enforcement and emergency health care personnel.

About the Contributors

Maureen Baginski
Executive Assistant Director
Office of Intelligence,
Federal Bureau of Investigation

In April 2003, Maureen Baginski was appointed by FBI Director Robert Mueller to lead the FBI's new Office of Intelligence. She oversees the collection, analysis, and dissemination of intelligence throughout the Bureau and is responsible for integrating the intelligence function into all FBI investigative operations. Baginski is developing a strategic analytic capacity at the Bureau and expanding its ability to convert investigative information into strategic intelligence. Under her direction, the Bureau has begun prioritizing national collection requirements and evaluating the performance of FBI field offices nationwide in meeting these requirements.

Baginski also serves as the Bureau's primary contact with the intelligence community, state and local law enforcement agencies, and national and international government agencies for disseminating and receiving information. She is active in efforts to establish, administer, and evaluate standards for intelligence sharing.

Prior to joining the FBI, Baginski spent 25 years with the National Security Agency (NSA). As the head of the NSA Signals Intelligence Directorate, the nation's high-technology cryptology organization, she managed a complex and geographically dispersed enterprise engaged in distributed information production. She began her NSA career in 1979 as a Russian language instructor. At NSA she held a variety of positions, including lead analyst for the former Soviet Union; executive assistant to the director of NSA; chief of operations policy; assistant deputy director for technology and systems; and chief in the Office of the Director. Baginski holds a master of arts degree in slavic languages and a bachelor of arts degree in Russian and Spanish from the State University of New York (SUNY), Albany, NY.

Daniel Bibel, Program Director
Crime Reporting Unit,
Massachusetts State Police

Daniel Bibel has extensive experience in collecting and analyzing summary and incident crime data for the Commonwealth of Massachusetts. He has been in charge of the Crime Reporting Unit of the Massachusetts State Police since 1988. Before then, he directed the Commonwealth's Statistical Analysis Center. He received his M.S. degree from Northeastern University and has done postgraduate work at Rutgers University.

For the past 15 years, Bibel has been actively involved in the development and implementation of the National Incident-Based Reporting System (NIBRS). He has organized several panels on NIBRS for the American Society of Criminology and given numerous talks on crime mapping and analysis using incident-specific crime data.

Melvin Carraway, Superintendent
Indiana State Police Service

Indiana Governor Frank O'Bannon appointed Melvin Carraway Superintendent of the Indiana

State Police on January 13, 1997. Superintendent Carraway also serves as the current chairman of the Global Advisory Committee of the Global Justice Information Sharing Initiative, in association with the National Criminal Intelligence Sharing Plan and the U.S. Department of Justice Office of Justice Programs. The Global Advisory Committee (GAC) is composed of key personnel from local, state, tribal, federal, and international justice and public safety entities and includes agency executives and policy makers, automation planners and managers, information practitioners, and, most importantly, end users. This last group distinguishes the GAC as a committee whose members remain actively dedicated to information sharing, because they continue to be producers, consumers, and administrators of crucial justice-related data. Fellow committee members elect leaders of the Global Advisory Committee (GAC) every two years.

Prior to his appointment as superintendent, Carraway served as the executive director for the Indiana State Emergency Management Agency, Department of Fire and Building Services. Carraway coordinated disaster relief for flood and tornado victims, and facilitated state activities during the investigation of and recovery from major incidents, including plane crashes and industrial accidents. He was also instrumental in reconfiguring the State Emergency Operations Center, and reorganizing the Public Safety Institute that trains volunteer and professional firefighters and emergency medical personnel for efficiency and accountability.

Carraway became a state trooper in 1979 and was assigned to the Indianapolis District. In his 22 years with the Indiana State Police, his assignments have included Commander of Training, Aviation Commander, and Enforcement Division Commander. He participates and provides leadership to various national and local boards and commissions, including the International Association of Chiefs of Police and the National Organization of Black Law Enforcement Executives. Carraway earned a bachelor of music degree from Heidelberg College and is also a graduate of the FBI National Academy.

Stuart Kirby, PhD,
Detective Chief Superintendent
and Divisional Commander,
Lancashire Constabulary, United Kingdom

Stuart Kirby is a Detective Chief Superintendent with the Lancashire Constabulary and commands the HQ Specialist Operations and Crime Division, which is responsible for the departments of intelligence, major crimes unit, scientific support, homicide investigation, air support, mounted police, motorway policing, community safety, and operational planning. Kirby has 27 years service experience and has performed in numerous supervisory capacities including head of intelligence, head of uniform and detective training, and divisional commander.

Kirby is a registered psychologist, and has a Ph.D. in investigative psychology. His area of expertise is in crimes against children. Since 1993, he has assisted police forces nationally in ongoing investigations concerning the sexual exploitation of children, and has published numerous articles on the subject. Kirby is also an honorary senior fellow at Lancaster and Liverpool Universities. He has won two national awards on behalf of his organization in the area of problem-oriented policing, and recently published an article on the inte-

gration of the UK National Intelligence Model with a problem-oriented approach.

Ritchie A. Martinez,
Criminal Intelligence Analyst Supervisor
Arizona Department of Public Safety

Ritchie A. Martinez has worked in the field of law enforcement for 32 years developing and instructing classes in law enforcement intelligence and management of major case investigations. He began his career as a deputy sheriff in 1972 when he was assigned to Arizona's first multi-agency narcotics investigative task force around the United States–Mexico border areas. He created the unit's first intelligence system, supported narcotics enforcement officers' intelligence requirements, and analyzed specific case/investigative targets. In 1976, Martinez became a special agent/intelligence analyst assigned to the Arizona Narcotics Strike Force. He also assisted in developing a regional statewide intelligence program and building an analytical section to support a multi-state intelligence system (Narcotics Information Network of Arizona, NINA & Quad State). During this time, he also worked with his agency's staff to establish and create the program known as RISSnet (Regional Information Sharing System), and the Rocky Mountain Information Network's (RMIN) intelligence and analytical systems. In 1981, he was appointed Manager of Criminal Intelligence Analysis Section, for the Arizona Criminal Intelligence System Agency (ACISA), and in 1984 he was transferred to the Arizona Department of Public Safety (DPS), Criminal Investigation Bureau's intelligence division. Upon retiring in 1994, he returned to DPS and began his civilian criminal intelligence analytical career. He was appointed to supervise criminal intelligence analysts assigned to the High Intensity Drug Trafficking Area (HIDTA), and Post Seizure Analysis Team (PSAT). Currently he coordinates four multi-agency intelligence analysts' teams in the Arizona HIDTA Center, Investigative Support Center.

Martinez is the former president of the International Association of Law Enforcement Intelligence Analysts (IALEIA 2000-2004), and a former member of the Board of Governors for the Society of Certified Crime Analysts (SCCA) for 10 years. He holds college degrees in both criminal justice and business administration. He has received numerous awards and citations for his work. Among those awards, was the Executive Office of the President of the United States, Office of National Drug Control Policy-High Intensity Drug Trafficking Area, "Outstanding Intelligence Analyst" December 2000.

Steve Sellers, Major
Fairfax County (VA) Police Department

Steve Sellers is a 22-year veteran of the Fairfax County Police Department. He oversees the Criminal Investigations Bureau, which is responsible for the department's Organized Crime & Narcotics Division, Major Crimes Division, Investigative Support Division, Crime Scene Section, Victim Services Section, and the Criminal Intelligence Division. As head of the Washington-Area Sniper Prosecution Taskforce, he was instrumental in the prosecution of Lee Malvo and John Mohammad. He coordinated the many agencies and individuals involved in the prosecution efforts (for example, Fairfax County Police, police from other local jurisdictions, prosecutors, officials in the FBI and ATF, and members of the Secret Service).

He has a bachelor of arts degree in business from National-Louis University and a

masters degree in public administration from Virginia Tech. Sellers is also a graduate of the FBI National Academy, and he holds a Graduate Certificate in criminal justice from the University of Virginia.

Sellers is a member of the International Association of Chiefs of Police, National Academy Associates, Leadership Fairfax, Major Cities Chiefs Association, National Association of Public Administrators, and other national and international police organizations.

John P. Sullivan, Sergeant
Los Angeles County Sheriff's Department

John Sullivan has been a member of the Los Angeles County Sheriff's Department since 1988. Assigned to the Emergency Operations Bureau, he serves as officer-in-charge of the Terrorism Early Warning (TEW) Group. He is a member of the InterAgency Board on Equipment Standardization and Interoperability for Terrorism Response (an independent group of federal, state, and local first responders) and the Board of Advisors for the Terrorism Research Center, an independent institute in northern Virginia, dedicated to research on terrorism, information warfare and security, critical infrastructure protection, and other issues.

Sullivan is the author of more than 50 articles on terrorism, policing, and emergency response topics. He is also coauthor of *Policing Transportation Facilities, Jane's Unconventional Weapons Response Handbook, Jane's Facility Security Handbook,* and *Emergency Preparedness for Transit Terrorism*. He holds a bachelor of arts degree in government from the College of William and Mary and a master of arts degree in urban affairs and policy analysis from the New School for Social Research.

About the Office of Community Oriented Policing Services

U.S. Department of Justice

The U.S. Department of Justice Office of Community Oriented Policing Services (COPS) was created in 1994 and has the unique mission to directly serve the needs of state and local law enforcement. The COPS Office has been the driving force in advancing the concept of community policing, and is responsible for one of the greatest infusions of resources into state, local, and tribal law enforcement in our nation's history.

Since 1994, COPS has invested over $10 billion to add community policing officers to the nation's streets, enhance crime fighting technology, support crime prevention initiatives, and provide training and technical assistance to help advance community policing. COPS funding has furthered the advancement of community policing through community policing innovation conferences, the development of best practices, pilot community policing programs, and applied research and evaluation initiatives. COPS has also positioned itself to respond directly to emerging law enforcement needs. Examples include working in partnership with departments to enhance police integrity, promoting safe schools, combating the methamphetamine drug problem, and supporting homeland security efforts.

Through its grant programs, COPS is assisting and encouraging local, state, and tribal law enforcement agencies to enhance their homeland security efforts using proven community policing strategies. Traditional COPS programs such as the Universal Hiring Program (UHP) gives priority consideration to those applicants that demonstrate a use of funds related to terrorism preparedness or response through community policing. The COPS in Schools (CIS) program has a mandatory training component that includes topics on terrorism prevention, emergency response, and the critical role schools can play in community response. Finally, COPS is implementing grant programs intended to develop interoperable voice and data communications networks among emergency response agencies that will assist in addressing local homeland security demands.

The COPS Office has made substantial investments in law enforcement training. COPS created a national network of Regional Community Policing Institutes (RCPIs) to offer state and local law enforcement, elected officials, and com-

munity leaders training opportunities on a wide range of community policing topics. Most recently the RCPIs have been focusing their efforts on developing and delivering homeland security training. COPS also supports the advancement of community policing strategies through the Community Policing Consortium. Additionally, COPS has made a major investment in applied research, which makes possible the growing body of substantive knowledge covering all aspects of community policing.

These substantial investments have produced a significant community policing infrastructure across the country as evidenced by the fact that at the present time, approximately 86 percent of the nation's population is served by law enforcement agencies practicing community policing. The COPS Office continues to respond proactively by providing critical resources, training, and technical assistance to help state, local, and tribal law enforcement implement innovative and effective community policing strategies.

About PERF

The Police Executive Research Forum (PERF) is a national professional association of chief executives of large city, county, and state law enforcement agencies. PERF's objective is to improve the delivery of police services and the effectiveness of crime control through several means:

- the exercise of strong national leadership,
- the public debate of police and criminal justice issues,
- the development of research and policy, and
- the provision of vital management and leadership services to law enforcement agencies.

PERF members are selected on the basis of their commitment to the organization's objectives and principles. PERF operates under the following tenets:

- Research, experimentation, and the exchange of ideas through public discussion and debate are paths for the development of a comprehensive body of knowledge about policing.
- Substantial and purposeful academic study is a prerequisite for acquiring, understanding, and adding to that body of knowledge.
- Maintenance of the highest standards of ethics and integrity is imperative in the improvement of policing.
- The police must, within the limits of the law, be responsible and accountable to the public as the ultimate source of law enforcement authority.
- The principles embodied in the Constitution are the foundation of policing.

Categories of membership also allow the organization to benefit from the diverse views of criminal justice researchers, law enforcement of all ranks, and other professionals committed to advancing law enforcement services to all communities.

Notes

Additional copies of this report can be downloaded free of charge at
www.policeforum.org and www.cops.usdoj.gov.