THE BASIC INTELLIGENCE STARTER KIT

A Practitioner's Handbook for Becoming Involved in the Intelligence Process With an Emphasis on the Preparation of Threat Assessments

June 2008
The Basic Intelligence Starter Kit:
A Practitioner’s Handbook for Becoming Involved in the Intelligence Process With an Emphasis on the Preparation of Threat Assessments

This handbook is dedicated to all of the men and women at the Institute for Intergovernmental Research (IIR) and the California Department of Justice’s Criminal Intelligence Bureau (CIB). These people are devoted to helping protect this great country from a growing number of violent crimes. It is through IIR’s untiring efforts that law enforcement authorities are receiving an unprecedented amount of highly professional training while implementing a national criminal intelligence sharing plan. The CIB (especially my former staff) remains committed to excellence by providing law enforcement authorities and security specialists with a wide range of timely intelligence-related services that focus on the identification of potentially volatile criminal situations in an effort to prevent them from escalating. May these men and women always champion the cause of public safety and national security!

June 2008
# TABLE OF CONTENTS

**PREFACE** ........................................................................................................................................... 1

**INTRODUCTION** .................................................................................................................................. 3

**INTELLIGENCE** ................................................................................................................................... 5

  Planning and Direction .......................................................................................................................... 7

  Collection ........................................................................................................................................... 10

    Law Enforcement Sources .................................................................................................................... 12

      *Regional Information Sharing Systems* ...................................................................................... 12

      *Law Enforcement Online* ............................................................................................................. 14

      *Homeland Security Information Network* ..................................................................................... 15

      *Other State and Regional Systems* ............................................................................................... 16

    Open Sources .................................................................................................................................... 16

      *Private Security* ............................................................................................................................. 17

      *Public* ............................................................................................................................................ 18

      *World Wide Web* .......................................................................................................................... 20

    Terrorism-Specific Sources .............................................................................................................. 21

    People, Businesses, Addresses, and Telephone Number Directories ............................................. 23

    Infrastructure-Related ...................................................................................................................... 24

    General Information .......................................................................................................................... 26

      *Open Source Center* ..................................................................................................................... 27

**Processing and Collation** .................................................................................................................. 27

  Source Reliability Table ....................................................................................................................... 28

  Information Validity Table ................................................................................................................... 28

  Matrix and Link Diagram Model ......................................................................................................... 28

  Visual Investigative Analysis Model ................................................................................................... 29

**Analysis** ............................................................................................................................................. 30

  Strategic ............................................................................................................................................. 31

  Tactical .............................................................................................................................................. 32

**Dissemination** ................................................................................................................................... 32

  Need to Know .................................................................................................................................... 32

  Right to Know .................................................................................................................................. 32

  Third-Agency Rule ............................................................................................................................... 33

**Reevaluation** ................................................................................................................................... 33

**THREAT ASSESSMENTS** .................................................................................................................... 36

  Infrastructure .................................................................................................................................... 38

  Groups ................................................................................................................................................. 40

  Issues and Events ............................................................................................................................... 42

  People ................................................................................................................................................. 42
RESOURCES ...............................................................................................................................45
  Information ..........................................................................................................................45
  Associations .......................................................................................................................45
  Training ...............................................................................................................................45

RECOMMENDED READING ....................................................................................................47
  Terrorism ..............................................................................................................................47
  Intelligence ..........................................................................................................................47
  Threat Assessments ..........................................................................................................47
  Regulations ..........................................................................................................................48

BIOGRAPHY ..........................................................................................................................49
THE BASIC INTELLIGENCE STARTER KIT:
A Practitioner’s Handbook for Becoming Involved in the Intelligence Process With an Emphasis on the Preparation of Threat Assessments

PREFACE

The days of intelligence units at the state and local law enforcement levels being the only game in town when it comes to intelligence-related operations have ended. These units are now a very small part of a much larger and fast-changing dynamic that has many law enforcement authorities applying the intelligence process to all crimes while eliminating stovepipe or stand-alone files in favor of a collaborative or sharing environment.

These authorities are going beyond the conventional wisdom of limiting intelligence to a single unit by establishing intelligence functions within other units, such as narcotics, organized crime, gangs, and terrorism. Many of the authorities have also accepted the growing premise that an individual law enforcement department’s intelligence process must adapt to the fusion center concept because the merging of information far outweighs the benefits derived from any isolated effort. These assumptions are the underlying foundations of today’s state and local law enforcement’s need to communicate instantaneously and coordinate with each other in order to successfully reduce crime and violence, particularly since many functions overlap and most crime and violence know no boundaries.

Even though intelligence from a law enforcement perspective is evolving to encompass all crimes, this handbook focuses on those criminal activities that have a nexus to terrorism. Following the tragic events of September 11, 2001, the intelligence process—particularly the collection and analysis of applicable information—has taken on a whole new sense of urgency in the form of threat assessments. The rapidly growing reliance on these assessments can be found at every level of law enforcement to the point where traditional threat assessments are now beginning to share the spotlight with risk assessments and vulnerability assessments while other forms of threat-driven information are being packaged as threat-related advisories, bulletins, and alerts.

The information in this handbook is designed from a practitioner’s point of view to help those state and local law enforcement authorities who want to become involved in the intelligence process and the preparation of threat assessments. It is also intended to complement the National Criminal Intelligence Sharing Plan, a strategy for improving law enforcement’s ability to share mission-critical information.

Since every law enforcement authority in the country is charged with public safety and helping to protect national security, there is no reason for not participating in the intelligence process. This handbook provides an introductory approach to understanding how that participation works in relationship to the process; to connecting with existing information networks that enhance the relationship; to accessing certain systems, databases, and Web sites that can be useful for
collecting and sharing information; to techniques and software for charting the information; and to standards for avoiding the pitfalls often associated with misusing the information.

There is also no reason why every authority should not accept the role that threat assessments have in helping protect the public and the nation. Preventing threats from occurring or spreading is, after all, the goal of any intelligence function. This handbook offers a guide for collecting and reporting threat-related information, a list of resources to access some of the more useful assessments the moment they are released, and a description of various types of assessments. Even though there are different kinds of assessments and most law enforcement authorities will never write one, it is still incumbent upon every authority to know they play an important part in the preparation of such assessments.

Former U.S. Attorney General John Ashcroft probably said it best when he remarked, “… while we think that Washington has a role to play and that it’s important, we understand that the security and the success of the defense of liberty and freedom in America depends upon state and local law enforcement.” Given that level of dependency, state and local authorities must recognize they are in the forefront when it comes to the early detection of pre-incident indicators or warning signs that may be precursors of possible terrorist-related activities in this country.

However, since nearly 75 percent of the law enforcement departments in this country have fewer than 25 sworn officers and no intelligence function, it is unlikely that many of them are trained in the intelligence process and the preparation of threat assessments. There are enough tools in The Basic Intelligence Starter Kit for every state and local department to overcome those deficiencies, and most important, all of the tools are within easy reach and doable, no matter the size of the department.

This handbook is not a textbook nor is it an instruction manual. It is intentionally written in such a format so as not to overload nor inundate any department with every possible resource. Rather, it references only those sources that many practitioners have found to be useful and worthwhile for following up for more information. By simply leveraging the 20 easy-to-use guidelines in this handbook, any law enforcement department can become self-sufficient in the intelligence process and the preparation of threat assessments. Nearly 700,000 of the approximately 800,000 law enforcement authorities nationwide are full-time officers with state and local agencies, and such a large federation can surely be an overwhelming force multiplier when working together to help protect this country from another terrorist attack.

The information in this handbook is taken from the author’s presentations regarding The Role of Intelligence: Now More Important Than Ever Before and A Practical Guide to Threat Assessments: A Prevent Defense, both of which are part of the U.S. Department of Justice, Bureau of Justice Assistance-sponsored State and Local Anti-Terrorism Training (SLATT®) Program.

---

1 Remark made by former U.S. Attorney General John Ashcroft during the release of the National Criminal Intelligence Sharing Plan; May 14, 2004.

2 Census of State and Local Law Enforcement Agencies, 2000; U.S. Department of Justice, Bureau of Justice Assistance; October 2002.
INTRODUCTION

*Intelligence* and threat assessments are now more important than ever before following the September 11, 2001, attacks on the World Trade Center and the Pentagon. They play a major role in helping state and local law enforcement authorities protect the public and prevent another devastating act of terrorism from occurring in the United States.

Unfortunately, there will likely be another attempt to attack this country, and it is only a matter of when, not if. *The 9/11 Commission Report* stated, “Because of offensive actions against al Qaeda since 9/11 and defensive actions to improve homeland security, we believe we are safer today. But we are not safe.”\(^3\) The report also stated, “What should Americans expect from their government? The goal seems unlimited: Defeat terrorism anywhere in the world. But Americans have also been told to expect the worst: An attack is probably coming; it may be more devastating still.”\(^4\) Participating in the intelligence process and the preparation of threat assessments can help state and local law enforcement authorities thwart that attack.

Guideline 1

Read *The 9/11 Commission Report* to better understand the dynamics of terrorism and to learn more about the tragic events that occurred on September 11, 2001. Realize the enormous potential that exists for another such terrorist attack. Refer to [www.9/11commission.gov](http://www.9/11commission.gov).

Intelligence and threat assessments can also help reduce the increasing number of crimes and acts of violence committed by domestic criminal extremist groups, evolving organized crime enterprises, and the proliferation of gangs. Just the growing number of gang members alone demonstrates a need for such tools. During a federal anti-gang bill hearing in 2005, it was stated, “If they were an army from a foreign country, they would be the sixth-largest army in the

---


\(^4\) Ibid.; page 17.
world when referring to the 25,000 gangs with 750,000 members in 3,000 jurisdictions throughout the country.

Compounding these growing threats to public safety and national security are the evolving coalitions among some of the groups, enterprises, and gangs, along with the fact that many of them do not recognize jurisdictional boundaries. Furthermore, with the world rapidly shrinking in terms of travel, communications, and wire transfers, there is an urgent need to stop relying on luck when trying to prevent these organizations, including terrorist groups, from expanding their activities and to start hedging our bets by thinking of intelligence and threat assessments as standard operating procedures that can help preclude the activities from occurring or expanding.

One successful method for hedging that bet would be state and local law enforcement’s willingness to share information. Toward that end, the National Criminal Intelligence Sharing Plan was born. This initiative provides a law enforcement department, regardless of size, with a blueprint to follow when enhancing or building an intelligence function. It also recognizes that providing “… agencies with the tools and resources necessary for developing, gathering, accessing, receiving, and sharing intelligence information is critically important to improving public safety and homeland security.”

Guideline 2

Adopt the minimum standards contained in the National Criminal Intelligence Sharing Plan and help strengthen public safety. Seek ways to enhance intelligence sharing efforts and to foster information sharing initiatives. Refer to www.it.ojp.gov/global.

---

5 Sacramento Bee; May 12, 2005.
6 National Criminal Intelligence Sharing Plan, Executive Summary; October 2003.
INTELLIGENCE

So, what exactly is intelligence? Basically, it is using the knowledge derived from an analysis of information to form some type of a defensive or protective measure. Knowledge is power, and if information can be collected in advance of a particular situation, then responses can be taken to prevent the situation from occurring or expanding.

Within the confines of this handbook, intelligence is the capacity of state and local law enforcement authorities to detect and assess what, if any, pre-incident indicators or warning signs of criminal-related threats may be impacting a given jurisdiction and then subjecting that information to the intelligence process so necessary precautions or preventive measures can be anticipated and implemented. Intelligence is the capacity to anticipate.

“Capacity to Anticipate”

“Because effective intelligence operations can be applied equally well to terrorist threats and crimes in the community, homeland security and local crime prevention are not mutually exclusive.”7 State and local law enforcement departments can use this application effectively against all crimes by simply employing the concept of intelligence-led policing. It is “a collaborative enterprise based on improved intelligence operations and community-oriented policing and problem solving …”8 that every department is capable of instituting.

Guideline 3


---

7 Intelligence-Led Policing: The New Intelligence Architecture, Executive Summary; U.S. Department of Justice, Bureau of Justice Assistance; September 2005.
8 Ibid.: Executive Summary.
Intelligence is attained through the systematic exploitation of information. It is a process of putting together several often disjointed and seemingly unrelated bits and pieces of information—much like putting together a puzzle, only without the advantage of being able to see an advance picture of the completed puzzle or knowing which corners, colors, and straight edges of the puzzle go where.

The intelligence process is composed of the following steps:

Source: National Criminal Intelligence Sharing Plan
Guideline 4


Planning and Direction

The planning and direction phase of the intelligence process helps guide a department’s overall activities regarding its criminal intelligence function(s). This phase involves the development of a mission statement, the establishment of policies and procedures and, most important, the identification of what criminal-related information or indicators will be the focus of a department’s collection efforts so they are neither indiscriminate nor unfocused, particularly since there are “… possible indicators of terrorist activity which may be encountered during the course of normal operations.”

Some of the more pertinent indicators concerning suspicious or criminal activity potentially related to terrorism that state and local law enforcement departments should be able to recognize and report can be found in the U.S. Department of Homeland Security (DHS) and the U.S. Department of Justice’s *Terrorist Threats to the U.S. Homeland Reporting Guide*. It includes information on personnel, organizations, and areas of activity; capabilities; operations (terrorist attacks); and criminal activities. However, for those departments that believe no such

---

indicators exist within their jurisdiction, remember that “the absence of evidence is not the absence of a threat.”

Guideline 5

Become familiar with the pre-incident indicators or warning signs of possible terrorist-related activity, and when encountered, subject them to the intelligence process. Read the *Terrorist Threats to the U.S. Homeland Reporting Guide* for information on recognizing activities or conditions that may be indicative of terrorist activity. Refer to the Federal Bureau of Investigation’s Law Enforcement Online at [www.leo.gov](http://www.leo.gov) or e-mail ttrgreporting@dhs.gov.

The DHS Homeland Security Advisory System also offers guidance to state and local law enforcement authorities regarding planning and direction, particularly pertaining to developing protective measures. In addition to Threat Advisories and Information Bulletins, it provides the *Color-Coded Threat Level System* for communicating suggested precautions that can be used to help reduce the likelihood or impact of a terrorist attack.

Guideline 6

Become familiar with the *Homeland Security Advisory System*, particularly as it pertains to developing department-specific protective measures, and be ready to implement the necessary precautions when appropriate. Refer to [www.dhs.gov/xinfoshare/programs/gc_1156876241477.shtm](http://www.dhs.gov/xinfoshare/programs/gc_1156876241477.shtm).

---

10 Remark made by former Federal Bureau of Investigation Executive Assistant Director Maureen Baginski during the Major Cities Chiefs Association Intelligence Commanders Conference; Washington, DC; May 2004.
A major consideration of each department’s planning and direction phase should be partnering with a fusion center, which is “… an effective and efficient mechanism to exchange information and intelligence, maximize resources, streamline operations, and improve the ability to fight crime and terrorism by merging data from a variety of sources.” Such centers allow state and local law enforcement authorities to better forecast and identify emerging crime trends; support multidisciplinary, proactive, risk-based, and community-focused problem-solving activities; provide a continuous flow of information and intelligence to assist in developing a depiction of evolving threats; and improve the delivery of emergency and nonemergency services.

Guideline 7

Establish a protocol with the nearest fusion center for collaborating on the intelligence process. Read the Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era to understand the collaborative process better. Refer to www.it.ojp.gov/documents/fusion_center_guidelines.pdf.

---

Partnering with the nearest Federal Bureau of Investigation’s Joint Terrorism Task Force, if staffing levels permit, should also be a consideration of the planning and direction phase, along with always querying the National Crime Information Center when checking the name of an individual suspected of being involved in criminal activity. Such queries are automatically referenced through the Terrorist Screening Center (which maintains the U.S. government’s consolidated terrorist watch lists from multiple federal agencies) to help determine whether the suspect may have some affiliation with terrorism.

Collection

The need to collect criminal-related information is recognized by all law enforcement authorities as a foundation of the intelligence process. The collection effort must be planned, focused, and based on reasonable suspicion and criminal predicate so it always protects civil liberties and constitutional rights. Reasonable suspicion and criminal predicate are defined by Title 28, Code of Federal Regulations, Part 23 as information “which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable probability that an individual or organization is involved in a definable criminal activity or enterprise.”

The collection of such information is a balancing act between the needs of law enforcement and public safety and an individual’s right to privacy.
There are six activities that will always abuse this balance:

- Maintaining *noncriminal information*
- Insinuating *guilt by association*
- Spying and *inappropriate surveillance*
- Assuming role of *agent provocateur*
- Knowingly keeping *inaccurate information*
- Profiling

Retaining and using such misapplied information can lead to its exclusion from criminal proceedings and/or a liability lawsuit, usually for violating *Title 42, U.S. Code, Section 1983 regarding civil action for deprivation of rights*. That is why information that has been collected, subjected to the intelligence process, and *maintained in a file* by state and local law enforcement authorities is regulated by *Title 28, Code of Federal Regulations, Part 23* (28 CFR Part 23) regarding Criminal Intelligence Systems Operating Policies. This regulation provides the standards for state and local law enforcement authorities to safeguard and access such information.

However, law enforcement information that is regulated by 28 CFR Part 23 differs from national security information, which is controlled by Executive Order 12958 (a system for classifying and safeguarding information at the national level) and Executive Order 12968 (a process for restricting access to the information). Law enforcement information is collected by state and local departments “… as evidence to support a prosecution of a criminal act, or to learn more about a criminal enterprise,”\(^{12}\) whereas national security information is collected by the Intelligence Community (IC), a “federation of executive branch agencies and organizations that work separately and together to conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States.”\(^{13}\)

State and local law enforcement departments are not part of the IC and have no jurisdiction to gather or control national security intelligence, although they may inadvertently collect criminal predicate-related information that could be connected to national security intelligence as part of their normal investigative operations or, given sufficient staffing, while helping staff a federal task force.

---

**Guideline 8**

Ensure that the information collected on all suspects is based on *reasonable suspicion* and *criminal predicate*. Protect an individual’s right to privacy by adhering to the regulations that govern civil liberties and constitutional rights if the information is to be retained in an intelligence file, especially if the information may be shared as an investigative lead with another law enforcement department. Read *Title 28, Code of Federal Regulations, Part 23* regarding *Criminal Intelligence Systems Operating Policies*. Refer to [www.gpoaccess.gov/cfr/index.html](http://www.gpoaccess.gov/cfr/index.html).

---


\(^{13}\) The United States Intelligence Community; [www.intelligence.gov/1-definition.shtml](http://www.intelligence.gov/1-definition.shtml).
Law Enforcement Sources

Notwithstanding Executive Orders 12958 and 12968, which restrict state and local authorities from routinely accessing classified national security information, there are several law enforcement sources that can provide useful data. The three main law enforcement sources available to state and local departments are the Regional Information Sharing Systems®, Law Enforcement Online, and the Homeland Security Information Network.

Regional Information Sharing Systems

The Regional Information Sharing Systems (RISS) Program serves over 750,000 police officers from more than 8,000 member criminal justice agencies in 50 states, the District of Columbia, U.S. territories, Canada, Australia, and England. “The vast majority of member agencies are at the municipal and county levels, but 529 state agencies and 962 federal agencies are also members.”

RISS consists of six multistate centers; for additional information about RISS, visit www.riss.net.

Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network® (MAGLOCLEN)

- The MAGLOCLEN geographical region includes Delaware, Indiana, Maryland, Michigan, New Jersey, New York, Ohio, Pennsylvania, and the District of Columbia. The center also has member agencies in England, the Canadian provinces of Ontario and Quebec, and Australia.
- Phone: (800) 345-1322
- E-mail: info@magloclen.riss.net

Mid-States Organized Crime Information Center® (MOCIC)

- The MOCIC geographical region includes Illinois, Iowa, Kansas, Minnesota, Missouri, Nebraska, North Dakota, South Dakota, and Wisconsin. The center also has member agencies in Canada.
- Phone: (800) 846-6242
- E-mail: info@mocic.riss.net

New England State Police Information Network® (NESPIN)
- The NESPIN geographical region includes Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, and Vermont. The center also has member agencies in Canada.
- Phone: (800) 343-5682
- E-mail: info@nespin.riss.net

Regional Organized Crime Information Center® (ROCIC)
- The ROCIC geographical region includes Alabama, Arkansas, Florida, Georgia, Kentucky, Louisiana, Mississippi, North Carolina, Oklahoma, South Carolina, Tennessee, Texas, Virginia, and West Virginia, as well as Puerto Rico and the U.S. Virgin Islands.
- Phone: (800) 238-7985
- E-mail: info@rocic.riss.net

Rocky Mountain Information Network® (RMIN)
- The RMIN geographical region includes Arizona, Colorado, Idaho, Montana, Nevada, New Mexico, Utah, and Wyoming. The center also has member agencies in Canada.
- Phone: (800) 821-0640
- E-mail: info@rmin.riss.net

Western States Information Network® (WSIN)
- The WSIN geographical region includes Alaska, California, Hawaii, Oregon, and Washington. The center also has member agencies in Canada and Guam.
- Phone: (800) 952-5258
- E-mail: info@wsin.riss.net

Each center maintains its own criminal intelligence database, all of which are electronically connected via RISSNET™, a secure and private intranet. An inquiry to one center can lead to a search of all six center databases for information on criminal suspects, organizations, and activities involving, but not limited to, narcotics and human trafficking, organized crime, gang activity, identity theft, cybercrime, and terrorism. RISSLinks™ can provide data visualization and a link chart of the database information.

The RISS centers also provide the following services:

- Analysis of investigative data to document connections among individuals in a criminal organization.
- Specialized investigative equipment for loan.
- Confidential funds for purchase of evidence or information or other investigative expenses to support multijurisdictional investigations.
- Training to build expertise in investigative techniques and emerging crime problems.

Additionally, RISS offers the Automated Trusted Information Exchange (RISS ATIX™), which provides member agencies with access to a secure information sharing environment for the exchange of information. RISS ATIX consists of a Web site and a connected service hosted on the RISS network.

**Law Enforcement Online**

Law Enforcement Online (LEO) is provided by the Federal Bureau of Investigation (FBI). Approximately 32,500 people have become LEO members since its inception in 1995, and members have access to FBI Intelligence Assessments, Intelligence Bulletins, and intelligence information, along with the following resources:

- Topical focus areas, which are custom Web-type pages that provide secure information, including text, graphics, audio, and videos.
- Law enforcement special-interest groups, which limit access to specialized groups with their own membership.
- E-mail capabilities to send and receive secure messages among LEO users.
- News groups that provide bulletin boards for posting information.
- Chat capabilities that involve real-time discussions among LEO users.
- Electronic calendar for posting dates of conferences, meetings, training courses, and seminars.
Topical electronic library, which is a repository of publications, documents, studies, research, technical bulletins, and reports of interest to law enforcement.

Distance learning for providing online learning modules.

LEO is interconnected as a virtual single system with RISS to provide the initial Sensitive But Unclassified (SBU) secure communications backbone for implementation of a nationwide criminal intelligence sharing capability.

Guideline 9
Join the Regional Information Sharing Systems (RISS) Program, and use it to exchange criminal predicate-related data regarding suspects involved in multijurisdictional terrorism, gang, or organized crime activity. Benefit from its many services, including the Automated Trusted Information Exchange that shares terrorist threat data. Contact the appropriate RISS center or refer to www.rissinfo.com. Also, connect to Law Enforcement Online (LEO) and receive assessments, bulletins, and other forms of information and services from the FBI that cover a variety of topics, including terrorism, gangs, and organized crime. Refer to www.fbi.gov/hq/cjisd/leo.htm.

Homeland Security Information Network

The Homeland Security Information Network (HSIN) is a computer-based counterterrorism communications system connecting all 50 states; five territories; Washington, DC; and 50 major urban areas. It allows the states and urban areas to collect and disseminate information among those federal, state, and local agencies involved in combating terrorism. It also provides situational awareness data, facilitates information exchange and collaboration, offers advanced analytical capabilities, and enables real-time sharing of threat warnings.
HSIN’s communications capability delivers interactive connectivity with the U.S. Department of Homeland Security’s National Operations Center, where state and local authorities can access morning briefs; daily, periodic, and ongoing reports; information bulletins; suspicious incident and pre-incident indicator data; media studies and analysis; mapping and imaging displays; the critical infrastructure protection repository; and strategic analysis of terrorist threats, tactics, and weapons.

Guideline 10

Connect to the Homeland Security Information Network to receive data that can help identify terrorism-related threats. It can also help facilitate the sharing of information and the collaboration among federal, state, and local law enforcement agencies. Contact the appropriate state Office of Homeland Security, or refer to www.dhs.gov and then click on information sharing and analysis.

Other State and Regional Systems

In addition, there are numerous state and regional systems that have been created to share and exchange information of mutual concern among relevant agencies, such as the Criminal Information Sharing Alliance network (CISAnet), California’s Joint Regional Information Exchange System (CALJRIES), and Florida’s Criminal Justice Network (CJN).

Guideline 11

Consider a system such as CALJRIES and develop the potential for becoming involved in virtual intelligence with real-time interactive capabilities shared among federal, state, and local law enforcement departments. For more information about CALJRIES, e-mail sttac@doj.ca.gov.

Open Sources

There are plenty of open sources that can be helpful to state and local law enforcement authorities needing additional mission-critical information. Some sources provide terrorism-specific and/or infrastructure protection-related data, while other sources provide crucial background information regarding criminal suspects or similar investigative-related topics once reasonable suspicion and criminal predicate have been established. Allen W. Dulles, the Director of the Central Intelligence Agency from 1953 to 1961, once acknowledged to a congressional committee that “more than 80 percent of intelligence is obtained from open sources.”¹⁵ That statement was made before the birth of the Internet. Lieutenant General Sam Wilson, former Director of the Defense Intelligence Agency, has since indicated that “… ninety percent of intelligence comes from open sources.”¹⁶

---

¹⁵ Richard S. Friedman; “Open Source Intelligence”; U.S. Army War College Quarterly; Summer 1998.
¹⁶ Ibid.
Regardless of the amount of intelligence that can be obtained from open sources, a good
*collector* can gather useful information from sources such as the private security industry, public
sources, and the World Wide Web. Some of the following sources may require registering as an
associate or member and/or paying a subscription fee, but all of them are accessible to state and
local law enforcement authorities.

**Private Security**

Nearly 85 percent of this country’s infrastructure is protected by over 2 million people within the
private security industry. These people can be a wealth of information regarding suspected
terrorist-related activity that occurs on or near infrastructure sites.

There are also agencies that regulate both this industry and similar organizations which provide
business-related security information regarding infrastructure protection. Usually, a state agency
regulates the license for private security people and firms, including infrastructure sites that
utilize such security precautions as a part of their workforce. These agencies can provide state
and local law enforcement authorities with a roster of firms and infrastructure sites that employ
security people who, in turn, could be a good source of information, particularly as it relates to
potential acts of suspected terrorism.

There are also organizations related to private businesses with connections at the international
level that specialize in security information. One good example is the Overseas Security
Advisory Council (OSAC), a federal advisory committee “with a U.S. Government Charter to
promote security cooperation between American business and private sector interests worldwide
and the U.S. Department of State.”\(^\text{17}\) OSAC maintains a Web site that is operated by the
Department of State’s Bureau of Diplomatic Security. It is a focal point for the exchange of
unclassified information between the Department and the private sector regarding international
security-related incidents and threats. Some of the information accessible from the Web site
includes Department of State Travel Warnings and Public Announcements, daily security-related
news articles, international reports on security and crime incidents, terrorist group profiles,
timely presentations on current terrorist attacks and other related incidents, general crime
information for specific cities and countries, cyber threat information, and critical incident
reporting. It is “available to Federal, State, and local law enforcement agencies on an associate
basis.”\(^\text{18}\) It is an encrypted site that requires a password.

---

\(^\text{17}\) Overseas Security Advisory Council; [www.osac.gov](http://www.osac.gov); October 29, 2006.

\(^\text{18}\) Ibid.
Guideline 12

Partner with the private security sectors responsible for protecting critical infrastructure sites, and take advantage of their *eyes and ears* by establishing regular communications and developing a protocol for exchanging information regarding pre-incident indicators or warning signs of potential terrorism. Consider becoming an associate of the *Overseas Security Advisory Council* and getting log-on privileges to its open source information that may have an impact on the protection of business-related infrastructure sites at a local or state level. Refer to [www.osac.gov](http://www.osac.gov).

Public

There are several public sources that can help provide information to state and local law enforcement authorities. Two such sources include ChoicePoint and LexisNexis. They require a subscription fee but may be able to supply valuable background information on a suspect or criminal investigation.

ChoicePoint offers a wide range of services that provide “… mission-critical information to the government, helping advance the efforts of law enforcement …”19 Services such as AutoTrackXP provide Internet access to more than 17 billion current and historical records on individuals and businesses. With as little information as a name or social security number, users can cross-reference public and proprietary records, including identity verification information, relatives and associates, corporate information, real property records, and deed transfers.

ChoicePoint’s iMapData delivers relevant and tailored information via a Web-based map interface with thousands of existing data layers of targeted and actionable information, including business, economic, demographic, and geographic displays. It can be particularly beneficial to state and local law enforcement authorities in the form of a Critical Infrastructure Management System.

---

iMapData is also the purveyor of a geographical information system utilized by the FBI’s Foreign Terrorist Tracking Task Force (FTTTF), which provides “information that helps keep foreign terrorists and their supporters out of the U.S. or leads to their removal, detention, prosecution or other legal action.” The system supplies unclassified data, public data, and/or critical infrastructures on a map of the nation and allows for the overlaying of diverse data that can be used in formulating predictive analysis and identifying potential terrorism targets. The FTTTF makes this tool available to state and local law enforcement.

ChoicePoint also provides i2, a visual investigative analysis software that is an integrated suite of products that enables investigators and intelligence analysts to quickly understand complex scenarios and volumes of seemingly unrelated data, perform analysis, and communicate the results. i2 is the technology that enables members of the Regional Information Sharing Systems Program to view its multijurisdictional crime and intelligence data in an easy-to-interpret visual format.

---

LexisNexis also offers a wide range of services, including access to over 1,400 data sources and 4.2 billion records that can help locate background information on suspects, fugitives, their businesses, and real estate assets. It also provides information on their current and previous addresses, phone numbers, aliases, judgment and bankruptcy records, tax liens, incorporation information, and associated people and businesses.

Additionally, LexisNexis includes information from the U.S. Department of the Treasury Office of Foreign Assets Control’s (OFAC) Specifically Designated Nationals and Blocked Persons list (which can also be accessed at www.treas.gov/offices/enforcement/ofac/sdn). The OFAC “administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction.”

LexisNexis SmartLinx also utilizes the i2 technology to sift through its records and then establish associations among people, businesses, locations, phone numbers, assets, and associated entities. It provides sounds like and proximity search capabilities, along with warning flags that alert on potential risk indicators of fraud. It can generate a link chart of the associations that could help discover relationships that were not readily apparent.

Guideline 13
Subscribe to public sources that provide information regarding criminal-related suspects and threat assessments. Refer to such sources as www.choicepoint.com and www.lexisnexis.com.

World Wide Web
There are plenty of World Wide Web sites that can supply state and local law enforcement authorities with open source information related to criminal suspects, investigations, and threat assessments. The following Web sites are only a few examples of that information, and even though they are by no means a complete listing of all such sites or an endorsement of them over those not listed in this handbook, they are provided as illustrations of sites where authorities can

seek such open source information. Some of the examples may require registering with the company and/or paying a fee for search services.

Terrorism-Specific Sources

www.tkb.org—Terrorism Knowledge Base provides research and analysis on global terrorist groups, leaders, members, locations, ideology, tactics, court cases, and 20,000-plus incidents from 1968 to the present. It features interactive maps, statistical summaries, analytical tools that can create custom graphs and tables regarding terrorist incidents statistics, and a comparison tool for groups by region, target, tactic, and date.

www.siteintelgroup.org—The Site Intelligence Group monitors terrorist Web sites and penetrates password-protected al Qaeda-linked sites. Then they provide original and translated transcripts of terrorist-related speeches, videos, audio messages, chatter, and communiqués.

www.trackingthethreat.com—The Tracking the Threat Web site provides a database on the al Qaeda terrorist network, including people, places, organizations, and events, along with personal, organizational, transactional, and historical connections among these entities. It also provides an interactive visual analysis tool that shows the connections in a link chart format and a geospatial view tool that shows the current geographical disposition of the entities.
Global Incident Map provides a global display of terrorism events with updated information regarding a variety of terrorism-related incidents. Clicking on the item of interest provides the full incident description and links to related news items as well as a more precise satellite and map image.

Other Web sites that are also worthy of mention but are less focused on terrorist groups, leaders, and members and more focused on counterterrorism-related issues include:

The Institute for Counter-Terrorism site focuses solely on the subject of counterterrorism. It contains a database of profiled international terrorist organizations and their history, structure, and activities along with their types, locations, and methods of attacks from 1988 to the present.
www.terrorismanswers.com—The Council on Foreign Relations is an American think tank that promotes research and analysis on issues regarding U.S. foreign policy—including terrorism—ranging from groups, state sponsors, targets, and weapons, to leaders, attacks, financing, and havens.

www.cia.gov/cia/publications/factbook—The Central Intelligence Agency’s The World Factbook is a yearly update to the former encyclopedic National Intelligence Survey, which provided the “essential elements of basic intelligence on all areas of the world.”

People, Businesses, Addresses, and Telephone Number Directories

www.infobel.com/world/default.asp (fee-based)—The infobel site contains international white and yellow pages for over 100 countries. The site offers search services for individuals and businesses; current and old addresses; current phone, cell phone, and unlisted phone numbers; property records; marriage and divorce records; and death records, as well as reverse e-mail, individual, business, and license plate searches.

www.infospace.com (fee-based)—The InfoSpace site helps locate people and businesses in North America, the Middle East, Latin America, Europe, Australia, Asia, and Africa; searches yellow pages for businesses by type and name and white pages for people; and provides reverse lookups for addresses and phone numbers.

www.iaf.net (fee-based)—IAF.NET provides reverse searches for residence and e-mail addresses along with phone numbers, including cell phones, and helps locate people.

There are several other Web sites that offer, among their many services, free information to help locate people and cross-reference addresses and phone numbers. The following examples provide links to some of those sites:

- **www.craigball.com/hotlinks.html**—This site provides links for finding people, corporations, insurance companies, aircraft ownership, Coast Guard registration of vessels, commercial interstate carriers, and information on product liability, medical issues, and banks. It also provides links to sites that find people, e-mail addresses, and phone numbers and that provide reverse searches by phone number and address as well as bankruptcy records for free.

- **www.melissadata.com/lookups/index.htm**—This site requires registration with the company but offers links for some free lookup capabilities regarding people, phone numbers Internet Protocol locations worldwide, business credit reports, U.S. and Canadian street and address data, radius searches for ZIP and area codes, and census demographics linked to a city, county, or state.

- **www.people-search-global.com**—This site links to international people-related search engines and is organized by country.

- **www.peoplesearchlinks.com**—This site offers a free search directory for locating people.

- **www.peoplessearch.net**—This site links most Web sites that can help locate people, businesses, and Internet addresses.

- **www.zabasearch.com**—This site provides a variety of people-related information searches for free.

**Infrastructure-Related**

“Protecting the critical infrastructure and key resources (CI/KR) of the United States is essential to the Nation’s security, public health and safety, economic vitality, and way of life. Attacks on the CI/KR could significantly disrupt the functioning of government and business alike and produce cascading effects far beyond the targeted sector and physical location of the incident.”

The protection of those infrastructures and resources—ranging from dams, bridges, and transportation hubs, such as airports and seaports, to nuclear reactors, electrical grids, and

---

cyberspace—is a priority responsibility of law enforcement authorities in every state and local jurisdiction. The following open source Web sites can help provide those authorities with some security alerts and bulletins, while other sites expose the location of certain infrastructures and resources.

www.dhs.gov—The U.S. Department of Homeland Security maintains the Daily Open Source Infrastructure Report, which is a daily summary of open source information concerning significant critical infrastructure issues that are divided by key assets such as energy, chemical industry, hazardous materials, defense industrial base, banking and finance, transportation and border security, postal and shipping, agriculture, food, water, public health, government, emergency services, and information technology and telecommunications.

www.us-cert.gov—The United States Computer Emergency Readiness Team (US-CERT), a partnership between the U.S. Department of Homeland Security and the public and private sectors, helps protect the nation’s Internet infrastructure while coordinating a defense against and a response to cyber attacks. US-CERT is the operational arm of the National Cyber Security Division at DHS, and it disseminates cyber threat warning information in the form of Technical Security Alerts, Security Bulletins, Security Alerts, and Security Tips, especially regarding the coordination of a virus and spyware defense. It also disseminates a regularly updated summary of the most frequent high-impact types of security incidents being reported, along with new and notable vulnerabilities.

www.infragard.net—The FBI’s InfraGard is an information sharing effort among businesses, academic institutions, the FBI, and state and local law enforcement agencies regarding physical and cyber threats to critical infrastructure sites. It provides information on matters related to counterterrorism and cybercrime as they pertain to these sites and their vulnerabilities. Reference www.infragard.net/membership to become a member of InfraGard. Members have access to InfraGard’s secure Web site, which provides information about recent intrusions and research related to critical infrastructure protection.
Some other open sources that could assist state and local law enforcement authorities with information regarding the protection of sensitive infrastructure sites within their jurisdiction include:

**www.transitsecurityreport.com**—This site produces security digests two to three times per week (plus special-incident reports when necessary) regarding railroad and train stations; buses and bus stations; aircraft and airports; hijacked and stolen buses, boats, and planes; cargo and container security; and maritime and seaport security.

**www.cryptome.org** and its counterparts **www.eyeballing-serie.org** and **www.cartome.org**—These sites provide information on the Web that includes satellite imagery, street maps, and pictures of many infrastructure sites.

**www.thehacktivist.com**—This site provides information on computer hacking, including anything that “aims to disrupt the operation of information.”24 *Hacktivists*—along with terrorists, industrial spies, and organized crime groups—are mentioned by the United States Computer Emergency Readiness Team (US-CERT) as “deliberate threats” to control systems or networks using a data communications pathway.

**General Information**

There are also plenty of open source Web sites that provide general background information and insight regarding the country of origin pertaining to terrorist-related suspects or strategic intelligence-related issues.

**www.clandestineradio.com**—This news site claims to provide “open source intelligence on subversive radio and TV broadcasts”25 with an emphasis on *country intelligence*. It is an online portal dedicated to the study of clandestine and subversive radio and can be an effective source of information when analyzing and tracking “psywar developments across the globe.”26

---

26 Ibid.
www.stratfor.com (fee-based)—Strategic Forecasting, Inc., was selected in 2003 as the Best Intelligence Website in Time.com’s 50 Best Websites. It provides strategic-related analysis of global geopolitical risks; free intelligence reports on the latest intelligence developments and issues in geopolitics, security, and public policy; and online subscriptions for individual or department access to its Web-based intelligence portal and daily e-mail briefs.

www.thepaperboy.com (fee-based)—Paperboy provides links to over 6,000 newspapers worldwide.

Open Source Center

The Open Source Center is a U.S. government organization that provides open source information to a variety of governmental agencies and other authorized organizations. A particularly useful source of information provided by the center is the Foreign Broadcast Information System, an open source component of the Central Intelligence Agency’s Directorate of Science and Technology. The center monitors, translates, and disseminates openly available news and information from foreign media sources. All users of the center, including state and local law enforcement agencies, must register for access to the information and get a user ID and password. Contact the Open Source Center at (800) 205-8615 for registration information.

Guideline 14

Take advantage of open sources, including the Open Source Center, which can help provide information regarding criminal-related suspects and the preparation of threat assessments. Just remember that information obtained from such sources must also meet the criminal-predicate requirement if it is to be retained in an intelligence file.

Processing and Collation

Information that is collected needs to be processed, collated, and evaluated for reliability of the source and validity of the data. Since some of the information will likely consist of unverified allegations, evaluating the source and data helps measure its usefulness and accuracy while weeding out disinformation.
To help ensure uniformity when systematically sifting out and eliminating the useless, irrelevant, and erroneous sources and data, information can be evaluated according to the criteria shown in the following tables.

**Source Reliability Table**

<table>
<thead>
<tr>
<th>Class</th>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Reliable</td>
<td>Source’s reliability is unquestioned or has been well tested in the past.</td>
</tr>
<tr>
<td>B</td>
<td>Usually reliable</td>
<td>Source’s reliability can usually be relied upon as factual. The majority of past information has proven to be reliable.</td>
</tr>
<tr>
<td>C</td>
<td>Unreliable</td>
<td>Source’s reliability has been sporadic.</td>
</tr>
<tr>
<td>D</td>
<td>Unknown</td>
<td>Source’s reliability cannot be judged. Authenticity or trustworthiness has not been determined by either experience or investigation.</td>
</tr>
</tbody>
</table>

Source: Threat Assessment Guide: Evaluating and Analyzing Criminal Extremist Groups

**Information Validity Table**

<table>
<thead>
<tr>
<th>Class</th>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Confirmed</td>
<td>The information has been corroborated.</td>
</tr>
<tr>
<td>2</td>
<td>Probable</td>
<td>The information is consistent with past accounts.</td>
</tr>
<tr>
<td>3</td>
<td>Doubtful</td>
<td>The information is inconsistent with past accounts.</td>
</tr>
<tr>
<td>4</td>
<td>Cannot be judged</td>
<td>The information cannot be evaluated.</td>
</tr>
</tbody>
</table>

Source: Threat Assessment Guide: Evaluating and Analyzing Criminal Extremist Groups

Information that has been evaluated, whereby fact has been separated from fiction, then needs to be sorted, organized, and collated to determine its relevancy to the *bigger picture*. This orderly arrangement of the remaining data helps establish associations and/or patterns between apparently disconnected elements.

**Matrix and Link Diagram Model**

One method of displaying associations and/or patterns is the matrix and link diagram model. It provides a meaningful way to reduce written information that is either extensive or disorganized—or both—to a visual format. Such a format helps clarify the association among members of a criminal organization or terrorist group.
A matrix documents, with dots, the known associations among members of the organization or group and, with circles, suspected associations among members of the organization or group using the following format.

Legend: ● (Dot) documents known associations
○ (Circle) documents suspected associations

A link diagram converts the dots and circles from the matrix into a visual representation using solid lines to represent the known associations and broken lines to represent the suspected associations in the following format.

Visual Investigative Analysis Model

A variation of the methodology based on associations and/or patterns is the rearrangement of the same elements, especially those focused on events, into a chronological order using a visual investigative analysis (VIA) model. Such a readjustment of the information may be able to help identify circumstances or situations that could be precursors or pre-incident indicators to a potential act of terrorism.
A VIA model, established on the elements posed in the previous matrix and link diagram, could look like the following format:

![Diagram of VIA model]

There are plenty of software options that help with the arrangement of information into a link diagram, a visual investigative analysis chart, or any of the other following products: telephone toll call analysis, financial transaction analysis, commodity flow analysis, crime pattern and crime scene analysis, and pre-incident indicators or warning signs. The International Association of Crime Analysts provides a shopping list of “crime analysis software” at www.iaca.net/software.asp.

One of the more useful software options is the Real-time Analytical Intelligence Database (RAID) offered by the U.S. Department of Justice’s National Drug Intelligence Center (NDIC) (www.usdoj.gov/ndic). It provides a methodology for managing large volumes of investigative information while helping to link people, places, businesses, telephone numbers, financial accounts, weapons, vehicles, and events contained in the information. Among its many procedures is the availability to exploit investigative data written in English, Spanish, French, German, and Arabic. The NDIC offers the software and training in its use at no cost.

**Guideline 15**

Understand the concept of visualizing information in a link diagram and visual investigative analysis format. Benefit from such visualization by utilizing software that helps piece together information that may identify the extent (and sometimes the intent) of a criminal organization, including a terrorist group. Refer to www.rff.com/link_analysis.htm and www.rff.com/sample_criminal_analysis.htm.

**Analysis**

So, what is the key ingredient to this process that often seems to be missing?
Analysis is the core of the intelligence process. It is the phase of the process that converts the bits and pieces of information collected from multiple sources into a bigger picture that has meaning. It is the so what syndrome that differentiates fact from fiction. The goal of analysis is to develop the most precise and valid inference possible from all available sources. Without analysis, information remains just that—a piece of information.

“Analysis supports good resource management and is directly involved in creating situational awareness, in assisting in decision making, and in providing knowledge bases for law enforcement action .... Law enforcement intelligence programs should produce both strategic and tactical products to support the mission and priorities of the agency.”

Strategic

Strategic analysis is the blending of facts that produces an informed judgment. It can describe, among many things, a criminal organization’s or terrorist group’s ideology, tactics, membership, capabilities, vulnerabilities, and violence potential. Strategic analysis deals with the major criminal-related issues that concern law enforcement authorities the most and allows for long-range planning to investigate the organizations and groups before they become a significant crime problem or commit an act of violence.
Tactical

Tactical analysis contributes directly to an immediate objective and is geared toward a specific criminal activity with the immediate goal of neutralizing it. It may be supplying an investigative lead, compiling a list of potential suspects, or highlighting some small fact about the activities of a particular suspect. Tactical intelligence can take many forms, but it is used mainly in assembling a report on a particular suspect with a view toward investigation and arrest.

Guideline 16

Appreciate the important role that analysis plays in the intelligence process by supporting the development of sound, professional analytic products. Develop the analytical capability or seek access to an analyst. Refer to the Law Enforcement Analytic Standards at www.jaleia.org.

Dissemination

To be useful, the products of the intelligence process need to be shared in a timely manner with those authorities who most need them. Dissemination of these products is determined by the purpose of the information and the recipient of the information, who must have both a need to know and a right to know the information.

Need to Know

The law enforcement authority seeking the information in order to execute his or her official responsibility must have a need to know the information in order to advance an investigation.

Right to Know

The law enforcement authority seeking the information must have the right to know the information by virtue of his or her official capacity.
Third-Agency Rule

Information received from an external law enforcement agency should never be shared or disseminated to another agency (third agency) without the approval of the external agency.

Guideline 17


Reevaluation

The focus of intelligence is a never-ending process and must always be reevaluated to make sure it is meeting the immediate needs of public safety. Because of the ongoing potential for another major terrorist attack in this country, the role of intelligence and the preparation of threat assessments remain critical functions for state and local law enforcement authorities.

However, it is not just terrorism that drives the need for such vigilance. Many authorities are also finding it necessary to adjust the intelligence process by including other criminal-related threats, such as gang members who frequently travel inter- and intrastate to commit their violent crimes, the growing number of national criminal alliances, and the global expansion of some criminal enterprises that victimize local jurisdictions.

In addition to these adjustments, state and local law enforcement authorities also have to adapt to threats posed by international organized crime groups, such as those involved in human trafficking and international fraud. “Globally, the United Nations estimates about 700,000 people become victims of human trafficking, the fastest growing form of international organized crime and one that generates about $10 billion in annual profit. It is tied with illegal arms as the second largest criminal activity in the world.” International fraud groups, such as the one that is believed to have perpetrated the biggest computer heist ever of customer debit card numbers, have also become a state and local issue. That heist alone “… led to potentially millions of dollars in theft by a global ring using the stolen debit information and personal identification numbers. It is thought that at least 350,000 accounts across the country were defrauded, involving more than $10 million in losses …”

A much bigger adjustment for state and local authorities is the ever-expanding arena of digital evidence, cybercrime, and hacking. Digital evidence of any crime that leaves an electronic trail taken from seized computers, laptops, hard drives, digital cameras, and phones can provide mountains of raw intelligence data for investigators and analysts. But accompanying the flurry of potential criminal intelligence is the problem of possible digital tampering, which most authorities are not trained to recognize. “Each day, state and local law enforcement officers must identify, gather, and analyze both physical and electronic evidence in a wide range of cases. Most police officers are skilled at recognizing physical evidence in such cases, but many have

29 “Banks Rush to Stem Gigantic PIN Rip-Off”; Sacramento Bee; April 22, 2006.
never been trained to recognize the existence or importance of electronic evidence in solving a crime or building a winning case.”

Cyber crimes, or weapons of mass disruption, affected “about one of every 16 U.S. adults ...” during 2005, and computer viruses and spyware cost U.S. businesses and consumers more than $67 billion, a number that is projected to get worse. Exasperating state and local authorities are the warnings being offered by computer company security personnel that they can expect to see an increase in pinpoint attacks that steal specific computer-related information from individuals and businesses, indicating that the attacks could become more targeted and potentially damaging.

Hacking is another cyber issue that is becoming a new investigative frontier for many state and local law enforcement authorities, and if the number of incidents being reported at the federal level is any indication, these authorities will need to expedite their investigative training efforts in this area. In one targeted arena alone at the federal level, the number of reported attempts “... to penetrate Pentagon computer networks rose dramatically in the past decade, from fewer than 800 in 1996 to more than 160,000 last year [2005]—thousands of them successful.”

Compounding the future of intelligence among state and local law enforcement authorities is the changing complexity and trend of some electronic surveillance. As far back as the late 1990s, federal authorities began to see an increasing sophistication in some investigations that involved global alliances among international criminal organizations. One investigation involved Russian organized crime, a Russian military submarine, Colombian narcotic traffickers, Florida, and potentially the Pacific Coast. “The investigation produced five hundred and thirty wiretapped conversations, in English, Russian, Hebrew, Yiddish, and Spanish. It took a team of 20 translators a year to transcribe and analyze the tapes.”

Recent technological advances such as PDA units and PayPal suggest that new trends could evolve and challenge the traditional electronic surveillances. A PDA could be used in lieu of a telephone. Nothing is said, data is erased, and anonymizers cut tracking capabilities. Thus, short-range transmission intercepts are virtually impossible to track once completed, and linguistic morphology-speaking, automatic encryption with PGP or similar tools makes the code virtually unbreakable. A PDA can also be used to securely transfer money, via PayPal, to any e-mail user in the world, and with this international connectivity, the transfer is as easy as making a phone call next door.

Unfortunately, other types of advances that threaten health, such as those being made by certain pandemics and pathogens, will also create a need for state and local law enforcement authorities to work together more closely while maintaining a relentless intelligence sharing effort. Avian influenza (bird flu), for example, which kills one of every two infected persons, could be a major threat. A typical flu kills only one of every 1,000 infected people. On the other hand, a bioterrorism-induced threat could be catastrophic. Anthrax, which is “considered one of the most likely substances to be used by terrorists ... can infect a person through a cut, contaminated food, or the air.” In addition, “smallpox, botulism, plague, cholera, and the Ebola virus ... could

---

33 “Land of the Stupid”; The New Yorker; April 10, 2000.
cause widespread havoc,” and experts believe that “contaminating a milk-processing facility with one gram of botulism toxin could sicken 150,000 people and kill more than half of them.”34

Regardless of how daunting these advances may seem to some state and local law enforcement authorities (especially when added to law enforcement’s current and constant campaign against another terrorist attack, the movement of gang members and organized crime figures among multiple jurisdictions, and the increasing level of violence and criminal sophistication that frequently accompany such movements), the role of intelligence and the preparation of threat assessments still remain two of most successful proactive methods to help protect public safety. Law enforcement authorities can easily participate in these methods by continuously reevaluating the threats to their jurisdictions and adjusting accordingly. Intelligence and threat assessments should be included as part of everyday operations because, without them, law enforcement’s response to any threat, especially national security, will only be reactive and after the fact, not preventive.

34 “Bioterror Fight Hits Big Snag”; Sacramento Bee; September 26, 2005.
THREAT ASSESSMENTS

Assessing threats to public safety is a primary purpose and an important by-product of the intelligence process. It is all about leverage, and threat assessments offer that advantage.

Just like intelligence, threat assessments provide authorities with the capacity to anticipate what, if any, pre-incident indicators or warning signs of threats may be impacting a given jurisdiction and then subject those indicators to the intelligence process so necessary prevention measures can be implemented.

“Capacity to Anticipate”

“Foremost among the demands that confront police in the post-September 11 environment is the ability to effectively and efficiently collect, assess, disseminate, and act on intelligence information regarding threats posed by transnational and domestic terrorists.”35 All state and local law enforcement authorities play a crucial role in fulfilling that demand. After all, threat assessments do not grow on trees. To be meaningful, they must be timely and contain the most accurate and complete information available. Toward that level of integrity, every law enforcement authority is undeniably a part of the whole and, capitalizing on the force multiplier concept, should share information that could be a vital or missing piece to a much larger puzzle. The preparation of threat assessments is so intertwined with the intelligence process that it is nearly impossible to have one without the other, and without everyone participating in the process, these assessments become unreliable.

So, what do threat assessments look like? Well, looks can be deceiving.

In today’s world, the concept of threat assessments is also being applied (and sometimes misapplied) when preparing risk assessments and, to a lesser degree, vulnerability assessments. Although all of

these assessments, especially threat and risk assessments, frequently contain many of the same elements (such as the potential threat, the likelihood of an attack, and the target’s weaknesses), they each have an individual purpose and a particular function. Determination of assessment depends on the precipitating nature of the information and whether the primary focus of the assessment is based on threats, risks, vulnerability, or all of the above.

Basically, threat assessments identify and evaluate potential threats made or posed by a specific individual or group. These assessments are predicated on several factors, including, but by no means limited to, the individual’s or group’s capability and intent of attacking a definitive target and the likelihood of an attack. (A target could be anything that may be the victim of a threat, such as a critical asset that is a possible objective of a terrorist attack, a community held hostage to gang activity, a person victimized by an organized crime group, or an event that could attract individuals intent on disrupting it by causing acts of violence.)

Risk assessments concentrate on the process of understanding the likelihood that a threat could attack a particular target with some severity of consequences, whereas vulnerability assessments focus on the identification of a target’s weaknesses, including physical structures, personnel protection systems, processes, or other areas that could be exploited.

At the same time, there are variations of threat assessments—other threat-related information is also being packaged in various forms, such as Threat Advisories, Information Bulletins, and Security Alerts. Threat Advisories usually contain immediate actionable information about a specific incident involving—or a significant threat targeting—critical infrastructures or key assets. Information Bulletins typically communicate information of interest to the nation’s critical infrastructures that does not meet the timeliness, specificity, or significance threshold of Threat Advisories. Security Alerts generally provide information on cyber-related security issues, vulnerabilities, and exploits.

The DHS Homeland Security Advisory System combines threat information with vulnerability assessments, which are available in the form of Threat Advisories and Information Bulletins from www.dhs.gov and Security Alerts from www.us-cert.gov.

An emphasis of this handbook is on the preparation of threat assessments, which more often than not will also include some references to risk and vulnerability. These assessments are transitional in the sense that they can be applied to every crime category and, regardless of the category, will always address threats to infrastructure from groups, about issues and/or events, or by people. Many of these assessments and most of the threat information are made available to state and local law enforcement authorities the moment they are disseminated and posted on the secure Regional Information Sharing Systems network (RISSNET), the Law Enforcement Online system, and/or the Homeland Security Information Network.

Guideline 18

Capitalize on accessing existing threat assessments and other threat-related information by participating in the various systems and networks distributing such data. Leverage the information to help safeguard community assets.
Infrastructure

Probably the most sought-after type of threat assessment that also focuses on risk and vulnerability by state and local law enforcement authorities is the one that centers on the protection of critical infrastructures and key assets. “Critical infrastructures are on the front line in the war on terror and therefore have a key role as primary sources of threat-related information.”36 “Terrorists seek to destroy, incapacitate, or exploit critical infrastructure and key resources across the United States to threaten national security, cause mass casualties, weaken our economy, and damage public morale and confidence. America’s open and technologically complex society includes a wide range of critical infrastructure and key resources that are potential terrorist targets. The majority of these are owned and operated by the private sector and state or local governments. These critical infrastructures and key resources are both physical and cyber-based and span all sectors of the economy.”37

The basic infrastructure sectors—those assets deemed most critical to public health and safety, governance, and economic and national security—include:

- Agriculture
- Banking and finance
- Chemical and hazardous waste
- Defense industrial base, including research centers
- Energy
- Emergency services
- Food
- Government
- Information and telecommunications
- Transportation facilities and terminals
- Postal and shipping services
- Public utilities, such as electricity, water, natural gas, and waste treatment

Besides aiding the federal government in taking stock and facilitating the protective measures of these infrastructures and assets, state and local law enforcement authorities must also ensure that their community’s vulnerability to attack is properly analyzed and monitored. There are sources that already produce and offer such information, including the Daily Open Source Infrastructure Report by the U.S. Department of Homeland Security at www.dhs.gov; the DHS and the United States Computer Emergency Readiness Team information regarding the Internet infrastructure, especially as it pertains to security issues, vulnerabilities, and exploits, at www.us-cert.gov; and the FBI’s InfraGard program, which shares information on physical and cyber threats to critical infrastructure at www.infragard.net.

The National Infrastructure Protection Plan, which is available at www.dhs.gov/nipp, can help state and local authorities enhance their ability to build a safer and more secure community while

strengthening their preparedness and response efforts. The Plan provides information regarding the vulnerability of the U.S. infrastructure to twenty-first-century threats; the nature of possible terrorist attacks; the protection of sensitive information; the sharing of information; the identification of assets, systems, networks, and functions; and the state and local roles in deterring the threat and mitigating the vulnerabilities.

The *Terrorist Threats to the U.S. Homeland Reporting Guide for Critical Infrastructure and Key Resource Owners and Operators* can also help state and local law enforcement authorities. It leverages the vast information resources of law enforcement and private industry to assist in recognizing activities or conditions that may be indicative of terrorist threats to the nation’s critical infrastructure. A copy of this document can be obtained from [www.tisp.org/files/pdf/ci_jan_07_2005.pdf](http://www.tisp.org/files/pdf/ci_jan_07_2005.pdf).

Finally, one methodology that can be used by state and local law enforcement authorities to help analyze and evaluate critical assets is a technique called CARVER. It is a well-defined process that has long been recognized as a model for using specific criteria to address a broad range of factors, and its attack-oriented perspective identifies those assets that might be among the most attractive to terrorists.
The CARVER methodology relies on the following factors:

- **Criticality**—A target is considered critical when its destruction has a significant impact on governmental or economic operations within a given jurisdiction.

- **Accessibility**—The ease by which the target can be accessed.

- **Recuperability**—The measure of time required to repair, replace, or bypass the damage inflicted on the target.

- **Vulnerability**—The measure of the target’s defensive capability against an attack.

- **Effect**—The positive or negative influence on the population within a given jurisdiction as a result of an attack.

- **Recognizability**—The ease by which the target can be recognized.

One example of the CARVER methodology being used as an assessment tool is the U.S. Food and Drug Administration’s *Risk Assessment for Food Terrorism and Other Food Safety Concerns*, which can be seen at [www.cfsan.fda.gov/~dms/rabtact.html](http://www.cfsan.fda.gov/~dms/rabtact.html).

**Groups**

Assessing groups (focusing on a specific group such as al Qaeda rather than multiple groups that make up the topic of terrorism per se) addresses the dynamics of a particular organization and can be used across the board to include terrorism, criminal extremism, gangs, organized crime, or any other criminal enterprise, such as a particular narcotic cartel.

A copy of the *Al Qaeda: Profile and Threat Assessment* is available via [www.usembassy.it/pdf/other/rl33038.pdf](http://www.usembassy.it/pdf/other/rl33038.pdf).

Some groups may be large and full of braggadocio (e.g., gangs), whereas others are small and clandestine (e.g., criminal extremists). Regardless of their size and tactics, their threat to public safety involves criminal activities, and when violence is involved, their threatening nature often seems limitless. These actions may be random, indiscriminate, or symbolic, or they may be complex, well-planned, and precise.
The anatomy of a group-related threat assessment will often contain many of the following characteristics:

- Membership—capable of committing an act of violence?
- Types of crimes—predatory, organized, violent?
- Ideology—determined, motivated, focused?
- Field of operations—geographical area(s) of activity?
- Tactics—preferred methods of operations?
- Motives—object influencing a choice?
- Intentions—propose to accomplish?
- Capability—capacity to commit an act of violence?
- Probability—likelihood and immediacy of threat?
- Violence potential—talking or planning?

One assessment tool that may help state and local law enforcement authorities is the Threat Assessment Guide: Evaluating and Analyzing Criminal Extremist Groups. It provides a checklist of information that is needed to make an assessment of criminal extremist groups that create a climate of fear and intimidation by endorsing or resorting to criminal activities involving force, loss of life, extensive harm to persons, or damage to property in order to further their goals or beliefs, thereby causing concern for the personal safety of others. The guide is based on the intelligence process and helps to evaluate the group’s characteristics, analyze the risks, and measure the violence potential associated with the group. Most important, the checklist format is designed to identify the type of information that is missing from the data already collected yet necessary to obtain before a comprehensive analysis and assessment can be completed. It can focus a collection effort for the missing information. A copy of the guide can be obtained from the National Criminal Intelligence Resource Center at www.ncirc.gov.
Issues and Events

Two other types of threat assessments include those that are related to issues—such as the topic of gangs, narcotics, or some other type of general criminal activity—and those that are related to events, such as national conventions and international conferences, which attract groups and individuals bent on committing crimes involving violence and property destruction.


State and local law enforcement authorities can also ask the U.S. Secret Service for assistance with some event-related assessments. The Secret Service helps plan and implement security designs for certain designated national security events.

People

Assessing threats made or posed by an individual is best left to professional profilers. They are trained to recognize whether an individual is, among many things, a fanatic or an extremist.

Fanatics are usually moved by a frenzy of unreasonable enthusiasm or zeal.

Extremists advocate excessive measures and often hold inordinate views.

“Individuals utter threats for many reasons, only some of which involve intention or capacity to commit a violent act. However, a person can present a grave threat without articulating it. The distinction between making and posing a threat is important:
Some persons who make threats ultimately pose threats.

Many persons who make threats do not pose threats.

Some persons who pose threats never make threats.**

The U.S. Secret Service is charged, among its many responsibilities, with protecting individuals such as the President, Vice President, their families, heads of state, and other designated individuals, with an additional focus on individuals involved in workplace, stalking, domestic, and school-based violence. Its National Threat Assessment Center, [www.secretservice.gov/ntac](http://www.secretservice.gov/ntac), provides state and local law enforcement authorities with access to several threat-related products, including *Protective Intelligence & Threat Assessment Investigations: A Guide for State and Local Law Enforcement Officials*. This guide can help authorities formulate their own processes and protocols for investigating and evaluating individuals who are considered threats to public officials. It also offers information on threat assessment protocols, assassins and assassination behavior, elements of a threat assessment program, key functions of a protective intelligence program, conducting a threat assessment investigation, evaluating a threat assessment case, and managing a protective intelligence case.

Another approach to helping prevent such violence is offered in the National Institute of Justice’s *Threat Assessment: An Approach to Prevent Targeted Violence*. It offers information on investigative techniques, fundamental principles of threat assessment, functions of a threat assessment program, and case management. A copy of this document can be obtained from [www.secretservice.gov](http://www.secretservice.gov).

An example of such violence that may lend itself to state and local law enforcement threat assessments is the FBI’s *The School Shooter: A Threat Assessment Perspective*. It provides information such as the school shooter phenomenon—i.e., what is a threat, motivation, signposts, types of threats, factors in threat assessment, and levels of risk.

---


Participate in the process of preparing threat assessments, especially as they pertain to the protection of this country’s key infrastructure sites and critical assets. Even though most state and local law enforcement authorities are not trained in the process, their involvement in collecting and sharing information that could be crucial to an assessment is still prized.

No matter how hard it may be for some agencies (because of their small size) to become involved in the preparation of threat assessments, it is imperative that all authorities be aware of the need for such information and understand the importance of sharing it. This country relies on state and local law enforcement authorities for much of that information. Without it, threat assessments run the risk of being constructed on partial data, which could lead to prevention efforts being based on unsound reasoning and misleading inferences. That is why threat assessments have a *shelf life* of being only as good as their last review and analysis. Like the intelligence process, assessing threats is a never-ending responsibility.

Finally, it is also imperative to remember that “risk management principles acknowledge that (1) while risk generally cannot be eliminated, it can be reduced by enhancing protection from validated and credible threats; (2) although many threats are possible, some are more likely to occur than others; and (3) all assets are not equally critical.”[^40] Toward that end, it is important to know that “we cannot protect every person in every place at every moment.”[^41] However, someone (unknown) once said that *it is always better to look into the future with imperfect vision than not to have looked at all.*

[^40]: *Combating Terrorism: Threat and Risk Assessments Can Help Prioritize and Target Program Investments*; United States General Accounting Office; April 1998.
RESOURCES

There are many resources to help state and local law enforcement authorities become more involved in the intelligence process and the preparation of threat assessments. Some of the more practical resources are described below.

Information

*National Criminal Intelligence Resource Center*, www.ncirc.gov, on the Regional Information Sharing Systems, Law Enforcement Online, and Homeland Security Information Network secure Web sites, provides a centralized location for seeking criminal intelligence-related standards, policies, and guidelines; contact information for intelligence units and organizations across the country; training standards; and *best practices*. It can also help to facilitate implementation of the *National Criminal Intelligence Sharing Plan*.

Associations

*International Association of Crime Analysts*, www.iaca.net, helps crime analysts around the world make contact with associates, improve their skills, and assist law enforcement departments with making the best use of crime analysis. It has nearly 1,000 members, which include intelligence analysts, crime analysts, and police officers, with approximately 10 percent of the membership from outside the United States. It hosts an annual training conference, has a Web site that provides a variety of analysis-related products, and is linked to other crime analyst associations that also include intelligence analysts such as the California Crime and Intelligence Analyst Association (www.crimeanalyst.org), the Florida Crime and Intelligence Analyst Association (www.fciaa.org), the Texas Association of Crime and Intelligence Analysts (www.tacia.org), and Canada’s Criminal Intelligence Service Alberta (www.cisaberta.ca).

*International Association of Law Enforcement Intelligence Analysts*, www.ialeia.org, promotes the standards of professionalism in law enforcement intelligence analysis by enhancing the general understanding of intelligence analysis. It encourages the recognition of intelligence analysis as a professional endeavor by developing international qualification and competence standards, devising training standards and curricula, and conducting analytic-related research studies. It has over 2,000 members from approximately 645 agencies and 43 countries (September 2004), and it hosts an annual training conference.

*Law Enforcement Intelligence Unit*, www.leiu.org, is composed of state and local police departments divided geographically into four national zones. It has about 250 member agencies, and membership is limited to law enforcement departments having an intelligence function. It also hosts an annual training seminar.

Training

*Foundations of Intelligence Analysis Training*, www.nw3c.org (National White Collar Crime Center), is a five-day course that meets the beginning analytic training standards of the *National Criminal Intelligence Sharing Plan*. The course includes topics on the history and purpose of intelligence analysis; intelligence models and cycle; legal aspects; resources; fundamentals of
creative and critical thinking logic; inference development; and an introduction to a variety of analytical methods and skills that include, but are not limited to, crime pattern, association, flow, strategic, and financial analysis.

*State and Local Anti-Terrorism Training Program, [www.slatt.org](http://www.slatt.org)*, provides specialized terrorism-related intelligence, interdiction, investigation, and prevention training. Training is offered in a variety of formats, such as Investigative/Intelligence Workshops, Specialized Training Events, Tribal Lands Anti-Terrorism Briefings, and Train-the-Trainer Workshops.

*Criminal Intelligence for the Chief Executive Briefing, [www.iir.com/cice](http://www.iir.com/cice)*, is designed for law enforcement executives and focuses on criminal intelligence sharing, the intelligence function, intelligence-led policing, legal and privacy issues, and information regarding available resources and networks. It also includes an overview of the *National Criminal Intelligence Sharing Plan*; Title 28, Code of Federal Regulations, Part 23; and the criminal intelligence process.


*Counter-Terrorism Training and Resources for Law Enforcement, [www.couterterrorismtraining.gov](http://www.couterterrorismtraining.gov)*, serves as a single access point to counterterrorism training opportunities and related materials available from the federal government along with private and nonprofit organizations.

---

**Guideline 20**

Benefit from the many resources available to enhance a state or local law enforcement department’s participation in the intelligence process and the preparation of threat assessments. Participate in professional organizations and support intelligence-related training.
RECOMMENDED READING

There are numerous reports, plans, and guides that state and local law enforcement authorities can use as references regarding terrorism, intelligence, and threat assessments. Some of the more useful documents include the following:

Terrorism


Intelligence

*National Criminal Intelligence Sharing Plan*; U.S. Department of Justice, Office of Justice Programs; October 2003; [www.it.ojp.gov/global](http://www.it.ojp.gov/global).


*Law Enforcement Analytic Standards*; International Association of Law Enforcement Intelligence Analysts; November 2004; [www.ialeia.org](http://www.ialeia.org).


Threat Assessments


**Regulations**


BIOGRAPHY

This handbook was written by Jerry Marynik, who retired in December 2005 after a 35-year career with the California Department of Justice. He spent 30 of those years assigned to the department’s Criminal Intelligence Operations Program. Throughout that time, he managed the California Anti-Terrorism Information Center’s Group Analysis Unit and supervised the department’s Gangs/Criminal Extremists Unit, the California Witness Protection Program, and the Organized Crime Unit.

Mr. Marynik wrote the *Threat Assessment Guide to Evaluating and Analyzing Criminal Extremist Groups*, which is one of the most comprehensive of its kind in the nation. It was drafted especially for use during his State and Local Anti-Terrorism Training (SLATT) Program presentation regarding *The Concept of Threat Assessments*. This guide earned him the 1998 International Association of Law Enforcement Intelligence Analysts award for “the individual who has made the greatest contribution to advancing the state-of-the-art in criminal intelligence analysis.”

Mr. Marynik’s current presentations for the SLATT Program include *The Role of Intelligence*, which includes a description of the criminal intelligence process from a practitioner’s point of view, provides an explanation of why the process is now more important for law enforcement authorities than ever before, and offers a compendium of resources that can serve those authorities as a primer for becoming involved in the process; and *A Practical Guide to Threat Assessments*, which describes the basic reasons why threat assessments are a significant responsibility for every law enforcement authority, provides a foundation for those authorities to collect and analyze criminal-related information when preparing such an assessment, and lists suggested sources where authorities can access timely assessments.

Mr. Marynik, as a member of the Global Intelligence Working Group, assisted in the development of the *National Criminal Intelligence Sharing Plan (2003)*, the *Law Enforcement Analytic Standards (2004)*, and the *Fusion Center Guidelines (2005)*. He has been referenced in other documents, including the U.S. Department of Justice’s *Assessing and Managing the Terrorism Threat* and *Intelligence-Led Policing: The New Intelligence Architecture*. He can be contacted by mail at the Institute for Intergovernmental Research, Post Office Box 12729, Tallahassee, Florida, 32317.