The Law Enforcement Intelligence Function
State, Local, and Tribal Agencies

By DAVID L. CARTER, Ph.D.

Law enforcement intelligence has changed dramatically since the terrorist attacks of September 11, 2001. Fueled by the need for more widespread information sharing and a higher quality of intelligence for counterterrorism, these reforms also have helped law enforcement agencies investigate criminal enterprises and prevent crimes of all types.

With the development of the intelligence-led policing (ILP) philosophy and its operationalization through the National Criminal Intelligence Sharing Plan (NCISP), state, local, and tribal law enforcement organizations have begun to revisit their roles in intelligence processes. Agencies that have intelligence units should reexamine their operating policies and guidelines to ensure consistency with national standards, contemporary laws, and current acceptable practices. Those without such units need to develop some type of intelligence capacity, even if it consists of only one person trained to understand the language, processes, and products available. This individual can serve as the department’s intelligence contact point, as well as the conduit to disseminate information to those who need it.

The foundation of developing an intelligence capacity rests on understanding its role in the overall mission of the organization. ILP serves as the contemporary model for this function. Emerging as a concept following an International Association of Chiefs of Police (IACP) summit on intelligence and information sharing, ILP seeks to provide guidance on operational activities based on
As the community policing philosophy evolved by embracing problem solving and, most recently, Compstat, it became clear that law enforcement agencies could effectively manage crime and disorder in their communities by basing their operations on an analysis of empirically collected data on trends of concern. While analysis (including Compstat) tends to concentrate on street crimes and burglaries within a jurisdiction, ILP focuses on complex, multijurisdictional crime and terrorism. Like community policing, ILP is proactive, giving operational guidance and, hence, using resources more efficiently and effectively. Importantly, ILP provides philosophical integration of intelligence activities within law enforcement operations, rather than being an undefined tangential activity as was too often the case in the past.

Of course, any concept must be translated to practice to have an effect. As a result, the NCISP serves as a blueprint for administrators to promote intelligence sharing while, at the same time, protecting citizens’ constitutional rights. The plan establishes standards for maintaining records, training personnel, developing information-sharing partnerships, and generally enhancing the ability of the law enforcement community to prevent terrorism and organized crime through a robust intelligence capacity.

The emergence of ILP and the NCISP significantly enhanced the law enforcement intelligence function. The challenge now centers on implementing these initiatives in America’s law enforcement agencies, addressing the concerns expressed by citizens on matters of privacy and the expression of free speech, and accomplishing these objectives in a relatively short time frame.

**PURPOSE SERVED**

In the purest sense, intelligence is the product of an analytic process that evaluates information collected from diverse sources, integrates the relevant data into a cohesive package, and produces a conclusion or estimate about a criminal phenomenon by using the scientific approach to problem solving (i.e., analysis). Thus, intelligence, a synergistic product, can provide meaningful and trustworthy direction to law enforcement decision makers about complex unlawful activities, including criminal enterprises and extremists, as well as terrorists.

Essentially, an intelligence function within a law enforcement organization serves two broad purposes. The first involves prevention (tactical intelligence). This includes gaining or developing information related to threats of terrorism or crime and using this information to apprehend offenders, harden targets, or employ strategies that will eliminate or mitigate the threat. The second purpose covers planning and resource allocation (strategic intelligence). The

Dr. Carter teaches at Michigan State University’s School of Criminal Justice in East Lansing.
intelligence function provides information to decision makers about the changing nature, characteristics, and methodologies of threats, as well as emerging threat idiosyncrasies, so they can develop response strategies and reallocate resources as necessary to accomplish effective prevention.

While investigation clearly constitutes part of the information collection process, the intelligence function often is more exploratory and broadly focused than a criminal investigation, per se. For example, a law enforcement department may reasonably suspect that a person or group has the intent, capacity, and resolve to commit a crime or terrorist act. However, evidence may fall short of the probable cause standard, even concerning an arrest for criminal attempt or conspiracy. Moreover, a compelling community safety reason may exist for keeping an inquiry open to identify other criminal offenders, notably leaders, and weapons that they may use.

Because of this broader role, as well as the need to keep information secure and to maintain records on individuals where evidence of criminal involvement is uncertain or tangential, law enforcement agencies must abide by rigid guidelines that protect the constitutional rights of citizens while, at the same time, permitting inquiries to proceed for purposes of community safety. These guidelines also facilitate accurate and secure information sharing because the nature of terrorism and criminal enterprise threats are inherently multijurisdictional. Further, if law enforcement organizations at all strata of government subscribe to the same guidelines, they can increase information sharing because they know that the security and integrity of the records will remain intact.

“Agencies must establish policies with respect to what types of data they will impart and to whom.”

ACCOUNTABILITY FACTOR

Law enforcement agencies must consider many factors in the development of an intelligence function; however, a number of contemporary issues rank as the “first among equals” in today’s environment. Part of the reason lies in a well-publicized history of past abuses of information collection and record keeping. As a result, various watchdog groups and members of the public have begun to scrutinize law enforcement intelligence operations. Moreover, modern police managers insist on careful accountability in the intelligence function because of the responsibility to uphold citizens’ rights, as well as to reduce exposure to liability.

Criminal Predicate

Lessons learned from a legacy of lawsuits against intelligence units dating back to the 1960s clearly demonstrate that departments cannot collect information about individuals and store it in an intelligence records system unless a criminal predicate exists. This often proves more difficult than it may appear. Individuals who support an unpopular cause, have radical beliefs, or express an ideology that undermines America’s founding principles may be distasteful, but these actions fall within their constitutionally protected rights. As such, agencies may not keep intelligence records on them, even ones personally held by unit employees, unless a reasonable suspicion documented in the records system demonstrates that the individuals are involved in criminal activity.

Policies and Procedures

To ensure that intelligence files meet constitutional standards, law enforcement
organizations must establish policies and procedures concerning the collection, assessment, storage, dissemination, and purging of criminal intelligence records. Agencies that receive federal funding for a multijurisdictional intelligence records system must adhere to the federal regulation 28 CFR Part 23, which establishes guidelines for submitting and entering data, securing the system, accessing the system for inquiries, disseminating information, reviewing records, and purging data. While the regulation exempts single-agency and nonfederally funded systems, adhering to the standard remains a sound practice, especially as an affirmative defense in a liability lawsuit related to records keeping.⁶

**Collection Issues**

Permeating both the criminal predicate and records system concerns is the collection and retention of information about people protesting issues in support of positions viewed as extreme that conceivably may result in violence, criminal disorder, or property damage.⁷ In such cases, the existence of a criminal predicate often is unclear. It proves difficult, if not impossible, to determine when members of a demonstration may continue a vocal, yet lawful, protest versus those who commit a criminal act, sometimes out of spontaneity. Often more problematic—for political, rather than legal, reasons—is an undercover officer’s attendance at an open planning meeting of a protest group to identify participants and assess the probability of unlawful actions.

> **Essentially, an intelligence function within a law enforcement organization serves two broad purposes.**

On one hand, collecting information on people in situations where criminal activity is only a possibility may violate their civil rights if no crime occurs and the records remain on file. Conversely, not gathering it may be negligent should community security become compromised if violence or property damage emerges from the event.

Departments should collect information that relates to establishing a criminal predicate, identifying and apprehending criminal law violators, gathering evidence and witnesses to support prosecution, and ensuring that community safety is not compromised. Information about demonstrators may include—

- personal data of each member (e.g., name, age, sex, race, ethnicity, and residence);
- group organization (Is there a parent or national group? How formal is the structure? What are the rules of the organization? What does the organization condone and condemn with respect to demonstrations?);
- the basis of their ideology and what it teaches them;
- their goals and what they want to accomplish, including changes to policy or law, making their cause known, disruption of society, or destruction of enemies;
- their protest style, such as their history, stated plans, and inferences from their informal network; and
- their mood, which can help determine community safety (Are they making or posing threats?).

To best accomplish these goals, law enforcement organizations should have clear procedures and training in place to deal with these issues. The following recommendations are perhaps the most restrictive approach to information collection under these circumstances;
however, they nonetheless present an avenue to afford both the strictest protection of citizens’ rights and the greatest precaution against liability.

- Agencies should have written guidelines and training on specific provisions of substantive law, including elements of the offenses, which may arise from a protest or demonstration.
- They should instruct their personnel to make detailed documentation of observations and actions that support the elements of offenses and to exclude First Amendment expressions and noncriminal statements.
- Supervisors should approve an information collection plan, including each incident wherein meetings are monitored, and review and approve reports. They should purge information that does not support the elements of the offenses or aid as evidence.
- Collection methods should use the least intrusive means available.
- Personnel should purge photographs and video recordings not evidentiary in nature nor supportive of a criminal investigation.
- If a surveillance is based, in part, on the fact that affiliate groups or persons within the group have committed criminal law violations in the past while participating in similar situations, these records should include appropriate documentation.
- The records should fully articulate any compelling community safety issues.

REQUIREMENTS AND PRODUCTS

Law enforcement departments should focus on what they do not know. “The absence of evidence is not the absence of a threat.” Agencies define intelligence requirements to gain these new insights. If they develop new intelligence, they must transmit it in a consumable form to permit personnel—from the executive to the street officer—to make the best decisions about how to deal with the threats.

Intelligence Requirements

In essence, an intelligence requirement seeks to fill a gap with the missing information that a decision maker needs. Defining a requirement is not necessarily an easy process. It involves detecting the potential threats (terrorist or criminal) within the jurisdiction and determining their veracity, as well as identifying potential targets in the area and assessing their vulnerability. Throughout this process, occasions will arise when departments have insufficient information to make judgments, thereby encountering an intelligence requirement. Threats will change over time, obligating agencies to make this process consistent. While the effort may appear laborious, it nonetheless provides the best use of resources because it focuses on true needs, not random or nonessential information.

Law enforcement organizations must report requirements in an easily understood manner that specifically addresses the need they fulfill. Hence, in the planning process, an intelligence unit should define its products, a series of regularly prepared intelligence reports that have a specific format and convey an intended message.

Intelligence Products

To accomplish its goals, the unit should place intelligence and critical information in a format that maximizes the consumption and use of the knowledge. The report should
identify the targeted consumer (e.g., patrol officers, administrators, or task force members), clearly convey the critical information, identify time parameters wherein the intelligence is actionable, and provide recommendations for follow-up.¹⁰

Intelligence products prove most useful when each has a specific purpose; follows a consistent, clear, and aesthetic format; and contains all of the critical information that the consumer needs without superfluous details. The types of products will vary by the character of the department (e.g., state/local, urban/rural, or large/small), as well as the collection and analytic capacity of unit personnel. As a general rule, agencies may need only three specific reports: 1) those that aid in the investigation and apprehension of offenders; 2) ones that provide threat advisories to harden targets; and 3) those that assist with planning and resource allocation.

Without fixed, identifiable intelligence products, departments will waste efforts and share information ineffectively.

### Operational Intelligence

This information often places law enforcement organizations in a controversial position. For purposes of community safety, agencies need to maintain information on some people and organizations for two reasons: 1) their potential to commit crimes and 2) their

---

**Comparing Compstat and Intelligence-Led Policing**

<table>
<thead>
<tr>
<th>Compstat</th>
<th>Commonalities</th>
<th>Intelligence-Led Policing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single jurisdiction</td>
<td>Each has a goal of prevention</td>
<td>Multijurisdiction</td>
</tr>
<tr>
<td>Incident driven</td>
<td>Each requires</td>
<td>Threat driven</td>
</tr>
<tr>
<td>Street crime and burglary</td>
<td>Organizational flexibility</td>
<td>Criminal enterprises and</td>
</tr>
<tr>
<td>Crime mapping</td>
<td>Consistent information input</td>
<td>terrorism</td>
</tr>
<tr>
<td>Time sensitive (24-hour</td>
<td>A significant analytic component</td>
<td>Commodity flow; trafficking</td>
</tr>
<tr>
<td>feedback and response</td>
<td></td>
<td>and transiting logistics</td>
</tr>
<tr>
<td>Disrupt crime series (e.g.,</td>
<td></td>
<td>Strategic</td>
</tr>
<tr>
<td>burglary ring)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Drives operations</td>
<td></td>
<td>Disrupt enterprises</td>
</tr>
<tr>
<td>Patrol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tactical unit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Investigators</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analysis of offender MOs</td>
<td>Bottom-up driven with respect to</td>
<td>Drives operations</td>
</tr>
<tr>
<td></td>
<td>operational needs</td>
<td>JTTF</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Organized crime investigations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Task forces</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Analysis of enterprise MOs</td>
</tr>
</tbody>
</table>

*Note: Correlated goals and methodologies make both concepts complement each other.*
existence as bona fide threats, although the parameters often prove difficult to specify. Departments monitor and record actions and affiliations of these individuals to help prevent future crimes or to build a criminal case later. Inherently problematic is the idea of a future offense. What is the rationale for keeping information on a person or group who has not committed a crime, but might? Essentially, if a compelling interest for community safety exists, law enforcement administrators can make an effective argument to maintain records on individuals who threaten that safety as long as they can present reasonable justification to show a relationship to criminality.

In this type of intelligence, a unit creates no product, per se, but, instead, develops regularly prepared and disseminated operational records on people and groups who pose threats. Departments must maintain an important, yet difficult, balance: ensuring that no violation of constitutional rights occurred during the course of the process while, at the same time, compiling a resource of credible information for legitimate law enforcement purposes.

**DISSEMINATION PROCESS**

Obviously, dissemination represents the heart of information sharing. Agencies must establish policies with respect to what types of data they will impart and to whom. Critical to appropriate dissemination is understanding which persons have the right and the need to know, both within the agency and externally. In some cases, the occasion may arise for multiple versions of one product. For example, a non-sensitive public edition of a report could advise citizens of possible threats, whereas another would provide more details to law enforcement personnel.

> **Without fixed, identifiable intelligence products, departments will waste efforts and share information ineffectively.**

With dissemination of sensitive material, a department should impose the third-agency rule, which means that any recipient of intelligence cannot share the information with another organization. This affords some degree of control and accountability, yet allows the originating department to waive the rule when appropriate.

Clearly, electronic networking provides the most efficient way to share information. With availability of secure e-mail systems, as well as Intranets in growing numbers of agencies, dissemination has become faster and easier. The caveat, however, is to ensure that the intelligence products contain essential information and reach the correct consumer. If reports deluge law enforcement officers, the overload will have the same outcome as not sharing information at all. That is, if officers delete intelligence products without reading them, then the effect becomes the same as not disseminating them in the first place.

**STANDARDS AND INITIATIVES**

To create the most professional and effective intelligence function, law enforcement executives should consider adopting a number of standards and initiatives. While most are not required, they nonetheless contribute to the efficacy of intelligence operations while concomitantly protecting civil rights and reducing liability.

- The philosophy of intelligence-led policing
- The tenets and standards of the Global Justice Information Sharing Initiative
- The standards of the National Criminal Intelligence Sharing Plan
• The guidelines for information and intelligence sharing of the Office of Domestic Preparedness Guidelines for Homeland Security

• The guidelines of the Commission on Accreditation for Law Enforcement Agencies (CALEA) Standard 51.1.1 Criminal Intelligence

• The provisions of the International Association of Chiefs of Police (IACP) Model Criminal Intelligence Policy

• The standards of the Law Enforcement Intelligence Bureau (LEIU) Criminal Intelligence File Guidelines

• The IACP Code of Ethics or an agency-developed articulated code of ethics

• The IACP Code of Conduct or an agency-created articulated code of conduct

• An agency-produced articulated statement of values

• The regulations of 28 CFR Part 23 for its criminal intelligence records system

• The tenets of the Justice Information Privacy Guidelines

• The tenets for information system security defined in the Applying Security Practices to Justice Information Sharing Report

• Defined activities designed exclusively to prevent and control crime with no political, religious, or doctrinal purpose

An intelligence unit does not need to incorporate all of these factors verbatim. Rather, adherence to the spirit of the standards as an overarching philosophy that is operationalized via policy and procedures in a manner consistent with local law will suffice.

Officials responsible for any aspect of law enforcement operations must understand current intelligence initiatives as they become part of the fabric of the overall security of this country. Recognizing the importance of a robust intelligence capacity can help agencies work together to share information and fulfill their mission as society’s protectors.

Endnotes
4. In the context of law enforcement intelligence, investigation is the pursuit of data based on leads and evidence associated with a particularly defined act to identify and apprehend offenders for prosecution. Information collection is the capture of data based on a reasonable suspicion of criminal involvement for use in developing cases, identifying crime trends, and protecting the community by means of intervention, apprehension, or target hardening.
5. This includes information in an intelligence temporary file, as well as noncriminal identifying information as defined in 28 CFR Part 23.
6. The File Guidelines prepared by the Law Enforcement Intelligence Unit (LEIU) may provide the best model for translating this regulation to policy and procedures. The provisions of this model have

"In essence, an intelligence requirement seeks to fill a gap with the missing information that a decision maker needs.

CONCLUSION
The terrorist attacks of September 11, 2001, brought the intelligence function of the law enforcement community to the forefront. Increased awareness of the need for compiling essential information on those who threaten the safety of all Americans has changed the profession’s role from solely fighting crime and disorder to include combating terrorism.
withstood the test of challenges and are comprehensive in nature. See http://

7 An extremist ideology is one in which
a commonly accepted set of core beliefs
are interpreted and often applied in a
frequently literal manner, rather than a
spiritual one, and embodies attitudes and
values considered unreasonable and
unacceptable to conventional doctrine.

8 From a presentation by FBI Executive
Assistant Director Maureen Baginski at
the Police Executive Research Forum
Conference on Intelligence, Washington,

9 From a presentation by FBI Executive
Assistant Director Maureen Baginski at the
Major City Chiefs Intelligence Command-
ers Conference, Washington, DC, April 6,
2004.

10 For example, follow-up instructions
may direct a patrol officer to complete a
field interview card, notify a special unit,
conduct surveillance of the target, or take
safety precautions.

11 Agencies must make distinctions
between people who make threats and
those who pose them. A person may pose
a threat without making one and vice
versa. This represents an intelligence
requirement.

12 Supra note 1.

http://it.ojp.gov/topic.jsp?topic_id=8

13 http://it.ojp.gov/topic.jsp?topic_id=93

14 http://www.ojp.usdoj.gov/odp/docs/
ODPRev1.pdf

15 http://www.calea.org/newweb/
accreditation%20Info/descriptions_of
standards_approv.htm

16 http://it.ojp.gov/process_links.jsp?
link_id=3774

17 http://it.ojp.gov/process_links.jsp?
link_id=3773

18 http://www.theiACP.org/documents/
index.cfm?fuseaction=document&document_type_
id=1&document_id=95

19 http://www.theiACP.org/documents/
index.cfm?fuseaction=document&document_
type_id=1&document_id=94

20 For one example, see the Santa Clara,
California, Police Department’s Value
Statements at http://www.scpd.org/
value_statement.html.

21 http://www.iir.com/28cfr/
22 http://www.ncja.org/pdf/
privacyguideline.pdf

23 http://it.ojp.gov/documents/asp/

Subscribe Now

Credit card orders are welcome!
Fax orders: (202) 512-2250
Phone orders: (202) 512-1800
Online orders: bookstore.gpo.gov

(FBIEB) at $36 each ($45 foreign) per year.
Price includes regular shipping & handling and is subject to change.

Check method of payment:

☐ Check payable to: Superintendent of Documents
☐ GPO Deposit Account[ ]
☐ VISA☐ MasterCard☐ Discover

[ ] Card number
[ ] expiration date
[ ] security code

Authorizing signature 1/2001

Mail to: Superintendent of Documents, PO Box 371954, Pittsburgh PA 15250-7954

Important: Please include this completed order form with your remittance.

Thank you for your order!