United States
Department of Justice

International Association of
Law Enforcement Intelligence
Analysts, Inc.

Law Enforcement Analytic Standards

November 2004

About Global

The U.S. Department of Justice's Global Justice Information Sharing Initiative (Global) serves as a Federal Advisory Committee to the U.S. Attorney General on critical justice information sharing initiatives. Global promotes standards-based electronic information exchange to provide justice and public safety communities with timely, accurate, complete, and accessible information in a secure and trusted environment. Global is administered by the U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance.

BJA

This document was prepared under the leadership, guidance, and funding of the Bureau of Justice Assistance (BJA), Office of Justice Programs, U.S. Department of Justice, in collaboration with the U.S. Department of Justice's Global Justice Information Sharing Initiative. The opinions, findings, and conclusions or recommendations expressed in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

Law Enforcement Analytic Standards

Global Justice Information Sharing Initiative

International Association of Law Enforcement Intelligence Analysts, Inc.

November 2004

Acknowledgements Page

Analytic Standards Committee:
Marilyn B. Peterson, C.C.A., chair and author, New Jersey Division of Criminal Justice; Ritchie A. Martinez, C.C.A., Arizona Department of Public Safety; Lisa M. Palmieri, C.C.A., Massachusetts State Police; Russell Porter, C.C.A., Iowa Department of Public Safety; Howard Atkin, C.C.A., West Yorkshire, England, Constabulary; David Jimenez, C.C.A., U.S. Border Patrol; David Lodge, Central Intelligence Agency; Robert Fahlman, C.C.A., Criminal Intelligence Service Canada; Edward Petersen, National Drug Intelligence Center; Ledra Brady, U.S. Drug Enforcement Administration; William Deyermond, New England State Police Information Network®; Jerry Marynik, California Department of Justice; Peter Modafferi, Rockland County, New York, District Attorney's Office; Scott Keay, Lancashire, England, Constabulary; Patty Dobbs, Institute for Intergovernmental Research®; and Karin-Anne Duncan, consultant.

IALEIA, Post Office Box 13857, Richmond, VA 23225

Table of Contents

History of the Standards

The Global Justice Information Sharing Initiative (Global) Intelligence Working Group (GIWG) requested the International Association of Law Enforcement Intelligence Analysts (IALEIA) to develop analyst standards on its behalf as stated in the *National Criminal Intelligence Sharing Plan* (NCISP). The charge was:

"Recommendation 12: The IALEIA should develop, on behalf of the Criminal Intelligence Coordinating Council (CICC), minimum standards for intelligence analysis to ensure intelligence products are accurate, timely, factual, and relevant and recommend implementing policy and/or action(s). These minimum standards should be developed by June 30, 2004. Law enforcement agencies should adopt these standards as soon as developed and approved by the CICC."

Discussion: The role of analysis in a law enforcement agency is to support the investigative, planning, and intelligence activities of the agency. Thus, the work that is performed by an intelligence function should reflect the priorities and goals of the specific agency or organization. There is a range of analytic products that results from a careful and thorough review of varied documents, and the types and formats of intelligence products also vary (e.g., working reports, analytic reports, assessments, or reports of raw data). Regardless of the format, intelligence products must be accurate, timely, and factual. "Reports are the very lifeblood of the intelligence process," and "intelligence reporting is the basis most often used for judging the value of a police intelligence unit." (Parks and Peterson 2001:121-133) "Therefore, it is critical that reports are done and that they are done well." (NCISP 2003:14-15)

IALEIA initiated its development of these standards by holding a workshop at the International Association of Chiefs of Police (IACP) Annual Conference in Philadelphia, Pennsylvania, in October 2003. This workshop was attended by about 40 individuals who included IALEIA members and other law enforcement managers interested in intelligence. IALEIA President Ritchie A. Martinez and CICC member Russell Porter conducted this workshop and received input from those assembled. For many, it was their first look at the NCISP and their first thoughts about developing analytic standards.

IALEIA went out to its membership in January 2004 through its *Intelscope* magazine, asking for input. Volunteers for the standards committee were sought, and several people from the United States, Canada, and the United Kingdom responded. A "strawman" set of standards was developed to generate discussion and encourage feedback. A meeting was established to occur in concert with the April 1-2, 2004, meeting of the GIWG to bring together people to discuss the "strawman" standards. Representatives from the U.S. Drug Enforcement Administration (DEA), National Drug Intelligence Center (NDIC), Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), IACP, and several local and state agencies were invited to attend. The reworked standards were also given to the GIWG at that meeting, and input from the Standards/Policy Committee was requested.

Later in April, the IALEIA annual conference was held in Sacramento, California, and two workshops were held on the standards. Approximately 100 people attended and gave informal comments on the draft. They were also invited to further review the standards and e-mail their comments, and some did.

The tenth draft version of the standards was approved by the IALEIA Board in June 2004 and forwarded to the GIWG. It was distributed to both the GIWG and the CICC for comments and suggestions. Suggested changes were then forwarded back to IALEIA. The CICC reviewed the standards on August 19 and made suggestions for additional changes. These were incorporated into the draft, and the standards were approved by the CICC, on behalf of the whole GIWG. The GIWG then forwarded the approved standards to the Global Advisory Committee (GAC) at its September 28, 2004, meeting. The GAC approved and endorsed the standards.

Law Enforcement Analytic Standards[1]

Preface

The *National Criminal Intelligence Sharing Plan* (NCISP) recommended that all agencies adopt the minimum standards for intelligence-led policing to support the development of sound, professional, analytical products (intelligence). The IACP previously directed that "the intelligence function shall establish and maintain a process to ensure that all information (raw data) gathered is subjected to review and analysis to derive its meaning and value . . . where possible this should be accomplished by professional, trained analysts."

Analyzed raw data (i.e., intelligence) should be used to direct and support law enforcement operations, and that analysis should be an integral part of every complex investigation. We realize, however, that not all agencies are able to hire, train, and maintain a cadre of civilian criminal analysts, and in some agencies, sworn officers must be trained so that the analytic function can be accomplished. Thus, where "analysts" are mentioned in these standards, this may also refer to sworn personnel filling the analytic role.

In general, the role of law enforcement intelligence is to help agencies reduce crime patterns and trends. The intended result of law enforcement is to lower crime rates, whether through apprehension, suppression, deterrence, or reduced opportunity. 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. Analysts work as team members with police officers and other staff members. For these critical reasons, every agency should have some analytic capability.

Law enforcement intelligence programs should produce both strategic and tactical products to support the mission and priorities of the agency.

[1] This document is not intended to create, does not create, and may not be relied upon to create any rights, substantive or procedural, enforceable at law by any party in any matter, civil or criminal.

Intelligence personnel should also maintain, on behalf of the agency, appropriate liaison with local, state, and federal law enforcement agencies. Intelligence units should not be used as file units, nor should analysts be used as data entry, administrative, or clerical personnel. The *General Counterdrug Intelligence Plan* noted, "Professionalizing the intelligence analytic cadre . . . requires that intelligence analysts will no longer perform data-entry tasks and other non-analytic-related tasks such as technical or graphics support . . . ." (Counter Narcotics Council 2000:51)

Listed herein are the standards for law enforcement analysts and analysis, based on the intelligence process or cycle.

Standards for Analysts

The first seven standards relate to analysts or those who fill the analytic function in agencies. The mission of the intelligence analyst, as described in the NCISP, is to research and analyze raw data, apply critical thinking and logic skills to develop sound conclusions and recommendations, and provide actionable intelligence in a cohesive and clear manner to management. (NCISP 2003:38)

#1. Education Standard

> ***Analysts hired should have four-year college degrees or commensurate experience. Commensurate experience is defined as no less than five years of previous research/analysis/intelligence-oriented experience with a two-year degree, or no less than ten years of previous research/analysis/intelligence-oriented experience with less than a two-year degree. This experience can come from the private, public, or military sector. The experience can be documented through job descriptions and/or examples of work products. Appropriate college degree areas include those with research and writing components, including social sciences, English, journalism, and criminal justice. The areas may also include business or science degrees if the knowledge gained will assist in the types of analysis needed to be completed.***

Analysts who have four-year degrees are best suited for their positions because they already have some experience in research and writing, and they may have been exposed to courses including statistics, sociology, anthropology, psychology, political science, computer software and hardware, history, or public speaking. Their qualifications allow them to be viewed by the agency's management and investigative staff as professionals.

Alternately, if they have five to ten years of professional experience in law enforcement and a two-year college degree or no degree, their past

work product and knowledge should allow them to be considered a novice analyst.

"Professional experience" in law enforcement could be experience as an investigator, a paralegal, a technical assistant, or a data analyst. It is counterproductive to promote a clerical staff member into an analytic position who has no college and no commensurate professional experience. Not only will the recipient of the analytic job be frustrated and not able to perform appropriately, but often the investigative staff will not accept this person as an analyst, and thus the person continues to fill a more clerical position while having the job title of analyst. This undermines the intelligence function and the proper use of analysts in the agency.

Educational requirements are also seen in the certification process. One international certifying body, the Society of Certified Criminal Analysts (SCCA), requires a college degree plus ten years of analytic experience for lifetime certification and two years of college and two years of analytic experience for regular certification.

#2. Training Standard

Initial analytic training shall be a minimum of 40 hours and shall be provided by instructors with law enforcement analytic experience. Training shall incorporate, but not necessarily be limited to, the following topics:[2]

- ***Intelligence cycle/process***
- ***Intelligence-led policing***
- ***NCISP***
- ***File management***
- ***Information evaluation***
- ***Critical thinking***
- ***Logic***
- ***Inference and recommendation development***
- ***Collection plans***

[2] The topics named are taken from the NCISP Intelligence Training Standards, page 39, with the exception of professionalism, court testimony, and presentation skills, which were added after discussion.

- ***Research methods and sources***
- ***Crime-pattern analysis***
- ***Association/network analysis***
- ***Telephone record analysis/communication analysis***
- ***Flow analysis***
- ***Spatial/geographic analysis***
- ***Financial analysis***
- ***Strategic analysis***
- ***Analytic writing***
- ***Presentation skills***
- ***Statistics***
- ***Graphical techniques***
- ***Computerized programs to assist analysis***
- ***Ethics***
- ***Professionalism***
- ***Court testimony***

The above standards describe the possible content of a 40-hour course. While a number of topics are listed, it is understood that many might be taught as awareness blocks only and not in depth. Advanced courses taught might expand upon one or more topics taught in a basic course.

The NCISP included a training recommendation (#18) that states: "Training should be provided to all levels of law enforcement personnel involved in the criminal intelligence process. The training standards, as contained within the *National Criminal Intelligence Sharing Plan*, shall be considered the minimum training standards for all affected personnel." (NCISP 2003:17)

Basic analytic training has been available since the 1970s through Anacapa Sciences, Inc., and other agencies, but the level of that training available has not always advanced to match the advancement of analytic methods.

Over the past 30 years, the training that analysts and officers who perform analysis have received has ranged from a few days to a few months, depending on the provider of the training. As a result, the level of understanding of analytic techniques among those individuals has been somewhat uncoordinated.

The lack of generally accepted standards for analytic instructors has made it difficult to assess their qualifications when choosing a training course.

As stated in the NCISP, the core training objectives of an introductory analytic course should be:

I. Intelligence analysts will understand the criminal intelligence process, intelligence-led policing, and their roles in enhancing public safety.
II. Analysts will understand the importance of the *National Criminal Intelligence Sharing Plan* and the role it plays in reducing crime and violence throughout the country.
III. Analysts will gain an understanding of the proper handling of criminal intelligence information, including file management and information evaluation.
IV. Analysts will experience the development of intelligence through the processes of critical thinking, logic, inference development, and recommendation development.
V. Analysts will understand the tasks of building and implementing collection and analytic plans.
VI. Analysts will be familiar with the legal, privacy, and ethical issues relating to intelligence.
VII. Analysts will be provided with information on research methods and sources, including the Internet, information sharing systems, networks, centers, commercial and public databases, and other sources of information.
VIII. Analysts will demonstrate a practical knowledge of the methods and techniques employed in analysis, including but not limited to crime-pattern analysis, association analysis, telephone record analysis, flow analysis, spatial analysis, financial analysis, and strategic analysis.
IX. Analysts will be familiar with the skills underlying analytic methods, including report writing, statistics, and graphic techniques.
X. Analysts will be familiar with available computer programs that support intelligence functions, including database, data/text mining, visualization, and mapping software. (NCISP 2003:39)

There was some discussion regarding the difficulty in managing all the topics into a 40-hour block. One schedule of the topics could be:

Day One

1. Introduction (intelligence cycle, intelligence-led policing, and the NCISP) (2 hours)
2. Information Management (file management, information evaluation, and collection plans) (2 hours)
3. Research Methods and Sources (2 hours)
4. Critical Thinking (1 hour)
5. Logic (1 hour)

Day Two

6. Inference and Recommendations Development (2 hours)
7. Crime-Pattern Analysis (CPA, statistics, and geographic analysis) (4 hours)
8. Association Analysis (2 hours)

Day Three

9. Telephone/Communication Analysis (3 hours)
10. Flow Analysis (2 hours)
11. Financial Analysis (3 hours)

Day Four

12. Strategic Analysis (2 hours)
13. Analytic Writing (2 hours)
14. Legal/Ethics (2 hours)
15. Professionalism (1 hour)
16. Review of Analytic Software (1 hour)

Day Five

17. Presentation Skills (3 hours)
18. Practical Exercise (3 hours)
19. Courtroom Testimony (2 hours)

It should also be noted that these analytic standards should be incorporated into all analytic training.

#3. Continuing Education Standard

> ***Continuing analytic education of at least eight hours per year shall be received by those performing the analytic function, to be accomplished through a combination of formal education, training classes, distance learning, or self-directed study efforts. The training provider should have professional association or academic credentials in the subject matter. Continuing education may include topics as listed in Analytic Standard #2.***

Most professions have continuing education standards that their members are required to achieve to keep up to date and maintain their status in their field. In 2000, IALEIA adopted the standard of 12 hours per year for continuing analytic education. Professional organizations for fraud examiners and public accountants require 20 hours of continuing education per year.

It is important to note that this training can be on analytic-related topics (such as computer software), various law enforcement topics (different types of crime groups, criminal law, etc.), supervision and management topics, or expansions of the topics from the previous list for basic analytic training.

Typically, this training is provided through attendance at professional seminars or conferences or through training courses given by agencies or private vendors. This training should meet general continuing education standards and should require student sign-in and record-keeping.

It is to be hoped that having this requirement will not only further train analysts but will also encourage organizations and agencies to develop advanced analytic training. Without a potential audience, training is seldom created.

#4. Professional Development Standard

> ***Analysts shall maintain a program of professional development throughout their career and be supported in this process by their employer. Employers should ensure that analysts provide maximum benefit to operations by implementing professional development programs for their analytic staff, whether analysts or sworn officers are performing the intelligence duties.***

Analysts are, or should be, by nature lifelong learners. The analytic approach to data is to see what we can learn from it—what it means. This approach to education gives individuals an ongoing commitment to broadening their knowledge and applying it to new assignments.

In 2002, IALEIA published the *Continuing Professional Development Workbook*, created by Inspector Howard Atkin of the West Yorkshire, England, Constabulary. This *Workbook* encourages members to document their learning and experiences to show their growth and development over their careers. It also encourages them to seek out new experiences to add to their knowledge base. All members of IALEIA were provided copies of the *Workbook*; additionally, it was translated into Spanish by IALEIA's Mexico chapter.

Professional development is not just training or gaining new experiences but also being recognized within the agency for the attainment of proficiency levels. The *General Counterdrug Intelligence Plan* (GCIP) of 2000 highlighted the need for career paths and career development for analysts to allow them to move into supervisory and management positions. DEA was one of the first agencies to allow intelligence analysts to be promoted to upper-management positions. Given the critical nature of analytic skills to developing policy and making sound decisions, it would seem fitting that analysts should be promoted into agency management as readily as investigators. Their planning, organizing, and communication skills make them adept managers.

#5. Certification Standard

Analysts should be certified by an agency or organization (governmental, professional association, or institution of higher learning) specifically developed for intelligence analysts. These analytic certification programs shall reflect experience, education, training, and proficiency testing.

Within law enforcement, certification is a common requirement. Police officers are certified when they successfully complete their basic, multiweek training course. Attorneys are "certified" when they pass their bar examinations. Certified public accountants and certified fraud examiners, specialists in the financial investigation areas of many police agencies, have met the education, experience, training, and testing requirements.

The need for analyst certification was spelled out in 1980 in the bylaws of the IALEIA. These bylaws called upon IALEIA to "develop qualification standards and indices of competence for the profession." (Article II, Section 2) One of the committees formed by IALEIA was a Standards and Accreditation Committee that was tasked with developing a certification program. For the first decade of IALEIA's existence, the committee was unsuccessful in this goal.

Since 1990, several certification programs have arisen. California has one program managed by the California Department of Justice, and Florida now has its own certification through the Florida Department of Law Enforcement. The SCCA was created in 1990 and offers certification to members of IALEIA who meet educational, training, experience, and testing requirements. Its certification is also open to members of the Australian Institute of Professional Intelligence Officers in Australia. IALEIA voted, in 1996, to recognize SCCA certification rather than develop its own program. The Regional Information Sharing Systems® (RISS) centers have made SCCA certification a requirement for their analysts, and a number of other agencies give bonuses or otherwise encourage their employees to become certified.

Some agencies certify their own analysts. The Royal Canadian Mounted Police has had a program in place for several years. The FBI is planning to certify its analysts.

There are numerous colleges and universities that offer "certificate programs" in intelligence or analysis; completion of the required courses provides a certificate from that educational institution. One certification program in California combines a state college "certificate" with California Department of Justice certification if the candidate meets their criteria. Some colleges have also developed degree programs in intelligence analysis. Among these colleges are Mercyhurst College in Erie, Pennsylvania; the American Military University in Virginia; Michigan State University; Manchester University in the United Kingdom; and St. Joseph's University in Philadelphia, Pennsylvania.

#6. Professional Liaison Standard

> ***Analysts and their organizations shall be encouraged to maintain links to and seek available support from recognized professional bodies and associations.***

This standard ties to NCISP Recommendation #13: "To further enhance professional judgment, especially as it relates to the protection of individuals' privacy and constitutional rights, the NCISP encourages participation in professional criminal intelligence organizations and supports intelligence training for all local, state, tribal, and federal law enforcement personnel."

In most agencies, the value of analysis remains unrecognized, and few people are employed in this endeavor. Many agencies have only a few analysts, and those who are thus employed may be geographically distant from each other. When analysts are supervised by investigators or attorneys and work in a single-analyst environment, they have no one to go to for analytic advice. Analysts need to share documentation and methodologies among analysts; they need to network.

The two primary law enforcement intelligence organizations in the United States are the IALEIA (www.ialeia.org) and the Law Enforcement Intelligence Unit (LEIU) (www.leiu-homepage.org).

One of the benefits of participating in these types of professional organizations includes access to documentation of the latest methodologies and new training as they are developed. Additionally, books, training, and conferences are often discounted for members.

Often, members are willing to share developed intelligence policies, procedures, and other materials with other members. They may have local or regional chapter meetings and provide localized training. Their reach may extend into dozens of countries outside the United States. Many analytic job descriptions require job holders to serve as a liaison to agencies with similar missions; professional association meetings, member listings, and bulletin boards further this objective.

#7. Analytic Attributes Standard

Analysts shall be hired and evaluated based on their work and attributes, including strong:

- ***Subject-matter expertise***
- ***Analytic methodologies***
- ***Customer-service ethics***
- ***Information handling and processing skills***
- ***Communication skills***
- ***Critical-thinking skills***
- ***Computer literacy***
- ***Objectivity and intellectual honesty***

These attributes summarize the comments of several earlier efforts, as shown below.

In the mid-1980s, Dr. Charles Frost wrote that analysts should have (a) a broad range of interests, (b) a developed research ability, (c) helpful previous experience, (d) intellectual curiosity, (e) rapid assimilation of information, (f) keen recall of information, (g) tenacity, (h) willingness and capacity to make judgments, (i) a developed writing ability, (j) skill in oral briefing, (k) initiative and self-direction, (l) effective personal interaction, and (m) disciplined intellectual courage. (Frost 1985:5-8)

The FBI, in 1998, developed a list of “core competencies” for analysts that included analysis, judgment, research, written communication,

oral communication, computer skills, professionalism/liaison, flexibility/adaptability, capacity to learn, initiative/motivation, organizing, planning and prioritizing, knowledge of current events, and coaching skills. (*Intelligence 2000*, 2001:59)

It was noted that generalist analysts should be intelligent, precise, and anxious to exploit generally uncharted waters . . . used to researching complex problems . . . exploiting all available sources . . . and applying logical, deductive techniques . . . to unravel covert criminal activity. (*Intelligence 2000*, 2001:59-60)

These descriptions of analysts' characteristics have a number of common elements. They hold analysts to high standards of both skills and knowledge; good analysts strive to meet these.

Standards for Analytic Products/ Processes

NCISP Recommendation #1 stated that the agency chief executive officer and the manager of intelligence functions should "support the development of sound, professional analytic products (intelligence)." One way to do that is to recommend that products meet substantive criteria.

The following are standards for analysis that correspond to the intelligence cycle. These standards additionally show the critical role that analysis plays in each portion of the intelligence cycle.

#8. Planning Standard

> ***Analysts shall understand the objective of their assignment, define the problem, and plan for the necessary resources. This shall be done through the use of a collection or investigative plan or through intelligence requirements. Specific steps to be taken to complete the assignment, including potential sources of information and a projected timeline, shall be included. The needs of the client (requirements) shall be reflected in the plan.***

"Intelligence up front" is a philosophy in at least one federal agency. Many agencies have found that using intelligence analysts in the beginning of an investigation saves them time, money, and resources. When a problem, requirement, or target is identified, an analyst should be assigned. The analyst will review what is known on the subject and identify what needs to be known. When appropriate, preliminary records checks can be performed for additional data.

From a combination of the information provided and researched, the analyst can develop a collection or investigative plan that will enable the team of investigators and analysts to move forward in obtaining the necessary data to meet the objective of the assignment. In an investigative setting, the package of material that an analyst can provide to the investigator will focus the investigation and save countless hours of less productive labor.

The intelligence cycle both begins and ends with planning. Collection plans may be drawn based on indicators resulting from previous turns of the cycle. The plan of action created through recommendations may contain requirements for further collection that reinitiate the cycle.

#9. Direction Standard

> ***Analysts shall be involved in planning and direction. Law enforcement agencies shall use analytic expertise to develop both short- and long-term investigative priorities and plans. Analytic expertise may also be used to develop intelligence requirements as a driving force to determine investigative priorities and for incorporation into investigative plans to drive operations.***

The concept of intelligence-led policing is, in effect, analyst-directed policing, since analysts produce intelligence.

Analytic skills of organizing, critical thinking, and modeling give analysts the ability to see not only what is there and what is needed, but what is missing. This allows them to conceive plans and requirements that will allow the problem and its solution(s) to be viewed clearly.

Analysis can also be integrated into a department's planning efforts. Strategic analysis identifies significant crime problems and recommends actions to reduce or prevent crime that should become part of the agency's strategic plan.

#10. Collection Standard

> ***Analytic research shall be thorough and use all available sources. An analytic product shall contain all relevant data available through sources and means available to the analyst.***

In the past, analysts have often been dependent solely upon the information they were provided by detectives or investigators. This information was generally from investigative reports, the results of interviews, surveillances, informant data, and the like. The information may or may not have been accurate, depending on the source.

Analysts also were used in components of an investigation, as opposed to being an asset to the entire process. For example, the most common form of analysis for decades was telephone record analysis. This was done regularly to assist investigations but was a piecemeal approach to analysis in investigations. The analyst would review and report on these records in a vacuum, not knowing the importance of the contacts or the surveillance results to determine who was at the location of a phone at a particular time.

Today, analysts have access to a wealth of information through the Internet and elsewhere. They may find information there that can further identify an individual, provide photographs of a suspect, give information on the location and purchase price of his residence, show where he works and what organizations he belongs to, show where he went to school, etc.

Open source reports on criminal groups can be done through the Internet as well. Many agencies post their past intelligence reports there, including the DEA, and background research can be done without leaving the office.

#11. Collection Follow-Up Standard

In the course of collection by investigators and others, analysts shall evaluate the progress of the collection to determine if the collection plan/requirements are being met and shall identify additional sources of information, as well as identify information that may be useful to other cases or activities. Where possible, analysts shall relay that information to an appropriate body for follow-up.

Today's information explosion makes analysts' jobs exponentially more complex while providing more of a likelihood that information to prove or disprove the crime may be found. Their information management role does not end with the creation of a collection plan or the identification of requirements. The initial collection or investigative plan may need to be updated and expanded to include new sources of potential information that are uncovered.

When a task is set before an analyst, the investigators or managers proposing the task may not be aware of its complexities or ramifications. The analyst knows the requirements and planning functions, what is needed and, most often, where to find it. Through networking, self-study, and discovery, they know what sources will provide them with what data.

As information is collected by the investigator or analyst, the collection plan needs to be checked to see what progress is being made. The time needed to garner certain types of information (such as bank records) may be greater than expected. If activity crosses international borders, information retrieval may also be slowed. The analyst needs to work with the investigative manager to note these difficulties and plan to surmount them. As productive paths end, decisions must be made to try other paths or work with what has been received.

In some instances, there are many leads in an investigation that may appear important to follow up. However, the investigative objective must be recalled and the leads that are not needed to support that objective must be set aside for possible future investigation. Keeping the focus

of the investigation is of critical importance, and analysts can assist in retaining that focus.

#12. Legal Constraints Standard

> ***Raw data that has been obtained in violation of any applicable local, state, or federal law or ordinance shall not be incorporated into an analytic product.***

This prohibition is based not only in best practice but also in the 28 Code of Federal Regulations (CFR) Part 23, which states:

> "A project shall not include in any criminal intelligence system information which has been obtained in violation of any applicable federal, state, or local law or ordinance . . . ."

Discussion on this point ensued during the standard-setting project. Some analysts said they might not know something had been collected illegally because it was provided to them by an investigator or another source, and thus, they might unwittingly include something that had been collected illegally in their analysis. One safeguard against this is the evaluation standard also found in 28 CFR Part 23 and in Standard #13. These levels of reliability and validity placed on reports or other data alert the analyst to possible inappropriate sources or weak data. Data from questionable sources should be treated carefully and noted as such in analytic reports.

It is important to note that there may be laws or regulations on intelligence at the state or municipal level, and the data that is collected from that area must be in compliance with the laws there.

#13. Evaluation Standard

> ***Information collected from all sources shall be evaluated and designated for source reliability, content validity, and relevancy. Effective evaluation is important not only to the validity of the intelligence product but also to officer safety, investigative effectiveness, and solidity of evidence in prosecutions.***

This standard is based in the 28 CFR Part 23.20 Operating principles, Section g, which states, "Information shall be labeled to indicate levels of sensitivity, levels of confidence, and the identity of submitting agencies and officers." The "levels of confidence" relate to reliability, validity, and relevancy.

Standard law enforcement data reliability gradients may go from "reliable" to "usually reliable" to "sometimes reliable" to "unreliable" to "reliability unknown," graded from A through E. Data in the last two categories would be considered questionable and would not be shared with others.

Standard law enforcement data validity gradients may go from "confirmed" to "probably true" to "possibly true" to "doubtful" to "cannot be judged." Again, data marked in the last two categories would be held for further corroboration but not disseminated.

The relevance standard includes no official gradients; either something is tied (or suspected to be tied) to criminal activity, in which case it is relevant, or it is not.

Sensitivity levels relate to the need to keep secret the information held. In law enforcement, gradients now used include "law enforcement sensitive," "sensitive but unclassified," "for official use only," "confidential," and "open source."

#14. Collation Standard

> ***Raw data shall be organized and formatted so the analyst can retrieve; sort; identify patterns, anomalies, and information gaps; and store the data. When possible, this shall be done in a computerized format using the most appropriate software available to the analyst.***

Information, once collected, must be organized logically and clearly. Analysis is often done on information that is diverse in nature; some data may be incident information, financial records, telephone call records, or surveillance reports. All these different forms of data may not be served by the same format or database. Nonetheless, it is most helpful to the analyst

if they all can be in similar formats so they can be compared and patterns can be ascertained.

Uncollated data is not helpful to an investigation or study. If data sits in boxes or files for months without any attention to their contents or organization, both evidence and exculpatory information may be present but not found. An inventory of the data is the quickest way to see gaps in the documents provided and identify further collection efforts that are needed.

A variety of software is available to assist the analyst in collating the data. Some of those are listed under Standard #16.

#15. Analytic Accuracy Standard

> ***An analytic product shall be an accurate representation of the data. In cases where exculpatory data has been found along with proofs, both should be included.***

While this standard seems to be a "given" in many situations, it is, nonetheless, important to be stated here. Analytic products (i.e., intelligence) can only be as accurate as the data that has been provided to create them. When the data is collected and reported by investigators to the analysts, it is critical that it be as correct as possible.

Inevitably, some data is not accurate. Letters are transposed in data entry, misinformation is passed on by informants or others, and data with errors is passed from agency to agency. When the analyst is suspicious of the veracity of the data that has been provided, that should be noted. Some of this may be handled through the evaluation process.

It is the duty of the analyst to verify computerized data (or have it verified) before treating it as accurate. If multiple versions of a name or spelling are given, the analyst should note the variances, while choosing the most likely to be accurate.

Likewise, it is important to note information that is in conflict with the hypothesis as well as that data which supports it. The best scenario is an analyst's having few to no preconceived ideas about what occurred but

letting the data tell what has occurred. The presence of exculpatory data may be critical to the decision-making process. Noting this information also allows the analyst to play "devil's advocate" to view the occurrences from the target's or defendant's point of view.

#16. Computerized Analysis Standard

Analyses shall utilize the best and most current computerized visualization and analytic tools available to the analyst.

There is a wide range of software available to support analysis. This software generally falls into five categories: databases, spreadsheets, visualization, mapping, and text/data mining.

Database software either has established fields or allows the user to develop fields. The former most often is proprietary software that has been designed to serve a specific purpose; the latter is most often Commercial Off-The-Shelf (COTS) software that the user can use to create a particular database. Some of the proprietary databases include Memex's Intelligence Manager, i2's iBase, PenLink, In-Tel-All, etc. Some of these, however, allow an administrator to add fields to customize the application. COTS software includes Microsoft Access, which may be the most commonly used database in law enforcement today. SQL Server and Oracle are also used.

Spreadsheet software most often organizes and displays financial data. There are some standard financial software packages that are used in specific fields (banking, auditing, etc.) or for personal use (checkbook programs), but there is not widespread use of these in law enforcement. Shelf spreadsheets include Microsoft Excel, Lotus 123 for Windows, and Corel QuatroPro. One benefit of using "shelf" software is that the data can easily be transferred from one type of software to another (e.g., database to spreadsheet and back).

Visualization software assists the analyst in producing charts, making changes as new information is known, often without having to completely redo the chart. Visualization software includes i2's Analyst's Notebook, Xanalys' Watson, and Visual Analytics' VisuaLinks.

Mapping software has become very popular in the last decade and is not just used to look at street crimes but can be used at the regional, county, or state level to look at criminal activity. The two most well-known mapping programs are ArcView/Environmental Systems Research Institute (ESRI) and MapInfo.

Text and data mining have opened many new doors to analysts because of the ability of these programs to review and cull multiple sources (databases) and bring in all relevant data for further analysis. Examples of text mining software include i2's iBridge, Memex's Intelligence Analyst, and Visual Analytics' Digital Information Gateway (DIG).

The agency's ability to purchase proprietary software varies from place to place. In some instances, the most advanced software available may be the Microsoft Office Professional package. In other agencies, tens of thousands (or even hundreds of thousands) of dollars may be spent on providing all analysts with specialized software. Some smaller agencies gain access to more expensive software solutions through working with regional organizations that have the software and can provide visuals for them.

#17. Analytic Product Content Standard

> ***Analytic products shall always include analysis, assessments, integrated data, judgments, conclusions, and recommendations. Forecasts, estimates, and models shall be developed, where appropriate.***

It is important to note that intelligence is not produced without a thorough analysis of the data at hand. In some agencies, analysts are asked to review data and enter important parts of the data into a computer and then hand the report to an investigator or manager. This is not analysis and is best done by a data-entry specialist under the guidance of an analyst.

Likewise, analysts are sometimes asked to produce a graphic (chart, map, or crime-scene diagram) from a rough version provided by an investigator. These graphics are not analysis in and of themselves. The resulting chart, map, or diagram must be analyzed by a professional to determine what it may say about the crime or the investigation in order for it to be analysis.

Also, investigators may provide only select information to an analyst to have him or her produce a graphic for grand jury or court shortly before the presentation date occurs. This is not effective use of the analytic component. Analysis of all the data should occur before parts are chosen to be represented in a graphic, and the analysis should be an ongoing part of the investigation.

Recommendations are critical in analysis. As Woodrow Wilson noted, "We are not put on this earth to sit still and know; we are put into it to act."

#18. Analytic Outcomes Standard

> ***Analyses shall include alternative scenarios and avoid single-solution outcomes where appropriate, especially when the outcomes could have significant consequences. Analyses shall indicate the most likely hypothesis, but this hypothesis shall be arrived at through the analysis of competing hypotheses. Those hypotheses not chosen shall also be noted.***

The results of analysis are conclusions/hypotheses and recommendations for action. However, it is often the case that there may be multiple hypotheses which could be drawn and multiple recommendations for actions to be taken, dependent upon which hypothesis is the best choice.

Choosing among hypotheses is a difficult task for analysts or management, particularly when not all the facts are known. One accepted technique for determining which hypothesis is best is the analysis of competing hypotheses, as detailed in Richards J. Heuer, Jr.'s book, *The Psychology of Intelligence Analysis*.[3]

The process explained by Heuer leads the analyst to list all known hypotheses and all bits of evidence that may disprove or prove, with the result of eliminating all but the most likely hypothesis.

[3] This book is available for download through the CIA at www.cia.gov/csi/books/19104.

#19. Dissemination Plan Standard

Analysts shall develop a dissemination plan to encourage sharing of the product with applicable agencies. This plan shall indicate the security level of the document. It shall be reviewed and approved by supervisory personnel.

Analytic products may be developed to support internal or multiagency needs and short- or long-term goals. As a result, their dissemination will differ with each product.

The potential audience of a report is most often decided upon before the analysis is done. If the report has been assigned as part of a specific investigation, then the audience would be the investigators and attorneys involved. If it was assigned to inform a wider number of agencies involved in a cooperative effort, then they would form the audience.

There should be a written dissemination plan for the product, even if it is a simple paragraph stating who the audience will be, so that the report is kept within that audience and there are no questions or misunderstandings.

It should also be noted that in the case of some strategic reports, two versions of the report may be done: one with specific recommendations for action to the agency's management and another without those recommendations and/or minus other sensitive information that may be released to a broader set of agencies for informational purposes.

#20. Analytic Report Standard

Reports shall be written clearly and facts documented thoroughly. A precise, analytic bottom line should be provided. A tight, logical organization of facts shall show how the analyst arrived at conclusions. Objective and dispassionate language shall be used, emphasizing brevity and clarity of expression.

Analysts must be accomplished writers. The ability to convey information in a brief, yet comprehensive manner is the hallmark of quality analytic writing. Half the battle of writing is logical organization of facts and

thoughts. Half of the battle in analytic writing is keeping facts separate from opinions. (See also Standard #23.)

Documentation is also very important. Statements may appear factual that may have come from a dubious source. That must be noted so the person arriving at a judgment based on the facts, whether it be the analyst or someone in management, can decide the weight or validity to ascribe to that statement. This is where Standard #13, Evaluation, comes into play.

The analytic process should be transparent to the reader; that is, what facts or findings were collected and how those build to the hypotheses or conclusions.

The facts should be presented in an objective manner, without the opinions of the analysts expressed. When the conclusions are articulated, opinions can be stated.

#21. Analytic Product Format Standard

Analytic product formats shall be tailored to the consumer's need. Products shall include, but are not limited to:

Strategic and tactical assessments
Problem and target profiles
Crime-pattern analysis
Criminal business profiles
Network analysis
Demographic/social trend analysis
Risk analysis
Market profiles
Results analysis
Communication analysis
Flow analysis
Financial analysis
Indicator analysis
Geographic analysis

The definitions of these products are found in the glossary addendum, but it should be noted that analyses are often a collection of subproducts. For example, a network analysis might include an association matrix, a link chart, a chart summary, conclusions, and recommendations, all of which might be defined as "products."

Likewise, a problem profile might include crime-pattern analysis, geographic analysis, demographic and/or social trend analysis, statistical analysis, indicators, conclusions, and recommendations.

As the standard notes, the products included in the analysis should be done in response to the communicated requirements of the consumer, or if the consumer is not aware of what might be provided, the analyst must interpret the consumer's need into the proper products.

#22. Analytic Testimony Standard

> ***Analysts shall be capable of giving testimony as fact/summary and expert witnesses. They shall be able to present and defend their qualifications as witnesses and explain and defend the material they present.***

Part of an analyst's assignment may be creating products for presentation in grand jury or court. In the past, some agencies have taken these products and had them presented by investigators who explained their development and meaning. Many (but not all) agencies have been using analysts to provide these products more recently. This is seen as an effective way to present the material, since analysts have particular training and credentials in analytic methodologies and are viewed as objective.

The standard above suggests that analysts should be capable of presenting materials in grand jury or court. Testifying as a fact/summary witness may only require a recitation of factual materials combined into tables, graphics, or spreadsheets. Testifying as an expert witness requires the analyst to be able to give an educated opinion on a topic relating to the criminal activity on which the prosecution is based.

To support such appearances in court, training in appropriate courtroom behavior should be provided to analysts, including how to respond to *voir dire* examination by the defense attorney and proper ways to respond to cross-examination.

#23. Data Source Attribution Standard

> ***Every intelligence product shall clearly distinguish which contents are public domains or general unclassified information, what information is restricted or classified, and what contents are the judgments or opinions of analysts and/or other professionals.***

This standard, along with Standard #12, refers to the sources and evaluation of data. While Standard #12 reflects the evaluation of data similarly to what is required in intelligence systems, this standard reflects the type of information that might be included in a tactical or strategic assessment.

The need to label the data results from a need to know the level of reliability of the data and the limitations on its sharing. If the data is public domain, the reliability may be less than if it is classified information from another agency. If the data is unclassified, it is important to know whether it is sensitive but unclassified (SBU) or law enforcement sensitive (LES) data, so it can be treated accordingly. Classified information must be kept and shared as appropriate.

It is also important for the analyst to separate his or her opinions from the facts in the case or study. Opinions must be labeled as such and should not be interspersed in the factual portion of the report.

#24. Analytic Feedback Standard

> ***The analytic product shall be reviewed, if appropriate, by peers and evaluated by customers. Peer review may be limited to factual content accuracy or may encompass collaborative comments concerning content and recommendations.***

Analytic products cannot exist in a vacuum, and conclusions may be open to interpretation. It is for this reason that it is important for the products to be aired and viewed by other intelligence professionals who may arrive at different conclusions based on the same facts.

Standard #14 states that opposing points of view and data that does not support the conclusion drawn should be included in the analytic report. So, too, alternate conclusions or recommendations should be noted.

Some federal agencies share intelligence products to check for inaccuracies. While this requires time to be built into the review process, it may be important to include.

Customer evaluation of analytic products is also essential. Some agencies include feedback forms in the disseminated product so recipients can provide comments. It is certain that products that are not sufficient to the customers' needs will not generate support for the intelligence function or further the mission of intelligence. Communication with customers before, during, and after the provision of the intelligence may help to develop better products.

#25. Analytic Product Evaluation

Analytic products shall be evaluated based on the standards set forth in this document.

A missing component to the intelligence function in law enforcement has been the evaluation of its efforts. Traditional policing measures success by arrests and/or convictions. Intelligence is not always created to effect either, and thus, its value has been difficult to quantify.

The charge for creating these standards was "to ensure intelligence products are accurate, timely, factual, and relevant and recommend implementing policy and/or action(s)." (NCISP 2003:14-15) These standards, taken in their totality, speak to all those issues in an attempt to give guidance on ensuring that intelligence products are the best possible.

In 1976, several questions were suggested that could be asked of the analytic product upon its completion. They remain relevant today:

- What other information would I like to have to complete the picture?
- What other information can I get that will be worth the effort?
- Given additional information, do I perceive a new dimension in the problem?
- What is the critical element in the problem?
- Can I match any of the information on hand with the other information in storage to broaden my understanding of the whole problem?
- Assembling all the pieces, can I now reconstruct the problem?
- Do the results present a clearer picture than the one I had before I started the process?
- Can I draw from this new overall picture a significant judgment of some kind?
- How confident am I of my judgment?

Summary/Conclusions

Analytic standards have been present informally for several years, but they have not previously been codified into a single document. It is hoped that by compiling these from the best sources available and disseminating them throughout the law enforcement intelligence community, standards will be more universally accepted and their adherence will be strongly encouraged. As a result, managers will have more trust in analytic judgments and products because they will know the basis for those results.

Addendum – Law Enforcement Intelligence Analysis Definitions

Analytic Writing – Written communication that focuses on distilling and summarizing factual information for the purpose of providing concise and clear reports for managers and other customers.

Analysis – The evaluation of information and its comparison to other information to determine the meaning of the data in reference to a criminal investigation or assessment.

Assessments – Strategic and tactical assessments are completed to assess the impact of a crime group or a criminal activity on a jurisdiction, now or in the future. These may include threat assessments, vulnerability assessments, or risk assessments.

Association Analysis/Network Analysis – Collection and analysis of information that shows relationships among varied individuals suspected of being involved in criminal activity that may provide insight into the criminal operation and which investigative strategies might work best.

Collation – The process whereby information is assembled together and compared critically.

Collection – The directed, focused gathering of information from all available sources.

Collection Plan – A plan that directs the collection of data on a particular topic with a specific objective, a list of potential sources of that data, and an estimated time frame.

Crime-Pattern Analysis – A process that looks for links between crimes and other incidents to reveal similarities and differences that can be used to help predict and prevent future criminal activity.

Criminal Analysis – Criminal analysis is the application of analytical methods and products to raw data that produces intelligence within the criminal justice field.

Criminal Business Profile – A product that details how criminal operations or techniques work, including how victims are chosen, how they are victimized, how proceeds of crime are used, and the strengths and weaknesses in the criminal system.

Criminal Intelligence – Information compiled, analyzed, and/or disseminated in an effort to anticipate, prevent, or monitor criminal activity.

Critical Thinking – The objective, open, and critical cognitive process applied to information to achieve a greater understanding of the data, often through developing and answering questions about the data.

Communication Analysis – See Telephone Record Analysis.

Content Validity – An evaluation scale generally represented from 1 to 5 or 1 to 4 that reflects the level of accuracy of the content of a raw data report. The scale ranges from known to be true to truthfulness unknown.

Customers – Consumers of intelligence products who may be within the agency of the analyst or in other agencies or organizations.

Demographic/Social Trend Analysis – An examination of the nature of demographic changes and their impact on criminality, the community, and law enforcement.

Dissemination – The release of information, usually under certain protocols.

Dissemination Plan – A plan that shows how an intelligence product is to be disseminated, at what security level, and to whom.

Estimate – A numeric forecast of activity based on facts but not able to be verified or known.

Evaluation – An assessment of the reliability of the source and accuracy of the raw data.

Feedback/Reevaluation – A review of the operation of the intelligence process and the value of the output to the consumer.

Financial Analysis – A review and analysis of financial data to ascertain the presence of criminal activity. It can include bank record analysis, net worth analysis, financial profiles, source and application of funds, financial statement analysis, and/or bank secrecy record analysis. It can also show destinations of proceeds of crime and support prosecutions.

Flow Analysis – The review of raw data to determine the sequence of events or interactions that may reflect criminal activity. It can include timelines, event-flow analysis, commodity-flow analysis, and activity-flow analysis. It may show missing actions or events that need further investigation.

Forecast – A look at what has happened or what may happen, based on what is known and verifiable, suspected and not verifiable, and unknown. Likelihoods or probabilities of future activity are usually included, with suggested steps to protect against criminal activity.

Geographic Analysis – A look at the locations of criminal activity or criminals to determine whether future criminal activity can be deterred or interdicted through forecasting activity based on historical raw data.

Hypothesis – A tentative assumption that is to be proven or disproved by further investigation and analysis.

Indicator Analysis – A review of past criminal activity to determine whether certain actions or postures taken can reflect future criminal activity. It can result in the development of "flagging" systems in computerized environments or behavioral profiles.

Intelligence – The product of systematic gathering, evaluation, and synthesis of raw data on individuals or activities suspected of being, or known to be, criminal in nature. Intelligence is information that has been analyzed to determine its meaning and relevance. Information is compiled, analyzed, and/or disseminated in an effort to anticipate, prevent, or monitor criminal activity.

Intelligence Cycle – Consists of planning, collection, collation, evaluation, analysis, dissemination, and feedback.

Intelligence-led Policing – The collection and analysis of information to produce an intelligence end product, designed to inform police decision making at both the tactical and strategic levels.

Market Profile – An assessment that surveys the criminal market around a particular commodity in an area for the purpose of determining how to lessen that market.

Models – Hypothetical sets of facts or circumstances that are developed to test the likelihood of a hypothesis.

Network Analysis – See Association Analysis.

Problem Profile – Identifies established and emerging crimes or incidents for the purpose of preventing or deterring further crime.

Raw Data – Data that is collected by officers or analysts that has not yet been subjected to the intelligence process and thus is not intelligence.

Results Analysis – An assessment of the effectiveness of police strategies and tactics as used to combat a particular crime problem. May include suggestions for changes to future policies and strategies.

Requirements – The details of what a customer needs from the intelligence function.

Risk Analysis/Assessment – Assesses the scale of risks posed by individual offenders or organizations to individual potential victims, the public at large, and law enforcement agencies. Generally includes preventative steps to be taken to lessen the risk.

Source Reliability – A scale that reflects the reliability of information sources; often shown as A–D or A–E. It ranges from factual source to reliability unknown.

Spatial Analysis – See Geographic Analysis.

Strategic Intelligence – Most often related to the structure and movement of organized criminal elements, patterns of criminal activity, criminal trend projections, or projective planning.

Tactical Intelligence – Information regarding a specific criminal event that can be used immediately by operational units to further a criminal investigation, plan tactical operations, and provide for officer safety.

Target Profile – A person- or organization-specific report that provides all that is known on the individual or organization that may be useful as the investigation is initiated. Based on the data, a best course of action regarding the investigation may be recommended.

Telephone Record Analysis/Communication Analysis – The review of records reflecting communications (telephone, e-mail, pager, text messaging, etc.) among entities that may be reflective of criminal associations or activity. It may recommend steps to take to continue or expand the investigation or study.

Threat Assessment – A report that looks at a criminal group or criminal activity and assesses the threat that activity or group poses to a jurisdiction, either at present or in the future, and recommends ways to lessen the threat.

Vulnerability Assessment – A report that looks at an individual, location, or event and assesses the vulnerability of that individual, location, or event to a criminal act and recommends ways to lessen or eliminate the vulnerability.

Sources

Atkin, Howard N., *Continuing Professional Development Workbook and Portfolio*, IALEIA, 2002.

Bureau of Justice Assistance, *Criminal Intelligence Systems Operating Policies* (28 Code of Federal Regulations Part 23.20), 1993.

Counterdrug Intelligence Executive Secretariat, *General Counterdrug Intelligence Plan*, U.S. Department of Justice, 2000.

Criminal Intelligence Committee, California Peace Officers' Association, *Criminal Intelligence Program for the Smaller Agency*, revised edition, 1998.

Frost, Charles, "Choosing Good Intelligence Analysts: What's Measurable," *Law Enforcement Intelligence Analysis Digest*, Vol. 1, No. 1, 1985.

Global Intelligence Working Group, *National Criminal Intelligence Sharing Plan*, October 2003.

Harris, Don R., et al., *The Basic Elements of Intelligence Revised*, Law Enforcement Assistance Administration, 1976.

_____ and E. Drexel Godfrey, *The Basic Elements of Intelligence*, Law Enforcement Assistance Administration, 1971.

McDowell, Donald, *Strategic Intelligence*, Istana Enterprises, 1998.

International Association of Chiefs of Police, National Law Enforcement Policy Center, *Criminal Intelligence*, 1998 and updated June 2003.

_____, *Law Enforcement Policy on the Management of Criminal Intelligence*, 1985.

International Association of Law Enforcement Intelligence Analysts (IALEIA), *Intelligence-Led Policing*, 1997.

IALEIA and Law Enforcement Intelligence Unit (LEIU), *Intelligence 2000: Revising the Basic Elements*, 2001.

INTERPOL, *Crime Analysis Booklet*, International Criminal Police Organization, Crime Analysis Working Group, 1996.

Morris, Jack, and Charles Frost, *Police Intelligence Files*, 1983.

Law Enforcement Intelligence Unit, *File Guidelines*, 2002.

National Criminal Intelligence Service UK, *The National Intelligence Model*, 2001.

Parks, Dean, and Marilyn B. Peterson, "Intelligence Reports," *Intelligence 2000: Revising the Basic Elements*, 2001.

Peterson, Marilyn B., *Applications in Criminal Analysis*, Greenwood Press, 1994, and Praeger, 1998.

Second Printing
August 2006