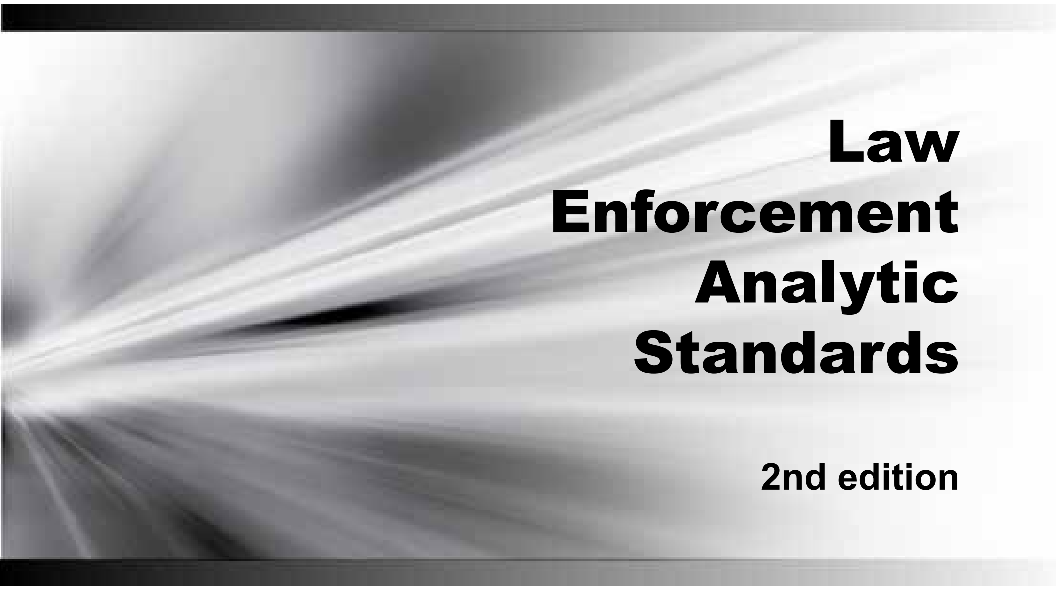
Global Justice Information Sharing Initiative
United States
Department of Justice

IALEIA

Law Enforcement Analytic Standards

2nd edition

April 2012



Law Enforcement Analytic Standards

2nd edition

Global Justice Information Sharing Initiative

International Association of Law
Enforcement Intelligence Analysts, Inc.

April 2012

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.

This project was supported by Grant No. 2009-DB-BX-K105 awarded by the Bureau of Justice Assistance, Office of Justice Programs, 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 publication are those of the author(s) and do not necessarily reflect the views of the U.S. Department of Justice.

Table of Contents

Introduction

The intelligence analyst is critical to the planning, intelligence, and investigative activities of a law enforcement agency. In this environment, analysts require the relevant experience, expertise, and training to perform their jobs effectively. The publication of the *National Criminal Intelligence Sharing Plan* (NCISP, 2003) prompted the Global Justice Information Sharing Initiative (Global) Intelligence Working Group (GIWG) Training Committee to act on this need. GIWG requested that the International Association of Law Enforcement Intelligence Analysts (IALEIA) develop analyst standards based on the tenets articulated in the NCISP.

> 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).

Publication of the *Law Enforcement Analytic Standards* (Standards, 2004), the result of this recommendation and the collation of previous contributions on the role of analysts, provided the foundation for the development of professional standards for analysts. As a result of a review of subsequent publications on analytical standards since 2004, Global and the CICC have published this 2012 version that reflects current progress toward institutionalizing the role of the analyst. In its entirety, this version describes management's role in shaping the analyst's environment—from hiring and supervising through producing professional products for investigators and decision makers.

Analyst Managers

Managers are vital to the intelligence process because they are responsible for intelligence analysis planning and oversight. The manager sets priorities for intelligence projects and directs the intelligence team to ensure the most efficient intelligence operations and comprehensive intelligence products possible.

- Managers will ensure that analysts possess the appropriate competencies and capabilities to perform the required analytic duties. This can be accomplished through recruitment, screening, and a process-based assessment conducted in a manner to identify the most suitable candidates.
- Managers must encourage and support a collaborative environment for all analytic and intelligence functions. Establishing a team-based approach to dealing with intelligence and analytic activities ensures a cooperative rather than competitive atmosphere. An integrated, holistic approach to law enforcement intelligence and analysis (Ratcliffe, 2007) guides decision making.
- Managers must develop an intelligence operational plan for the overall agency intelligence function, including mission, goals, and objectives, as a guide to activities. This operational plan will be used to guide and direct collection and analytic activities.
- Managers must develop and apply appropriate evaluation measures and encourage, support, and reinforce the production of high-quality intelligence products. Evaluating the quality of analytic performance should be based on job task analyses. Law enforcement intelligence analysts should be provided with the objective measures upon which their performance is assessed. The Federal Bureau of Investigation (FBI) Career Path Standards are used to evaluate intelligence analysts by reviewing performance on seven “critical elements” (2000):

- Organizing, Planning, and Coordinating
- Technical Expertise
- Critical Thinking
- Engagement and Collaboration (internal and external to the organization)
- Personal Leadership and Integrity
- Communication (written and oral)
- Accountability for Results

Within the intelligence-led policing model, a quality intelligence analysis manager influences and directs the eventual success of law enforcement intelligence analysts.

Standards for Analysts

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. The standards in this section relate to analysts or individuals performing an agency's analytical function.

Analytic Attributes

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

- Subject-matter expertise
- Analytical methodologies
- Critical-thinking skills
- Customer-service ethic
- Communication skills
- Information sharing and collaboration abilities
- Information handling and processing skills
- Computer and technical literacy
- Objectivity, integrity, and intellectual honesty

The *Common Competencies for State, Local, and Tribal Intelligence Analysts* (2010) identifies common analytic competencies exhibited by state, local, and tribal intelligence analysts working in state or major urban area fusion centers or similar analytic law enforcement entities. The five baseline analytical competencies identified are thinking critically, sharing and collaborating, fusing intelligence and law enforcement tradecraft, communicating, and turning concepts and principles into action.

Additional generic characteristics an analyst should possess include intellectual curiosity, rapid assimilation of information, keen recall, tenacity, willingness and capacity to make judgments, initiative and self-direction, effective personal interaction, and disciplined intellectual courage (Frost, 1985).

The FBI’s list of core competencies for analysts, or critical elements, includes judgment, professionalism/liaison, flexibility/adaptability, capacity to learn, initiative/motivation, organizing, planning and prioritizing, knowledge of current events, and coaching skills (2000).

Education

> ***Ideally, analysts should have either a four-year college degree or commensurate experience, which is:***
>
> - At least five years of previous research, analysis, and intelligence-oriented experience with a two-year degree
>
> or
>
> - At least ten years of previous research, analysis, and intelligence-oriented experience with less than a two-year degree.

Relevant experience in the public, military, academic, or private sector should be documented through job descriptions and examples of work products. Appropriate college degree areas should include those with intensive research, writing, and critical-thinking components.

Basic Training

> ***Initial analytic training shall be a minimum of 40 hours and be provided by instructors with law enforcement analytic experience, adult learning skills, and certification by an accrediting entity.***

Training is important to understand how to conduct effective and timely analysis. Setting and maintaining analytic standards will allow employers to ensure that analysts achieve similar objectives and competencies to support agency tactical and strategic operations effectively. The following topics identify specific training areas, core competencies, and critical-thinking concepts recommended as components of a basic 40-hour training course.

- Introduction to intelligence
- Analytic guideline documents (refer to Sources)
- Analytical techniques
- Analytical tools
- Civil liability
- Crime indicators
- Crime-pattern analysis
- Critical thinking
- Data mining
- Effective planning of intelligence products
- Ethics
- Inference development
- Information evaluation
- Information management
- Information sharing framework
- Infusing consumer feedback into the intelligence cycle
- Intelligence cycle/ process
- Intelligence requirements/collection
- Law and legal aspects
- Logic/fallacies of logic
- Markings and using confidential information
- National security
- Needs of the consumer (strategic, tactical)
- Networking
- Presentation of information
- Privacy, civil liberties, and civil rights protections
- Professional standards/ certification program for analysts
- Report writing
- Sources of information/ available resources
- Threat assessments

The *Minimum Criminal Intelligence Training Standards for Law Enforcement and Other Criminal Justice Agencies in the United States (*MCITS, 2007) provides guidance for the development and delivery of law enforcement intelligence training. This document contains recommendations for standards and competencies to be included in training courses for entry-level intelligence analysts.

Advanced courses should expand on these concepts and principles to provide greater breadth and depth of tradecraft, content, and analytical thinking. Analysts and agency leadership should evaluate and determine the specific training courses for their analysts to meet the agency's analytical needs.

Continuing Education and Advanced Training

> ***Those performing the analytical function shall annually receive at least eight hours of continuing analytic education through a combination of formal education, training classes, distance learning, or documented self-directed study efforts.***

Most professions require continuing education for their members to maintain currency and professional standing in their field. For analysts, this training can be on topics related to analytical methods and tradecraft; analytical software and tools; law enforcement trends, crimes, and criminal groups; investigative and analytic techniques; supervision and management; and recent statutes and regulations. An added benefit to training is the creation of a collaborative environment in which analysts can build relationships with other analysts, learn from each other, and adapt to ongoing changes in the intelligence arena.

This training should meet continuing education standards, document student attendance, and measure achievement of a specified level of performance. Analysts should strive to develop specific subject-matter expertise in their area of responsibility.

> ***The training provider should have academic or professional association credentialing and subject-matter expertise in law enforcement intelligence analysis. Instructors should be certified to ensure the use of proper techniques in adult learning and instruction.***

Any organization engaged in teaching law enforcement intelligence analysts should ensure that instructors successfully complete an instructor development program or a Train-the-Trainer program. The Minimum Criminal Intelligence Training Standards for a Train-the-Trainer program are designed to ensure that the critical information needed for the new trainer is incorporated into the curriculum.
In addition, the International Association of Directors of Law Enforcement Standards and Training (IADLEST) provides a model policy for Training and Instructor Standards (Section 5.0) as a guide for standards for training instructor development.

Professional Development

> ***Analysts shall maintain a program of professional development throughout their career. Their employers should ensure that analysts provide maximum benefit to operations by implementing professional development programs for their analytic staff, whether they are analysts or sworn officers.***

The *Continuing Professional Development Workbook and Portfolio* (Atkin, 2002) encourages analysts to assemble a document to track their learning and experiences to demonstrate growth and development over their careers. It also encourages analysts to seek out new experiences to add to their knowledge base.

Professional development is not only training or gaining new experiences but also recognition within the agency for professionalism and attaining proficiency levels.

Certification

> ***Analysts should be certified by completing a program specifically developed for intelligence analysts, provided and certified by an agency or organization (governmental, professional association, or institution of higher learning). Such analytic certification programs shall reflect practitioner experience, education, training, knowledge of adult instructional techniques, and proficiency testing.***

Certification provides employers with an enhanced means to measure analysts' competence and experience. In addition, it grants analysts other benefits, notably the recognition of their professional abilities and skills. The certification process promotes professionalism and leadership within the analytical community and encourages continuing participation, education, and contributions to the analyst and intelligence communities. Certification reinforces the credibility of an analyst.

In a joint effort, Global and IALEIA published the *Law Enforcement Analyst Certification Standards* in 2006 as a guide to operating a certification program. The first section provides guidance to agencies and organizations offering analyst certification. The second section offers guidance regarding instituting the analyst certification process. The result of applying these standards within agencies and organizations will be the institutionalization of the law enforcement analyst as a professional within the law enforcement field.

Law enforcement managers' need for certified analysts engendered a proliferation of certification programs throughout the analytical world. These programs include state, provincial, and national-level law enforcement agencies, academic institutions, corporate entities, and international associations. IALEIA offers the Law Enforcement Criminal Intelligence Certified Analyst (CICA) certification, which is based on practitioner hands-on experience, education, intelligence training, and proficiency testing.

Professional Liaison

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

"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" (NCISP, 2003).

Networking—liaising with other professional analysts—is an essential component of an analyst's position. Sharing documentation, sources, methodologies, and contacts among analysts enhances their ability to provide a cogent product to the investigators, attorneys, and management. The *Common Competencies for State, Local, and Tribal Intelligence Analysts* encourages analysts to engage in collaborative, team-oriented analysis to "establish trusted networks of key contributors within the homeland security and law enforcement community to share information and analytic insights that will lead to action on critical issues" (Global, 2010).

The two primary law enforcement intelligence associations/organizations in the United States are the International Association of Law Enforcement Intelligence Analysts (IALEIA) and the Association of Law Enforcement Intelligence Units (LEIU). Participation in these international professional organizations provides access to the latest methodologies, trends, policies, procedures, and innovations in research, analytical software, and networking through publications, training, conferences, and local, regional, and international chapters.

Leadership

> ***By modeling excellence in the intelligence-led policing decision-making process, analysts have an opportunity to lead and influence peers, subordinates, and supervisors.***

Leaders excel in managing tasks, teams, projects, and individuals while striving for performance excellence. Rather than demonstrating command and control, personal leadership is the activity or practice of influencing people, while using ethical values and goals to produce intended changes. Senior analysts can mentor less experienced personnel in developing analytic excellence in competencies and skills.

Leadership training, mentoring, and succession planning are vital for the continuity and success of law enforcement intelligence analysis units. The *General Counterdrug Intelligence Plan* (GCIP, 2000) highlights the need for career paths and career development for analysts to allow them to move into supervisory and management positions. Global's *Intermediate Analyst Training Standards*[1] avers that seasoned law enforcement intelligence analysts should be provided with the opportunity to receive management training.

Law enforcement intelligence is a sensitive area requiring effective intelligence managers to understand the inherent responsibilities, hazards, and challenges (MCITS). Given the critical nature of analytic skills necessary to develop policy and make sound decisions, analysts should be promoted into agency management. The U.S. Drug Enforcement Administration was one of the first agencies to promote analysts into key management positions.

[1] To be released in 2012.

Standards for Analytical Processes

NCISP (2003) Recommendation 1 states that the agency chief executive officer and the manager of intelligence functions should "support the development of sound, professional analytic products (intelligence)." One method is to recommend that products meet substantive criteria. The following standards for analysis, which correspond to the intelligence cycle, show the critical role analysis plays in each section of the intelligence cycle. Additional details on analytic products and processes are described in the *Common Competencies for State, Local, and Tribal Intelligence Analysts* (2010).

Planning and Direction

> ***Analysts shall understand the objective of their assignment, define the problem, and plan for the necessary resources through the use of a collection or investigative plan or intelligence requirements reflecting the needs of the customer. Specific steps to complete the assignment, including potential sources of information and a projected timeline, shall be included.***

The intelligence cycle begins and ends with planning. Collection plans may be drawn based on indicators resulting from previous elements of the cycle. The plan of action created through recommendations may contain requirements for further collection to reinitiate the cycle. Many agencies have discovered that using intelligence analysts at the beginning of an investigation focuses the investigation and saves 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. From a combination of the information provided and researched, the analyst can develop a collection or investigative plan to enable the investigators and analysts to obtain the necessary data to meet the objective of the assignment.

> ***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 also what is missing. This allows them to conceive plans and requirements to view the problem and its solution(s) clearly. Analysis can also be integrated into a department's planning efforts. Strategic analysis, which identifies significant crime problems and recommends actions to reduce or prevent crime, should become part of the agency's strategic plan.

Collection and Follow-Up

> ***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.***

Analysts are an asset when provided with primary information, such as investigative reports, field and police interviews, surveillances, and informant data. The information collected can be used to discover threats and criminal conspiracies. Analysts, with access to a wealth of information on the Internet and elsewhere, should utilize analytic approaches, collection plans, and priority information needs while balancing a short-term response with long-term value. They may find information to identify the suspect and his location, employment, affiliated organizations, schools attended, etc.

The *Analyst Toolbox*: *A Toolbox for the Intelligence Analyst* (2006) identifies public information databases as a key tool in the analytic repository. Additionally, open source information, suspicious activity reports, intelligence bulletins, and other routine information collected by law enforcement agencies may provide relevant information to analysts. As analysts collect information, they should be cognizant of privacy, civil rights, and civil liberties policies and ensure the information collected is legally gathered, integrated, and utilized.

> ***In the course of collection by investigators and others, analysts shall evaluate the progress of the collection to determine whether the collection plan/requirements are met and shall identify additional sources of information, as well as information useful to other cases or activities. When possible, analysts shall relay pertinent information to an appropriate body for follow-up.***

Analysts' information management role does not end with the creation of a collection plan or the identification of requirements but continues as new sources of potential information are developed. As information is collected by the investigator or analyst, the collection plan should be reevaluated to monitor progress. The analyst knows the requirements and planning functions, what is needed, and what sources will provide additional information. The collection should be flexible so the analyst and the investigative manager can surmount impediments as they arise.

Evaluation

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

28 Code of Federal Regulations (CFR) Part 23.20 states:

> Information shall be labeled to indicate levels of sensitivity, levels of confidence, and the identity of submitting agencies and control officials.

The "levels of confidence" relate to reliability, validity, and relevancy. Analysts must remain current on policy changes regarding classification standards and levels in order to ensure proper safeguarding of information shared with federal, state, local, tribal, and private sector entities.

Reliability gradients progress from "reliable" to "usually reliable," "sometimes reliable," "unreliable," and "reliability unknown." Data in the last two categories would be considered questionable and should not be shared with others.

Validity gradients may include “confirmed,” “probably true,” “possibly true,” “doubtful,” and “cannot be judged.” Data in the last two categories should be held for further corroboration but not disseminated.

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

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.”

Collation

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

An inventory of the data is the quickest way to see gaps in the documents provided and identify further collection efforts. Information, once collected, must be organized logically and clearly. Analysis is often done on diverse information from a variety of formats, such as incident information, financial records, telephone call records, or surveillance reports. Critical elements can be combined into similar formats for retrieval and sorting and will assist the analysts in ascertaining patterns.

Computer-Aided Analysis

> ***Computerized assets available in the modern age can expedite, streamline, and enhance the analytic outcomes and products when applied by experienced analysts. Analysts shall utilize the best and most current computerized visualization and analytic tools available to them.***

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

Database software is used to store, organize, and manage information from disparate sources so it can be retrieved and analyzed.

Spreadsheet software most often organizes, tabulates, displays, and graphically depicts mathematical or financial data.

Visualization software assists the analyst in extracting information from all sources, databases, and spreadsheets to produce and change charts as new information is known. A subset of visualization software, mapping software, may geographically depict criminal activity from the street, local, county, state, regional, or national level.

Text and data mining search engines provide analysts with the ability to review and cull multiple sources (databases, spreadsheets, text files, etc.) for further analysis.

The *Analyst Toolbox* (2006) contains a list of software representative of the basic toolbox intelligence analysts will need to perform their duties effectively and efficiently and produce meaningful and useful intelligence products.

Analytic Outcomes

> ***Analyses shall include alternative scenarios and avoid single-solution outcomes when appropriate. Analyses shall indicate all the hypotheses evaluated, in addition to the most likely hypothesis arrived at through the analysis of all competing hypotheses.***

The results of analysis are hypotheses, conclusions, and recommendations for action. However, dependent upon which hypothesis is the best choice, multiple hypotheses could be drawn and the analyst could make multiple recommendations for actions. Although choosing among hypotheses is a difficult task, one technique to determine which hypothesis is best is the Analysis of Competing Hypotheses, detailed in Richards J. Heuer, Jr.'s book *Psychology of Intelligence Analysis* (1999). Heuer's process leads the analyst to evaluate known hypotheses and all bits of evidence to eliminate all but the most likely hypothesis.

The *Common Competencies for State, Local, and Tribal Intelligence Analysts* (2010) states that analysts should structure "logical arguments that have clear and meaningful conclusions, are supported by logical claims and relevant data, and account for inconsistent data." The document also indicates that an analyst's behavior indicators include "overcoming mental mind-sets and avoiding common fallacies in selection and use of data and development of arguments and conclusions."

Dissemination Plan

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

Intelligence is of no value unless it is shared. Analytic products may be developed to support internal or multiagency needs and short-term or long-term goals. As a result, dissemination will differ with each product.

The intelligence analysis product must have a purpose and must align the issue and the customer. If the report has been assigned as part of a specific investigation, 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, they would form the audience. A written dissemination plan for the product is essential, even if it is only a paragraph stating the specific audience, to avoid intelligence sharing misunderstandings. The report may require multiple versions, depending on its sensitivity and intended purpose and/or recipient: one with specific recommendations for a target audience and another for a more general audience.

Proactive dissemination may also be appropriate when there is an indication the information may be of value to an external agency, even when that agency may not be aware of the data.

Standards for Analytical Products

Analytical Accuracy

> ***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.***

Analytic products (i.e., intelligence) can be only as accurate as the data provided to create them. When the data is collected and reported by investigators to the analysts, accuracy is critical. When the analyst is suspicious of the veracity of the data provided, it should be noted. The analyst must verify all data (or have it verified) before treating it as accurate. Information in conflict with the hypothesis as well as data that supports it must be noted. Analysts should have few to no preconceived ideas about what occurred. The presence of exculpatory data may be critical to the decision-making process. Noting this information also allows the analyst to view the occurrences from the target's or subject's point of view.

Analytic Product Content

> ***Analytic products shall always include analysis, assessment, integrated data, judgments, conclusions, recommendations, and caveats (when appropriate). Forecasts, estimates, and models shall be developed when appropriate.***

Analysts should strive to transform customer needs into intelligence requirements and ensure that the products correspond to the issue, customer, and/or purpose. Intelligence is produced with a thorough analysis of the information available. This may include charts, maps, tables, and diagrams detailing how they relate to the threat, problem, crime, investigation, or trial. The final report should reflect the analysis while providing conclusions and recommendations.

Analytic Product Format

Analytic intelligence report formats shall be tailored to the consumer's needs. Strategic, tactical, and operational assessments can include a variety of analytic techniques, such as:

- Communication analysis
- Crime-pattern analysis
- Criminal business profiles
- Demographic/social trend analysis
- Financial
- Flow analysis
- Geographic analysis
- Geospatial analysis
- Indicator analysis
- Market profiles
- Network analysis
- Problem and target profiles
- Results analysis
- Risk analysis
- Threat analysis
- Vulnerability analysis

The definitions of these products are included in the Glossary of Terms. Each analytic product may be a collection of subproducts. A network analysis might include an association matrix, a link chart, a map, a geospatial chart, a summary, conclusions, and recommendations, all of which might be defined as individual "products." A problem profile might include crime-pattern analysis, geographic analysis, demographic and/or social trend analysis, statistical analysis, indicators, conclusions, and recommendations. More in-depth information is included in the LEIU/IALEIA *Criminal Intelligence for the 21st Century: A Guide for Intelligence Professionals* (2011).

Analytic Report

Reports shall be written clearly and facts documented thoroughly. A logically derived, analytic conclusion, including key intelligence gaps, should be provided. A concise, coherent organization of facts shall indicate how the analyst arrived at conclusions. Objective and dispassionate language shall be used, emphasizing brevity and clarity of expression.

Analysts should be accomplished writers with the ability to convey information in a brief, yet comprehensive manner. Effective writing includes logical organization of analysis and conclusions separating facts from opinions. Documentation is crucial. Dubious statements and sources must be noted so the person making a judgment is able to decide the weight or validity to ascribe to the statement. The analytic process should be presented in an objective manner. With the exception of appropriately labeled hypotheses and conclusions based upon logical analysis, opinion should be omitted.

Data Source Attribution

> ***Every intelligence product shall clearly distinguish which content is public domain or general unclassified information, which information is restricted or classified, and which content reflects the judgment or opinion of analysts and/or other professionals.***

The analyst and the customers must be cognizant of the intelligence sources and limitations to sharing. If the data is from public domain sources, the resulting intelligence will be less sensitive than if it is based upon classified information from another agency. If 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 stored and shared as appropriate. Analysts should be knowledgeable of all current marking rules for classified or unclassified information, including the use of portion marking to ensure that all products can be disseminated to the appropriate partners. The analyst must separate 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.

Analytic Feedback and Product Evaluation

> ***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.***

Conclusions within analytic products may be open to interpretation. Hence, products should be reviewed and evaluated by other intelligence professionals, who may arrive at different conclusions based on the same facts. Alternate conclusions or recommendations should be included. Some agencies share intelligence products to check for inaccuracies. Customer evaluation of analytic products is essential. A customer feedback form that solicits comments, accompanying the product, may facilitate developing better, more relevant products.

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

The charge for creating these analytic standards is "to ensure intelligence products are accurate, timely, factual, and relevant and recommend implementing policy and/or action(s)" (NCISP 2003). These analytic standards, taken in their entirety, are not only the response to this charge but also guidelines for professional and reliable products. Throughout the process, the analyst should employ structured analytic techniques, critical thinking, and rigorous evaluation to elicit key judgments, conclusions, and recommendations. Final evaluation should use similar techniques, which may engender additional questions of the finished analytic product.

- What other information would I like to have to complete the picture?
- What other information can I collect 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 of 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?

Presentations

> ***Briefings and presentations are key opportunities to convey the vital points of the intelligence analysis. Oral presentations should be concise, effective, and appropriately tailored to the target audience and should communicate analytic judgments and relevant intelligence gaps.***

Effective briefers are poised, prepared, and precise as they communicate analytic observations and judgments. Visual presentation software and graphics are tools to support intelligence analysis, rather than the focal point of the briefing. Quality presentations are adapted to meet time constraints and the needs of the audience.

Testimony

> ***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; therefore, analysts should be capable of presenting materials in these forums. Testifying as a fact/summary witness may require only 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.

Legal Considerations

> ***Analysts must be familiar with the legal; privacy, civil rights, and civil liberties; ethics; and operational security issues surrounding intelligence.***

Analysts must be able to apply their agency's policies, guidelines, and operating procedures to information and intelligence sharing, analysis, and dissemination. Relevant legal concerns include issues surrounding:

- Privacy, civil rights, and civil liberties protections
- Security of information
- Operational security practices
- Storage and retention of law enforcement intelligence and information

The purpose for which information is collected, retained, used, and shared and the manner in which it is done may impact individual privacy, civil rights, and civil liberties. Consequently, agencies should ensure that privacy, civil rights, and civil liberties are protected. Information collected from an agency at the local or state level must comply with applicable local or state law. Proper handling and protection of personally identifiable information (PII) is vital, particularly in national security and interagency environments such as task forces, fusion and intelligence centers, and cooperative intelligence initiatives. 28 CFR Part 23 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.

Data from questionable sources should be treated carefully and noted as such in analytic reports. Raw data obtained in violation of any applicable local, state, or federal law should not be incorporated into an analytic product. If, subsequent to the release of the product, the analyst discovers inaccuracies in the collection of the information, the analyst should make every reasonable effort to notify both the provider of the information and the recipients of the product that it has been withdrawn and should not be used because of data quality issues.

Summary and Conclusions

This *Law Enforcement Analytic Standards* is a compendium of theories and practices proved to be successful in the analytical field. Disseminating these standards throughout the law enforcement intelligence community will allow them to become more universally accepted, and adherence to them is strongly encouraged. As a result, managers will put more trust in analytic judgments and products because they will have a greater understanding of the underlying basis for those results.

Glossary of Terms

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.

Analytic Writing. Written communication focusing on distilling and summarizing factual information to provide concise and clear reports for managers and other customers.

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

Association Analysis/Network Analysis. Collection and analysis of information that indicates relationships among varied individuals suspected of involvement in criminal activity and providing insight into the criminal operation and which investigative strategies might be the most effective.

Collation. The process by which information is assembled and compared critically.

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

Collection Plan. A plan directing 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.

Communications Analysis. The review of records reflecting communications (telephone, e-mail, pager, text messaging, etc.) among entities for indicators of criminal associations or activity. Results may recommend steps to take to continue or expand the investigation or study.

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

Crime-Pattern Analysis. A process seeking links between crimes and other incidents to reveal similarities and differences to help predict and prevent future criminal activity.

Criminal Analysis. The application of analytical methods and products to raw data to produce intelligence within the criminal justice field.

Criminal Business Profile. A product detailing 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 data, often through developing and answering questions about the data.

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

Data. Raw facts or variables used as a basis for reasoning, discussion, or calculation.

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 to show 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 and may show missing actions or events needing further investigation.

Forecast. An evaluation of 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. An evaluation of 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 to be proved 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 behavioral profiles or early warning systems in computerized environments.

Information. Facts, data, or knowledge that has not been subjected to analysis. Often referred to as “knowledge in raw form.”

Intelligence. Information + Evaluation. The product of systematic gathering, evaluation, and synthesis of raw data on individuals or activities. Intelligence is information 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. Planning, collection, collation, evaluation, analysis, dissemination, and feedback.

Intelligence Gap. A topic requiring additional information collection and analysis.

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 surveying 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 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 collected by officers or analysts not yet subjected to the intelligence process, thus it is not intelligence.

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

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.

Risk Analysis/Assessment. An evaluation of untoward outcomes from an incident, event, or occurrence. Assesses the likelihood of risks and consequences posed by individual offenders or organizations to potential victims, the public at large, and law enforcement agencies. It generally includes preventative steps to be taken to lessen the risk.

Source Reliability. A scale reflecting 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. 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 of immediate use by operational units to further a criminal investigation, plan tactical operations, and provide for officer safety.

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

Telephone Record/Toll Analysis. See Communications Analysis.

Threat Assessment. A report that evaluates a natural or man-made occurrence, an individual, an entity, or an action which has harmed or could harm life, information, operations, the environment, and/or property. Assesses the present or future threat and recommends ways to lessen the impact.

Vulnerability Assessment. A report evaluating physical features or operational attributes that render an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard. Recommends ways to lessen or eliminate the vulnerability.

Sources

Association of Law Enforcement Intelligence Units and International Association of Law Enforcement Intelligence Analysts*, Criminal Intelligence for the 21st Century: A Guide for Intelligence Professionals,* 2011.

Atkin, Howard N., *Continuing Professional Development Workbook and Portfolio*, International Association of Law Enforcement Intelligence Analysts, 2002.

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

Carter, David L., *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies* (2nd ed.), U.S. Department of Justice, 2009.

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.

Europol, *Analytical Guidelines*, 2000.

Europol, *Intelligence Management Model for Europe, Phase One: Guidelines to Standards and Best Practice Within the Analysis Function*, 2003.

Federal Bureau of Investigation, Career Path Standards, 2000.

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.

Global Justice Information Sharing Initiative, *Analyst Toolbox: A Toolbox for the Intelligence Analyst,* 2006, updated 2007.

———, *Baseline Capabilities for State and Major Urban Area Fusion Centers: A Supplement to the Fusion Center Guidelines*, 2008.

———, *Common Competencies for State, Local, and Tribal Intelligence Analysts*, 2010.

———, *Minimum Criminal Intelligence Training Standards for Law Enforcement and Other Criminal Justice Agencies in the United States* (version 2), 2007.

———, *Minimum Training Standards for Enhanced Analyst Training,* 2011.

——— and International Association of Law Enforcement Intelligence Analysts, *Law Enforcement Analyst Certification Standards,* 2006.

———, *Law Enforcement Analytic Standards*, 2004.

Godfrey, E. Drexel, and Don R. Harris, *Basic Elements of Intelligence*, Law Enforcement Assistance Administration, 1971.

Harris, Don R., et al., *Basic Elements of Intelligence (*revised), Law Enforcement Assistance Administration, 1976.

Heuer, Jr., Richards, *Psychology of Intelligence Analysis,* Center for the Study of Intelligence, 1999.

International Association of Chiefs of Police, *Law Enforcement Policy on the Management of Criminal Intelligence*, 1985.

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

International Association of Directors of Law Enforcement Standards and Training, *Model Minimum Standards,* 4065001

.

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

International Association of Law Enforcement Intelligence Analysts (IALEIA) and Law Enforcement Intelligence Unit, *Intelligence 2000: Revising the Basic Elements*, 2001.

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

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

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

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

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.

Ratcliffe, Jerry H., *Integrated Intelligence and Crime Analysis: Enhanced Information Management for Law Enforcement Leaders,* Police Foundation and U.S. Department of Justice, Office of Community Oriented Policing Services, August 2007.

United Nations Office on Drugs and Crime, *Criminal Intelligence Training Manual for Analysts*, n.d.

U.S. Department of Homeland Security, Risk Steering Committee, *DHS Risk Lexicon,* September 2008.

Bureau of Justice Assistance
U.S. Department of Justice

For More Information

www.it.ojp.gov
www.ialeia.org