IALEIA

Intelligence Analysis Standards

3rd edition

May 2026

Intelligence Analysis Standards

3rd edition

International Association of Law Enforcement Intelligence Analysts, Inc.

May 2026

This initial 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 (Global). 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. 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.

Preface

This revised edition of the analytic standards draws on the expertise and insights from current practitioners as well as research into the best practices of the discipline of intelligence analysis. Upon initiating this project, the team of contributors focused on three main objectives:

- Expand the analytic standards beyond the law enforcement field
- Apply the standards to an international audience
- Ensure the standards incorporate current tools, techniques, policies, and processes.

While many of the existing standards remain largely intact, some have been revised to meet these objectives. Others have been added to reflect transformations to the discipline of intelligence analysis since the last edition was published. The intent is that these standards contribute to the professionalization of the field of intelligence analysis.

Many thanks to those who contributed content, research, edits, and suggestions to this project. Also, much appreciation to those who initiated the analytic standards project and wrote the first and second editions of the document. The hope is that it will continue to be revised as the job of the intelligence analyst advances.

Gregory Thomas, PhD
3rd Edition Project Coordinator

Table of Contents

Introduction

The role of the intelligence analyst is critical to the planning, intelligence, and investigative activities of law enforcement, security, defense, and private sector intelligence agencies. In this environment, analysts require the relevant experience, expertise, and training to perform their jobs effectively. These elements develop the discipline of intelligence analysis into a profession. Another important element of a profession is to establish a set of rigorous standards for the competencies of intelligence analysis. While previous studies (Bruce & George, 2015) examined the state of professionalization and standards in national security intelligence analysis in the United States government, this publication expands the standards to an international perspective and covers broader intelligence and security sectors.

The *National Criminal Intelligence Sharing Plan (NCISP),* published by the United States Department of Justice, Global Justice Information Sharing Initiative (Global) in 2003, requested that the International Association of Law Enforcement Intelligence Analysts (IALEIA) develop analyst standards based on the tenets articulated in the plan. Publication of the *Law Enforcement Analytic Standards* (2004), by IALEIA and Global was the result of this recommendation and the collation of previous contributions on the role of analysts. That publication provided the foundation for developing professional standards for analysts. A review of subsequent publications on analytical standards resulted in a revised edition published in 2012 that reflected progress toward institutionalizing the role of the analyst.

This current document revises and extends the 2012 publication to create an international, competency-based framework for intelligence professionals. This revised standard recognizes the evolving role of intelligence analysis across national security, defense, regulatory intelligence, corporate security, financial intelligence, cyber threat intelligence, and academic research settings. It reflects advances in technology, data science, and ethical practice. This edition updates the analytic standards based on best practices and research within the discipline.

This edition provides an international perspective of the standards for intelligence analysis. Editors and reviewers for this edition represent organizations from Australia, Canada, the United Kingdom, and the United States. These individuals are practitioners, professionals, and scholars in the field. This update draws on references from the U.S. Intelligence Community, the United Nations analyst standards, the North Atlantic Treaty Organization intelligence doctrine, the United Kingdom's College of Policing and National Intelligence Model, the European Union security and intelligence education frameworks, the Australian Institute of Professional Intelligence Officers Ltd. and Australian National Intelligence Community professional standards, the Canadian Intelligence Analyst Community of Practice and others.

This publication is guided by the below overall principles and competencies for the intelligence analysis profession.

Core Principles

The Analytic Standards are based on five pillars:

- Professional integrity and ethical practice
- Analytical excellence and critical thinking
- Technological and digital literacy
- Collaborative and cross-sector engagement
- Continuous learning and professional development

Analyst Competencies

Analysts must demonstrate competency across five domains:

- Analytical competence – Apply analytic approaches, manage uncertainty, and integrate data-driven methods.
- Professional practice – Uphold ethical, legal, and accountable intelligence conduct.
- Communication and collaboration – Communicate clearly, foster teamwork, and consider cultural and cognitive diversity.
- Leadership and development – Demonstrate reflective practice, mentorship, and contribute to professionalization.
- Data and technical literacy – Utilize technology, automation, and visualization tools responsibly.

This document sets forth current standards for analyst managers, intelligence analysts, the analytic tradecraft, and analytic products.

Analyst Managers

Managers and those responsible for supervising the analytical function are vital to the intelligence process. A core part of their role is their responsibility for the planning and oversight of the analytical function. The manager sets priorities for analytical projects and directs the analytical team to ensure the most effective products are produced to service intelligence operations.

Intelligence analyst managers may have roles that include:

- National security, defense, and intelligence-led regulatory functions
- Private sector and financial intelligence environments
- Cross-border and multi-agency collaboration
- Governance of analytic technology, including artificial intelligence and automation tools, and their ethical use.

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 a competitive atmosphere. An integrated, holistic approach to intelligence and analysis guides decision making.

Managers must identify skills, knowledge, and training gaps to consistently enable analysis across an ever-changing environment of subject matters. Then managers must enable and provide access to that training.

Managers must develop an intelligence operational plan for the overall agency's 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. Intelligence analysts should be provided with the objective measures upon which their performance is assessed.

National competency frameworks set the required demonstratable skills, along with knowledge and understanding, to be considered proficient in the analyst role and identify core competencies that represent the abilities to be successful in the field. Within the intelligence-led policing model, good intelligence managers and leaders influence, enable, and direct the eventual success of intelligence analysts (Ratcliffe, 2026).

Standards for Analysts

The mission of the intelligence analyst, as described in the NCISP (2003), 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. Similarly, it is expected that the analyst will identify intelligence gaps and make inferences to fill them. The standards in this section relate to analysts or individuals performing an agency's analytical function. These standards set forth the competencies required for an intelligence analyst to complete their mission. For example, Canada's Intelligence Analyst Community of Practice established common competencies for analysts as well as proficiency levels for each (Government of Canada, 2023).

Analytic Attributes

Analysts shall be hired and evaluated based on the following attributes:

- Subject-matter expertise
- Application of analytical methodologies
- Critical-thinking skills
- Customer service and interpersonal ability
- Communication skills
- Information sharing and collaboration abilities
- Organization and planning skills
- Computer, technical, and digital literacy
- Objectivity, integrity, and intellectual honesty
- Cross-cultural and cross jurisdictional competence
- Familiarity with relevant legal and ethical frameworks
- Bias mitigation and reflective practice

These attributes can be measured through the selection and hiring process and should be assessed during performance evaluations.

Additional 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). Analysts should also be proactively engaged in their own continuing professional development, recording new skills, knowledge, and experiences.

Education

> ***Analysts shall have a college bachelor's degree in a relevant discipline or a commensurate combination of education and experience.***

While most job descriptions for intelligence analysts require at least a bachelor's degree, some agencies and organizations have policies that allow for the substitution of relevant experience for education requirements. Each jurisdiction and agency will have its own requirements. Ideally, a new analyst would have a combination of education and relevant experience in intelligence. Experience in the public, military, academic, or private sector should be documented through job descriptions and examples of work products. When considering relevant degrees and higher education qualifications, those with an emphasis on research, writing, and critical thinking provide key skills for an analyst.

Training

> ***Basic analytic training shall be a minimum of 40 hours provided by instructors with law enforcement analytic experience, adult learning skills, and appropriate analytical certification.***

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.

- Analytic techniques
- Analytical tools
- Crime-pattern analysis
- Critical thinking
- Cyber intelligence
- Data analytics and visualization
- Effective planning of intelligence products
- Ethics
- Inference development
- Information evaluation
- Information management
- Information sharing framework
- Intelligence cycle
- Intelligence requirements/ collection
- Introduction to intelligence
- Law and legal aspects
- Logic/fallacies of logic
- Markings and using confidential information
- Needs of the consumer (strategic, tactical, operational)
- Presentation of information
- Privacy, civil liberties, and civil rights protections
- Products of intelligence
- Report writing
- Sources of information/ available resources
- Strategic and tactical assessments

The *Minimum Criminal Intelligence Training Standards for Law Enforcement and Other Criminal Justice Agencies in the United States (*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.

Various agencies and organizations offer basic training programs that meet this standard. These programs can be found in the private sector, military, non-profit organizations, academic setting, and law enforcement agencies. For example, the International Association of Law Enforcement Intelligence Analysts (IALEIA) and Law Enforcement Intelligence Unit (LEIU) offer the Foundations of Intelligence Analysis Training, a five-day introduction to the basics of law enforcement intelligence analysis. The United Nations Office on Drugs and Crime offers relevant courses through its Global eLearning platform.

Continuous Professional Development

Intelligence analysts shall annually receive at least 16 hours of continuing professional development through a combination of formal education, training classes, or documented self-directed study efforts.

Most professions require continuing education for their members to maintain currency and professional standing in their field. Analysts are expected to maintain qualifications aligned with their national qualification framework levels or equivalent. For analysts, this advanced 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, 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 discipline.

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

This training should meet continuing education requirements, document student performance, and measure achievement of a specified level of accomplishment. Analysts should strive to develop specific subject-matter expertise in their area of responsibility. The *Analyst Professional Development Road Map* (2019) offers a sustainable, professional career pathway for analysts.

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

Any organization engaged in teaching intelligence analysts should ensure that instructors successfully complete an instructor development program or a Train-the-Trainer program.

Analysts shall maintain a program of professional development throughout their careers. Their employers should ensure that analysts are provided these opportunities by implementing professional development programs for their analytic staff.

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

As they progress through their careers, analysts should track their learning and professional experiences to demonstrate growth and development (Atkin, 2002). This encourages analysts to seek out new experiences to add to their knowledge base. Bias mitigation and reflective practice training should be part of continuing professional development.

Certification

Analysts should seek certification developed for intelligence analysts and provided by an accredited agency, professional association, or institution of higher learning. Such analytic certification programs shall reflect practitioner experience, education, training, and proficiency testing.

Certification provides employers with an enhanced means to measure analysts' competencies and experience. In addition, it grants analysts other benefits, notably the recognition of their professional abilities and skills. Expert accreditation or recognition may be required if analysts testify in court proceedings. 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 pathways should be competency-based and recognize knowledge, skills, and behaviors rather than tenure. Certification reinforces the credibility of an analyst. For example, in the United Kingdom, the Intelligence Professionalisation Program accreditation by the College of Policing provides interoperability across law enforcement by ensuring analysts have evidenced the same knowledge and proficiency in their roles.

Analyst managers' need for certified analysts engendered a proliferation of certification programs throughout the analytical world. In a joint effort, Global and IALEIA published the *Law Enforcement Analyst Certification Standards* in 2006 as a guide to operating a certification program. Such certification programs include state, provincial, and national-level law enforcement agencies, academic institutions, corporate entities, and international associations. For example, IALEIA offers an international Professional Certification Program based on a combination of work experience, professional training, and proficiency testing. An initiative in Australia is the Australian Institute of Professional Intelligence Officers Ltd. (AIPIO) Certification and Accreditation Scheme (ACAS), a national program for intelligence professionals. Recognition of prior learning is encouraged to facilitate mutual recognition between national systems.

Professional Liaison

Analysts and their organizations shall maintain connections with, and seek available support from, recognized professional bodies and associations.

Networking and liaising with other professional analysts are essential components of an analyst's position. Sharing documentation, sources, methodologies, and contacts among analysts enhances the 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, p. 6).

Professional growth requires structured mentorship, reflective learning, and participation in Communities of Practice. Analysts should contribute to professional bodies and engage in peer learning. Professional intelligence analyst associations include:

- Association of Crime and Intelligence Analysts (ACIA UK)
- Association of Law Enforcement Intelligence Units (LEIU)
- Australian Institute of Professional Intelligence Officers Ltd. (AIPIO)

- Canadian Academy of Intelligence Analysis (CAIA)
- Canadian Intelligence Analyst Community of Practice (IACOP)
- International Association for Intelligence Education (IAFIE)
- International Association of Law Enforcement Intelligence Analysts (IALEIA)

Participation in these and other international professional organizations provides access to the latest methodologies, trends, policies, procedures, and innovations in research, analytical software and tools, and networking through publications, training, conferences, and local, regional, and international chapters.

Leadership

By modeling excellence in the intelligence 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. Certified analysts can mentor less experienced personnel in developing analytic excellence in competencies and skills, with senior analysts or supervisors providing this function across the unit.

Leadership training, mentoring, and succession planning are vital for the continuity and success of intelligence analysis units. Intelligence is a sensitive area requiring effective leaders and analyst managers to understand the inherent responsibilities, hazards, and challenges. Given the critical nature of analytic skills necessary to develop policy and make sound decisions, analysts should be promoted into agency management.

Ethics

Intelligence analysts shall adhere to a code of ethics, either prescribed by their agency or a professional association.

A code of ethics is a fundamental characteristic of a profession. It provides a guiding framework for principles and values that intelligence analysts should follow. It sets a standard for personal and professional conduct.

Adopting a code of ethics is especially significant for those in the intelligence discipline. Professional analyst associations, such as AIPIO and IALEIA, have a code of ethics that members are expected to follow.

Standards for Analytic Tradecraft

It is important that intelligence analysts have overall standards or principles that guide their process even as tools, techniques, and tradecrafts evolve. For example, the Government of Canada Intelligence Analyst Community of Practice established the following principles for intelligence analysis (Government of Canada, 2025):

- Relevant and actionable – Analysts focus on client requirements.
- Rigorous – Analysts use a systematic approach to analysis to ensure objectivity and accuracy.
- Timely – Timely intelligence can prevent surprises and increase the client's ability to integrate analyses and judgments into plans, operations, and strategies.
- Impartial – Analysis is policy neutral and free from external influence.
- Accountable – Analysis and processes are explained, supported, and compliant with organizational frameworks.

While the intelligence process has generally withstood the test of time since it was outlined by Godfrey and Harris (1971), elements of the tradecraft have adapted to the process. The following standards for the tradecraft of intelligence analysis, which correspond to the intelligence cycle, show the critical role analysis plays in each section of the cycle. Modern practice extends this with feedback loops, data provenance tracking, and AI-supported methods. Analysts must ensure:

- Ethical and lawful data collection consistent with privacy principles.
- Integration of relevant and appropriate data sources to include open-source, social media, and geospatial data.
- Application of analytic approaches to shape the structure of the analysis.
- Awareness of cognitive bias, confirmation bias, and analytical pitfalls.
- Documentation of analytical reasoning and decision traceability.

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 needs of the customers and the objective of their assignment, define the problem, and plan for the necessary resources using a collection plan or investigative plan (analytic plan). Analysts should document and prioritize the steps to complete the assignment, including potential sources of information, analytic methods, and a projected timeline. This information should be recorded in a terms of reference which has been scoped with the customer, when feasible.***

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. Agencies have discovered that using intelligence analysts at the beginning of an investigation focuses the investigation and saves time, money, and resources. Analysts should assist in defining the problem, establishing the requirements, and identifying the target of an investigation. 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. A dissemination plan should also be developed during this stage to ensure appropriate sharing of the product with applicable partners and security level of the document.

Analysts shall be involved in planning and direction. 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 to incorporate into investigative plans to drive operations.

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

Collection and Follow-Up

Analytic research should 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 access to information, such as investigative reports, field and police interviews, surveillance reports, and informant data. The information collected can be used to discover threats and conspiracies. Analysts should draw from multiple intelligence disciplines, such as open-source intelligence (OSINT), geospatial intelligence (GEOINT), social media intelligence (SOCMINT), human intelligence (HUMINT), and imagery intelligence (IMINT). They should utilize appropriate approaches, collection plans, and priority information needs while balancing a short-term response with long-term value.

Open sources, such as public records, social media, and commercially available databases are key resources in the analytic repository that can provide reliable yet unclassified insights and evidence. Additionally, suspicious activity reports, intelligence bulletins, and other routine information collected by 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. It is therefore imperative that analysts are aware of relevant legislation in their jurisdiction. For those whose work crosses international borders, an awareness of the legislative framework of partner agencies is also important.

> ***During collection by investigators and others, analysts shall evaluate the progress of the collection process to determine whether the collection plan/requirements are met and shall identify appropriate sources of information.***

The analyst's 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 investigative team can surmount impediments as they arise.

To obtain the data that is pertinent to the analysis, a collection plan should be created to identify:

- What data is required?
- Why is the data required?
- What is the level of priority of the data; essential, valuable but not essential, low impact?
- How do I obtain the data?
- What authorities are required?
- When was the data requested?
- Who made the request?
- When was the data received?
- Who received the data?
- Evaluate the source of the data
- Identify problems, limitations and gaps.
- Establish action items to remedy any issues.

Processing

> ***Information collected shall be properly organized, stored for retrieval, and evaluated for source reliability, content validity, and relevancy. The veracity and processing of information are crucial not only to the validity of the intelligence product but also to officer safety, investigative effectiveness, and solidity of evidence in prosecutions.***

Analysts must remain current of agency policies regarding the handling, processing, storage, and classification standards and levels to ensure proper safeguarding of information shared with federal, state, local, tribal, and private sector entities.

Collation

> ***Data shall be organized and formatted so the analyst can store, retrieve, and sort the information to identify patterns, anomalies, and gaps. If possible, this should 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, gaps, and trends.

> ***Computerized assets can expedite, streamline, and enhance the analytic outcomes and products. 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. Traditional applications include 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 and graphs as new information is known. Mapping software geographically depicts and analyzes 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. Some software platforms integrate multiple applications, but these functions remain analytically distinct.

Analysis

> ***Analytical products should be bespoke. Analyses should 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 possibilities.***

Analysis involves evaluating data and breaking it down into its component parts to compare it to other information to determine meaning in relation to an investigation or problem. The results of analysis are hypotheses, conclusions, identified intelligence gaps with solutions, and recommendations for action. Multiple hypotheses could be drawn, and the analyst could make multiple recommendations for actions.

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. Analysts may use various tools and structured analytic techniques in this process. Pherson and Heuer (2020) highlight commonly used structured analytic techniques by law enforcement, homeland security, and business professionals such as brainstorming, key assumptions check, red hat analysis, and others. Analysts might use methodologies such as analysis of competing hypotheses (Heuer, 1999) or activity-based intelligence (Biltgen and Ryan, 2015).

Applications such as artificial intelligence, machine learning, and natural language processing are legitimate tools in modern analysis and can assist in functions such as large-scale data triage and automated link analysis. Agentic AI can assist in predictive analysis and sensemaking of data. Automated data ingestion can assist in the collation and analysis of data. Use of these tools requires

"human-in-the-loop" oversight, documentation of model limitations, and attention to automation bias. AI-assisted analytical work requires data provenance, reproducibility, and auditability.

Dissemination

> ***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 intelligence product 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. Guidelines should be established regarding dissemination to secondary customers. Classification review protocols should be interoperable with partner jurisdictions.

Intelligence can be disseminated using dynamic dashboards and interactive analytic products. Data visualization and augmented analytics can aid dissemination through real-time situational awareness dashboards.

Reevaluation

The effectiveness of the stages of the intelligence cycle shall be evaluated through customer feedback and review.

The intelligence cycle is a continuous feedback loop. Each component of the cycle should be evaluated for quality, accuracy, and relevance to ensure refinements are made to the process as needed. In addition, the entire process should be evaluated to ensure efficiency, integrity, and timeliness to the customer. The following can assist in the revaluation of the cycle:

- Analytic quality assurance (peer review, independent validation, after-action review).
- Key Performance Indicators: timeliness, accuracy, influence on decision-making.
- Ethical oversight and audit: algorithmic transparency, data equity, and human-in-the-loop control.
- Performance benchmarking: using internal metrics or best practices.

Standards for Analytic Products

Products developed by law enforcement analysts should be tailored to meet the needs of the consumer. However, the finished product should adhere to basic standards. For example, while the U.S. Intelligence Community is comprised of 18 separate organizations, analytic products are consistent with the following analytic tradecraft standards (ODNI, 2023):

- Properly describes quality and credibility of underlying sources, data, and methodologies
- Properly expresses and explains uncertainties associated with major analytic judgments
- Properly distinguishes between underlying intelligence information and analysts' assumptions and judgments
- Incorporates analysis of alternatives
- Demonstrates customer relevance and addresses implications
- Uses clear and logical argumentation
- Explains change to, or consistency of, analytic judgments
- Makes accurate judgements and assessments
- Incorporates effective visual information where appropriate

Analytic output must be precise, transparent, and actionable. Products should include data provenance, classification markings, and metadata. Analysts are encouraged to use visualization, dashboards, and interactive reporting tools. Reports should distinguish factual data from judgment and clearly specify confidence levels. Products may take the form of written assessments, interactive dashboards, or dynamic intelligence briefs.

Following are standards for analytic products of intelligence analysis.

> ***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 processes, critical thinking, and rigorous evaluation to elicit key judgments, conclusions, and recommendations.

Analytical Accuracy

> ***An analytic product shall be an accurate representation of the incident, intelligence, and other datasets. 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 are collected and reported by investigators to the analysts, accuracy is critical. When the analyst has identified limitations with, or has concerns with, 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 not have fixed expectations or assumptions 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 or subject point of view.

Analytic Product Content

> ***Analytic products shall 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 products should be bespoke to meet the customer's requirements. Strategic, tactical, and operational assessments can include a variety of analytic techniques, such as:

- Association analysis
- Communication analysis
- Crime-pattern analysis
- Criminal business profiles
- Demographic/social trend analysis
- Financial analysis
- Flow analysis
- Geospatial analysis
- Indicator analysis
- Market profiles
- Problem and target profiles
- Results analysis
- Risk analysis
- Social network 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. An association analysis might include an association matrix, a link chart, a chart, a geospatial map, a summary, conclusions, and recommendations, all of which might be defined as individual products. A problem profile might include crime-pattern analysis, geospatial analysis, demographic and/or social trend analysis, statistical analysis, indicators, conclusions, and recommendations. More in-depth information on these products is included in *Criminal Intelligence for the 21st Century: A Guide for Intelligence Professionals* (2011).

Analytic Report

Reports shall be written clearly and concisely. Facts shall be 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 impartial language should be used, emphasizing brevity and clarity of expression. Inferences should be clearly delineated as the professional opinions of the analyst.

Analysts should be accomplished writers with the ability to convey information in a brief, yet comprehensive manner and use such principles as the bottom line up front (BLUF). 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 ascribed 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 or other professionals.

The analyst and the customers must be cognizant of the intelligence sources and limitations to sharing. Although datasets may combine multiple unclassified data, the data together may create a comprehensive picture, which may become protected or classified. Analysts must take this into consideration to ensure data is appropriately safeguarded. If unclassified, it is important to know the source of the information 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 and quality assured by peers and evaluated with feedback from customers. Where required, the final product will be evaluated against the initial plan or terms of reference.

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 accompanying the product that solicits comments may facilitate developing more relevant products.

Throughout the intelligence process, the analyst should employ structured analytic processes, critical thinking, and rigorous evaluation. Final evaluation should use similar techniques, which may engender additional questions of the finished analytic product.

- What other information would I like to have?
- What other information can I realistically collect?
- Are elements missing from the collection plan that need to be revisited?
- 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 significant judgments 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 the time constraints and needs of the audience.

Testimony

Analysts shall be capable of giving testimony as witnesses of fact 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 work will often involve creating evidential products for court, hearings, and public inquiries. Therefore, analysts should be capable of presenting materials in these forums. Testifying as a witness of fact may require a recitation of factual materials with appropriate data visualizations. Testifying as an expert witness will vary depending on jurisdiction but typically requires the analyst to be suitably qualified to give an 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 cross examination by the defense attorney.

Legal Considerations

Analysts must be familiar with legal, privacy, civil rights, civil liberties, ethical, 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. Analysts must follow domestic law in their own jurisdiction. They must follow relevant legal frameworks and international human rights conventions.

Relevant legal concerns include issues surrounding:

- Privacy, civil rights, and civil liberties protections
- Security of information
- Operational security practices
- Storage and retention of intelligence and information
- Privacy-by design principles
- Ethical artificial intelligence guidelines

The purpose for which information is collected, retained, used, and shared and the way it is done may impact on individual privacy, civil rights, and civil liberties. Consequently, agencies should ensure that privacy, civil rights, and civil liberties are protected. Proper handling and protection of personally identifiable information is vital, particularly in national security and interagency environments such as task forces, fusion and intelligence centers, and cooperative intelligence initiatives.

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, provincial, or federal law should not be incorporated into an analytic product. If, after 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.

International instruments, such as the United Nations Human Rights Conventions, the European Union General Data Protection Regulation, and ISO Information Security Standards, can be used as illustrative examples of operational standards. Agencies and organizations should align their local legal obligations to the standards.

Summary and Conclusions

This *Intelligence Analysis Standards* document is a compendium of practices that proved to be successful in the analytical field.[1] Disseminating these standards throughout the intelligence community, to include law enforcement, security, defense, and private sector intelligence agencies, will allow them to become more universally accepted. Adherence to them is strongly encouraged. As a result, consumers of intelligence developed by analysts will put more trust in analytic judgments and products because they will have a greater understanding of the underlying basis for those results. In addition, as agencies and organizations adopt these standards, the role of intelligence analysis will be more generally transferrable throughout the broader intelligence discipline.

[1] Contributors to this edition represent the following agencies and organizations:

- Australian Institute of Professional Intelligence Officers Ltd.
- Canadian Intelligence Analyst Community of Practice
- Government of Canada, Privy Council Office
- International Association for Intelligence Education
- International Association of Law Enforcement Intelligence Analysts
- Pennsylvania State University
- United Kingdom Civil Service
- United Kingdom Law Enforcement

Glossary of Terms

ACAS. Australian Institute of Professional Intelligence Officers Ltd. (AIPIO) Certification and Accreditation Scheme.

Agentic AI. Autonomous artificial intelligence tools supporting but not replacing human analytic judgment.

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 reports to evaluate the impact of a crime group or criminal activity on a jurisdiction, now or in the future. These may include assessments of threat, vulnerability, or risk.

Association 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.

Bias. A disproportionate prejudice for or against a person, group, or idea, which can be explicit or implicit.

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 systematic directing of the gathering of data on a particular topic with a specific objective, a list of potential sources of that data, and an estimated time frame.

Communication Analysis. The review of records reflecting message interactions (telephone, e-mail, text messaging, etc.) among entities for indicators of associations or activity.

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 operation.

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

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

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

Data Provenance. Metadata tracking data origins and transformations.

Demographic/Social Trend Analysis. An examination of the nature of population sector characteristics 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 business 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 crime proceeds 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.

GEOINT. Geospatial intelligence.

Geospatial 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.

HUMINT. Human intelligence.

Hypothesis. A tentative assumption to be proved or disproved by further investigation and analysis.

IMINT. Imagery intelligence.

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.

Inferences. Drawing conclusions based on established facts.

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

Intelligence. Information + Analysis. 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.

Intelligence Cycle. Plan and direct, collect, process/collate, analyze, disseminate, and reevaluation.

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

Intelligence-Led Policing. The collection and analysis of information to produce an intelligence 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 the demand or supply of that product.

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

OSINT. Open-source intelligence.

Probability Yardstick. Estimates of likelihood in intelligence reporting.

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

Raw Data. See data.

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

Results Analysis. An assessment of the effectiveness of police strategies and tactics 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.

Social Network Analysis. A research method for analyzing social structures by mapping relationships between entities such as people, organizations, or businesses.

SOCMINT. Social media intelligence.

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

Structured Analytic Techniques (SAT). Systematic methods to analyze data to mitigate bias.

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.

Telephone Record/Toll Analysis. See Communications Analysis.

Terms of Reference. A document defining the purpose, scope, objectives, and structure of a project or assignment.

Threat Analysis/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 Analysis/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 vulnerability

Sources of Information

Following is a list of references cited in this publication as well as additional sources of information that might be useful.

AIPIO. (2024). Certification and Accreditation Scheme for Australian Intelligence Professionals.

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

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

Biltgen, Patrick and Ryan, Stephen. (2015). *Activity-Based Intelligence: Principles and Applications*. Boston: Artech House.

Bruce, James B. and George, Roger. (2015). "Professionalizing intelligence analysis." *Journal of Strategic Security* 8, no. 3: 1-23. DOI: http://dx.doi.org/10.5038/1944-0472.8.3.1454

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

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

Carter, Paula, Johnstone, Jennifer, and Peterson, Marilyn (eds.). (2018). *Applications in Intelligence-Led Policing: Where Theory Meets Reality*.

European Commission. (2019). *Ethics Guidelines for Trustworthy AI*.

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

Global Justice Information Sharing Initiative. (2019). *Analyst Professional Development Road Map*.

_____. (2010). C*ommon Competencies for State, Local, and Tribal Intelligence Analysts*.

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

———. (2013). *Minimum Standards for Intermediate-Level Analytic Training Courses.*

_____. (2003). *National Criminal Intelligence Sharing Plan*.

_____. (2013). *National Criminal Intelligence Sharing Plan*. *Version 2.0.*

Global Justice Information Sharing Initiative and International Association of Law Enforcement Intelligence Analysts. (2006). *Law Enforcement Analyst Certification Standards*.

———. (2004). *Law Enforcement Analytic Standards*.

——— (2012). *Law Enforcement Analytic Standards,* 2nd edition.

Godfrey, Jr., E. Drexel and Harris, Don R. (1971). *Basic Elements of Intelligence*. Department of Justice.

Government of Canada, Intelligence Analyst Community of Practice. (2025). *The Principles of Intelligence Analysis*.

Government of Canada, Intelligence Analyst Community of Practice. Privy Council Office. (2023). *Competency Dictionary for Intelligence Analysts*.

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

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

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

Law Enforcement Intelligence Unit. (2002). *Criminal Intelligence File Guidelines*.

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

Ministry of Defence. (2023). *Intelligence, Counter-intelligence and Security Support to Joint Operations*. Joint Doctrine Publication 2-00 (JDP 2-00) (4th edition).

National Criminal Intelligence Service. (2000). *The National Intelligence Model*.

Office of the Director of National Intelligence. (2023). *Intelligence Community Directive 203 Analytic Standards*.

Peterson, Marilyn B. (1994) *Applications in Criminal Analysis*, Greenwood Press.

Pherson, Randolph H. and Heuer, Jr., Richards J. (2020). *Structured Analytic Techniques for Intelligence Analysis*, (3rd edition). CQ Press.

Ratcliffe, Jerry H. (2007). *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.

Ratcliffe, Jerry H. (2026). *Intelligence-led policing,* (third edition). New York: Routledge.

United Nations Office on Drugs and Crime (2011). *Criminal Intelligence Training Manual for Analysts*.

U.S. Department of Homeland Security, Risk Steering Committee. (2010). *DHS Risk Lexicon*.

IALEIA BOARD 2025-2027

PRESIDENT
David McClocklin, CICA

VICE PRESIDENT
Phil Powell, CICA

TREASURER
Peggy Pingel, CICA, CFE

SECRETARY
Sara Lee, CICA

DIRECTORS

CHAPTERS
Kelly Kimsey

COMMUNICATIONS
Olivia Moore

INTERNATIONAL
Milena Bruns, CICA

MEMBERSHIP
Jonathan Larkin, ThD

PARTNERSHIPS
Tracy Lempke, CICA

PROFESSIONAL STANDARDS
Joe Stobie, CICA

TRAINING AND DEVELOPMENT
Marina Cerón-Perez, CICA

Committed to the professional development of intelligence analysts and advancing analytic standards through advocacy, certification, networking, professionalism, research, and training.