

# Minimum Standards for Intermediate-Level Analytic Training Courses

October 2013





# Table of Contents

Introduction .....	5
Minimum Standards for Intermediate-Level Analytic Training Courses.....	12
Appendix A: Endnotes.....	22
Appendix B: Glossary of Terms .....	24

## About the Global Advisory Committee

The Global Advisory Committee (GAC) serves as a Federal Advisory Committee to the U.S. Attorney General. Through recommendations to the Bureau of Justice Assistance (BJA), the GAC supports standards-based electronic information exchanges that provide justice and public safety communities with timely, accurate, complete, and accessible information, appropriately shared in a secure and trusted environment. GAC recommendations support the mission of the U.S. Department of Justice, initiatives sponsored by BJA, and related activities sponsored by BJA’s Global Justice Information Sharing Initiative (Global). BJA engages GAC-member organizations and the constituents they serve through collaborative efforts, such as Global working groups, to help address critical justice information sharing issues for the benefit of practitioners in the field.

This project was supported by Grant No. 2010-MU-BX-K019 awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, in collaboration with the 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.



# Introduction

The role of the analyst<sup>1</sup> is a critical component of state, local, and tribal law enforcement agencies' crime analysis centers and intelligence units, as well as state and major urban area fusion centers, Regional Information Sharing Systems<sup>®</sup> (RISS) Centers, and High Intensity Drug Trafficking Area (HIDTA) Investigative Support Centers. Intelligence and crime analysts (herein referred to as analysts) play an integral role in law enforcement and homeland security operations, are essential to the successful completion of the intelligence and analysis process,<sup>2</sup> and provide valuable support to agency leadership, command staff, and officers on the street. Through the utilization of tactical, operational, and strategic analysis, analysts can support such agency functions as resource allocation, personnel deployment, case support, assessment development, and crime pattern and trend analysis.

As the role of the analyst continues to become institutionalized within law enforcement and homeland security agencies, a defined set of training standards is important to assist in the creation of a nationwide cadre of analysts who have comparable knowledge, skills, and expertise. Nationally recognized training standards will assist in this effort; organizations that develop and deliver analytic training would be able to use the standards as they develop intermediate-level analytic training, thereby helping to ensure continuity among training and the analytic function throughout the country. Nationally recognized training standards will also assist analysts in their professional development as well as provide agency leadership with awareness of the types of training analysts should be undergoing. Further, training standards assist analysts in meeting the competencies identified in the *Common Competencies for State, Local, and Tribal Intelligence Analysts* (Common Competencies).

Not all intermediate-level analysts will achieve the standards identified in this document. These objectives, topics, and standards are designed, rather, to ensure that training partners develop training to similar standards, creating continuity and consistency among analysts throughout the country.

To assist in the realization of these functions, the Criminal Intelligence Coordinating Council (CICC), in partnership with the U.S. Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the Office of the Director of National Intelligence (ODNI)—based on recommendations from the Global Justice Information Sharing Initiative (Global) Advisory Committee (GAC), a Federal Advisory Committee to the U.S. Attorney General—developed the following minimum standards for intermediate-level analytic training courses.

## Purpose

The purpose of this document is to articulate minimum training standards to ensure continuity and consistency among training courses developed for intermediate analysts, as well as to create parity of knowledge, skills, and abilities of these analysts. The resource identifies nationally recognized training standards and objectives and topics that training partners should utilize as they develop intermediate-level training courses. As an example, a training course focused on intermediate-level report writing should review and integrate the topics and standards identified in Objective V, “Communicating analytic observations and judgments and generating analytic products.” The standards identified in this document should also be applied to analyst training programs that include a mission-specific focus, such as organized and enterprise crime, gang activity, and financial crimes, as well as courses focused on terrorist activity.<sup>3</sup>

This resource should also be used by agency leadership in determining the types of training courses that are appropriate for intermediate analysts. For instance, a supervisor who is planning to send an analyst to training on analytic tradecraft should compare potential training courses against the objectives, topics, and standards identified under Objective IV, “Fusing intelligence and law enforcement analytic tradecraft in a law enforcement or homeland security environment.” Ensuring that training partners develop courses that incorporate these objectives, topics, and standards and recommending that analysts attend courses that adhere to these concepts will further support the realization of a nationwide law enforcement analytic capability.

These minimum training standards may also be used with other career development tools and processes as a component of an analyst career progression road map. This document and its components are designed to build upon basic analytic training, improving the knowledge, skills, and abilities of analysts; they are not intended to represent standards or criteria for promotion. The information provided should serve as guidelines and tools to help intermediate-level analysts develop appropriate analytic skills and abilities and succeed in their positions.<sup>4</sup> As a part of this use, agency leadership should review the objectives, topics, and standards identified in this document to determine which are relevant to the agency mission. Training delivery methods, as well as the number of hours dedicated to a topic, should be based on organizational goals.



## Audience

The primary audience for this resource is training providers, who should use this document as they develop and deliver intermediate-level training to analysts or personnel performing an analytic function.

In addition to training providers, analyst supervisors and agency leadership should use this document to determine relevant intermediate-level training courses for their intermediate-level analysts. Analyst supervisors and analysts may also use these training standards to identify current competency levels and training gaps and also create professional development plans for analysts, based on agency needs and mission.

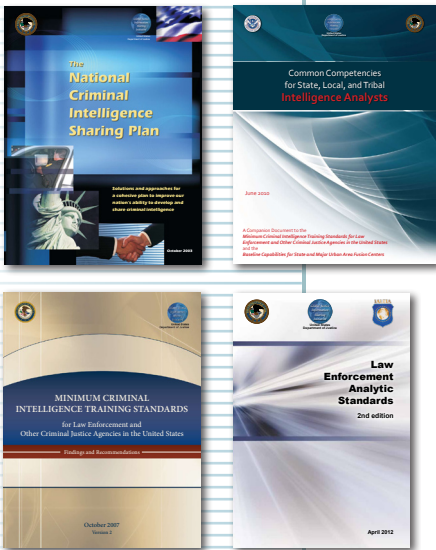
## Background

The analytic component is integral in the prevention and investigation of criminal activity and/or acts of terrorism. According to the *National Criminal Intelligence Sharing Plan* (NCISP),<sup>5</sup> the analyst's role is to collect, evaluate, analyze, and disseminate information in support of specific agency collection requirements or operations. In this role, analysts can support the prevention mission by facilitating the process of transforming data and information into timely, relevant, and comprehensive intelligence and information. By utilizing a wide array of sources of information, analysts create a multitude of tactical, operational, and strategic intelligence products, such as threat and risk assessments, intelligence reports, tactical response products, and reports on jurisdictional crime trends. These resources help guide law enforcement and homeland security operations in many ways, including threat mitigation, investigative strategy development, case development and support, situational awareness, long-term planning, and resource allocation.

Training is a foundational element for developing analytical capabilities; when combined with practical experience, it enables an analyst to apply analytical processes to provide support to the fullest extent possible. Training, coupled with the application of critical-thinking skills, enhances analytic capability, resulting in the successful execution of analytical functions and improved development of sound, well-reasoned, informative, timely, and actionable analytic products. Further, training enhances the ability of an analyst to support partners at all levels of government to more effectively identify and prioritize threats while framing them within the context of their geographic areas of responsibility (AORs).

As the role of the analyst continues to be institutionalized within law enforcement and homeland security agencies, nationally recognized training standards are needed to ensure the development and delivery of relevant, consistent, and quality training to all analysts. In addition to this continuity, training standards can provide agency leadership with an awareness of the type(s) of training analysts should undergo and also assist supervisors in developing analyst progression plans and performance evaluations. However, it is important to note that minimum training standards are designed to be primarily used for the development of training and not as performance measures for intermediate-level analysts (not all intermediate analysts will meet minimum training standards).

**It is important to note that minimum training standards are designed to be primarily used for the development of training and not as performance measures for intermediate-level analysts (not all intermediate analysts will meet minimum training standards).**



The 2003 NCISP began the effort to develop nationally recognized training standards through the identification of core criminal intelligence training standards for different levels of law enforcement, including standards for the intelligence analyst. These core standards led to the development of the *Minimum Criminal Intelligence Training Standards for Law Enforcement and Other Criminal Justice Agencies in the United States* (initially released in 2004 and updated in 2007), which identifies the minimum training standards for a basic intelligence analyst curriculum. These training standards also were incorporated into various other national resources, including the *Law Enforcement Analytic Standards*,<sup>6</sup> as well as many basic/fundamental analyst training programs. In addition to these intelligence-based training products, other tools and resources have been developed for the analysis function, such as the identification of a crime analysis skill set as well as core training curricula.<sup>7</sup>

To build on the basic minimum training standards and objectives designed to support the role of the analyst, the *Common Competencies for State, Local, and Tribal Intelligence Analysts* (Common Competencies)<sup>8</sup> was released in 2010. The common competencies identified in this document resulted from a crosswalk of state, local, and tribal law enforcement analyst training, guidance documents, and standards with those of the federal Intelligence Community (IC). The Common Competencies document builds on the standards identified in the NCISP, the *Minimum Criminal Intelligence Training Standards*, and the *Law Enforcement Analytic Standards* and identifies common analytic competencies that should be exhibited by all analysts, whether working in a fusion center, a crime analysis center, or other similar task force environment. The competencies identified are essential to enable analysts to effectively perform their job duties and are integral to their unique operating environments.





After the release of the Common Competencies, it became evident that additional, enhanced training standards were necessary to support the increasing role of analysts in crime prevention, mitigation, and investigation. The training standards should be built on the minimum standards developed for basic analyst training courses<sup>9</sup> by focusing on standards for analysts who have mastered the basic analytic competencies. Additionally, these standards should incorporate the relevant competencies and behavioral indicators identified in the Common Competencies and comparable abilities for crime analysts. The goal of this effort would be to create a comprehensive set of resources that tie together state, local, tribal, and federal requirements and training objectives, further aiding and supporting the institutionalization of the comprehensive analytic profession. The need for these training standards has resulted in this document.

## Methodology

The *Minimum Standards for Intermediate-Level Analyst Training Courses* was developed collaboratively by state, local, and tribal practitioners; training providers; law enforcement and intelligence agency leadership and analytic supervisors; and federal partners, including agencies in the Intelligence Community.<sup>10</sup> The purpose of this collaboration was to ensure a comprehensive set of training standards and objectives that are relevant to training partners who develop intermediate-level analyst training, as well as to analysts in the field, analyst supervisors, and agency leadership.

During the development of these standards, a number of topics were addressed, including the recommended number of analytic professional development and training levels.<sup>11</sup> As a result of the discussions among partners, three analyst progression levels were identified; these three levels incorporate the core competencies and indicators identified in the Common Competencies. Even though some agencies may have different levels of development, these three levels are broad enough for many state, local, and tribal agencies to incorporate. The three levels include:

- **Basic:** entry-level or apprentice
- **Intermediate:** practitioner and/or experienced analyst
- **Advanced:** lead/supervisory analyst and/or topic specialization

These three analyst levels reflect the levels of the minimum training standards. The basic level incorporates those standards identified in the *Minimum Criminal Intelligence Training Standards* and the *Law Enforcement Analytic Standards*. The intermediate level focuses on the standards and objectives identified in this document. It is important to note that intermediate-level analysts will not achieve all of these objectives and standards; rather, this resource focuses on ensuring continuity and consistency in analytic training. The advanced analytic training standards will be identified in a future resource. The culmination of the knowledge, skills, and abilities within these three progression levels combined with applied training standards will result in an analyst professional development road map.

## Analyst Progression Levels

A necessary component of minimum standards for the identification of intermediate-level analytic training is the understanding of the three analyst progression levels (basic, intermediate, advanced) and how the training standards apply to each training level. The three progression levels build on each other, and each level has a set of independent core competencies and behavioral indicators. Professional development consists not only of training but also of recognition within the agency of analytic professionalism and proficiency.

### Basic

An analyst at the basic, or entry, level is just beginning in the analytic field and should seek a foundational understanding of basic crime and/or intelligence standards and concepts, including an understanding of the handling and use of law enforcement, criminal, and intelligence information. An analyst at the basic level should attend training courses that cover the fundamentals of crime and/or intelligence analysis necessary for every step of the intelligence cycle: planning and direction, collection, processing and collation, analysis, dissemination, and reevaluation/assessment. Such fundamental analysis includes, but is not limited to, understanding information sources; privacy, civil rights, and civil liberties issues; analytical techniques; developing assessments; and product dissemination. The *Minimum Criminal Intelligence Training Standards for Law Enforcement and Other Criminal Justice Agencies in the United States* and the *Law Enforcement Analytic Standards* are the foundation for the basic-level analytical training.

### Intermediate

Intermediate-level analysts should focus on refining their ability to perform specialized analyses, generate strategic assessments, and present analytic findings to various audiences and should begin to develop expertise in a specific subject-matter area. Intermediate-level analysts should also have a more in-depth understanding of the analyst's role, function, and critical-thinking techniques, dependent on the role of the analyst within his or her organization. Intermediate analysts also begin to build leadership skills and may also serve as a mentor to new analysts, provide on-the-job training to other analysts, and assist in the creation of professional development plans.

### Advanced

Advanced-level analysts should possess the skills necessary to oversee a wide range of analytic activities in a lead or supervisory role. Analysts at this level may also serve as recognized subject-matter experts in an analysis specialization. Such specialization can include sex crimes, property crimes, hate crimes, terrorism, narcotics, gangs, critical infrastructure, financial crimes, cybercrimes, etc., based on the priorities of the agency or entity to which they are assigned.

## Analyst Certification

The objectives and standards identified in this resource also may be integrated into analyst certification processes. A beneficial component of analyst professionalization is certification, and these standards can support the development of certification qualifications. The *Law Enforcement Analytic Standards* includes a standard regarding certification, and in 2006, the *Law Enforcement Analytic Certification Standards* identified a recommended certification process for agencies and organizations. Entities seeking to develop or enhance a certification program should reference and incorporate these resources, as well as the *Minimum Standards for Intermediate-Level Analyst Training Courses*, into the certification process. In addition, training providers who desire to have their programs meet analyst certification standards should adhere to the training objectives identified in this document.

The International Association of Law Enforcement Intelligence Analysts (IALEIA)<sup>12</sup> and the International Association of Crime Analysts (IACA) both have international certification programs; agencies should review these certification programs (and programs such as state-centric certification programs) as they develop and institutionalize an analysis component.

The minimum standards for the intermediate-level analyst training reflect the various areas and competencies that are applicable to an intermediate-level analyst, depending on the agency focus and mission and the role of the analyst within the agency.

The training standards are not intended to be utilized as a listing of the skills and abilities necessary for an intermediate-level analyst but rather to provide objectives, topics, and standards for training partners as they develop specific and specialized training for the intermediate-level analyst.

Additionally, as analysts or supervisors evaluate courses to attend, the objectives of the proposed course should be evaluated against the standards and objectives identified in this document to ensure that comparable topics are addressed.

**The training standards are not intended to be utilized as a listing of the skills and abilities necessary for an intermediate-level analyst but rather to provide objectives, topics, and standards for training partners as they develop specific and specialized training for the intermediate-level analyst.**

# Minimum Standards for Intermediate-Level Analytic Training Courses

The following seven objectives have been identified to meet minimum standards for intermediate-level analytic training courses.

Objective I	Ensuring the protection of privacy, civil rights, and civil liberties
Objective II	Thinking critically within the intelligence and analysis process
Objective III	Understanding the importance of sharing information and collaborating in a law enforcement or homeland security environment
Objective IV	Fusing intelligence and law enforcement analytic tradecraft in a law enforcement or homeland security environment
Objective V	Communicating analytic observations and judgments and generating analytic products
Objective VI	Making concepts and principles actionable
Objective VII	Developing leadership and project management skills

## Exercises

It is recognized that a key component of training is the application of concepts to demonstrate proficiency. Consequently, intermediate analyst training courses should include real-world exercises that demonstrate attendee understanding and application of the concepts learned. Exercises may include hands-on practice that will enable analysts to sharpen writing and editing skills, learn how to express uncertainties, and improve the presentation of analytical findings.

Topics	Standard
<p><b>Privacy, civil rights, and civil liberties protections</b></p>	<ul style="list-style-type: none"> <li>• Understand the importance of privacy, civil rights, and civil liberties protections</li> <li>• Understand the implications of not protecting privacy, civil rights, and civil liberties</li> <li>• Understand privacy, civil rights, and civil liberties problems in regards to law enforcement standards, investigations, and criminal evidence</li> <li>• Identify personally identifiable information (PII) and its utilization within the analytical profession</li> <li>• Identify state, local, and federal agency privacy laws, policies, and procedures and their application in the analytic process</li> </ul>
<p><b>Implementation of privacy, civil rights, and civil liberties protections</b></p>	<ul style="list-style-type: none"> <li>• Learn about privacy-related tools that address implementation of privacy, civil rights, and civil liberties protections and products</li> <li>• Navigate the <a href="http://www.it.ojp.gov/privacyliberty">www.it.ojp.gov/privacyliberty</a> Web portal and understand its value to law enforcement and homeland security personnel</li> <li>• Discuss the importance of training agency personnel and law enforcement, homeland security, and public safety partners on privacy-related topics</li> </ul>
<p><b>Privacy, civil rights, and civil liberties and the intelligence cycle</b></p>	<ul style="list-style-type: none"> <li>• Identify privacy, civil rights, and civil liberties implications in:                         <ul style="list-style-type: none"> <li>• Collection of information</li> <li>• Review of information</li> <li>• Storage of information</li> <li>• Report writing</li> <li>• Dissemination of information and products</li> </ul> </li> </ul>



## Objective II

Thinking critically within the intelligence and analysis process.

Topics	Standard
<b>Critical thinking</b>	<ul style="list-style-type: none"><li>• Understand crime and intelligence analysis development methods</li><li>• Evaluate the quality of thinking and analytic processes through comparisons with established standards</li><li>• Overcome mental mind-sets and avoid common fallacies in the selection and use of data and the development of arguments and conclusions</li><li>• Structure arguments and findings that have clear and meaningful conclusions and are supported by logical claims and relevant data</li><li>• Account for inconsistent data</li><li>• Identify, task, access, and evaluate sources of information for validity and relevance in reducing uncertainty and filling knowledge gaps</li><li>• Describe quality and reliability of underlying sources</li><li>• Understand caveats and express uncertainties or confidence in analytic judgments</li><li>• Analyze the process of thinking</li><li>• Distinguish between thinking and reasoning</li></ul>
<b>Logic and inference development</b>	<ul style="list-style-type: none"><li>• Develop and offer analytical conclusions independently and collaboratively<ul style="list-style-type: none"><li>• Systematically challenge key assumptions</li></ul></li><li>• Generate and test multiple hypotheses and conclusions</li><li>• Understand the importance of incorporating alternative analysis into products</li><li>• Distinguish between underlying intelligence and analysts' assumptions and judgments</li></ul>

Topics	Standard
<p><b>Role of state, local, and tribal partners in the Information Sharing Environment (ISE)</b></p>	<ul style="list-style-type: none"> <li>• Understand the roles and functions of state, local, and tribal law enforcement agencies and the importance of including them in sharing efforts</li> <li>• Understand the roles and responsibilities of state, local, and tribal intelligence and crime analysis in the ISE<sup>14</sup></li> <li>• Understand the differences and similarities between national intelligence, law enforcement intelligence, and other types of intelligence (e.g., military)</li> <li>• Learn about the purpose and function of the Intelligence Community (IC)</li> <li>• Understand the role of state, local, and tribal agencies in the IC</li> <li>• Understand the purpose and role of the domestic network as it relates to information and intelligence sharing</li> <li>• Learn about the Office of the Director of National Intelligence’s (ODNI) Analytic Standards</li> <li>• Understand the role and functions of the U.S. Department of Homeland Security (DHS), the U.S. Department of Justice, the Federal Bureau of Investigation (FBI), ODNI, and other federal partners in information sharing efforts</li> </ul>
<p><b>Collaboration and sharing information</b></p>	<ul style="list-style-type: none"> <li>• Understand how relationships enhance collaboration and information sharing</li> <li>• 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</li> <li>• Collaborate across organizational and functional boundaries to share analytic work, avoid duplication, and increase analytic impact</li> <li>• Deconflict analytic viewpoints/conclusions</li> <li>• Understand where and how to collect information, including open source, secondhand sources, primary sources, and confidential sources</li> <li>• Understand the need and purpose of local and regional information sharing and analysis</li> </ul>

## Objective III—(continued)

Topics	Standard
<b>Security considerations regarding handling, storage, and retention of information</b>	<ul style="list-style-type: none"><li>• Store and maintain information for maximum use, including ensuring that documents are appropriately marked with caveats and restrictions</li><li>• Apply legal, privacy, civil rights, civil liberties, and security guidelines; restrictions; and operational privacy and security practices to information sharing, storage, and analysis</li><li>• Understand the role of security officers and their responsibility in the protection of information</li><li>• Understand the policies and protocols for receiving, handling, storing, and disseminating classified and unclassified information (e.g., For Official Use Only [FOUO], Law Enforcement Sensitive [LES])</li></ul>
<b>Incorporating technology into information sharing and collaboration</b>	<ul style="list-style-type: none"><li>• Identify and understand available technologies to enable exchange and collaboration and publish content</li></ul>

Topics	Standard
<p>Using structured analytic techniques and tools</p>	<ul style="list-style-type: none"> <li>• Analyze different homeland security, law enforcement, and non-law enforcement data and trends (both tactical and strategic), including:                             <ul style="list-style-type: none"> <li>• Demographic analysis</li> <li>• Financial analysis</li> <li>• Association analysis</li> <li>• Process flows</li> <li>• Geospatial analysis</li> <li>• Forecasting/predictive analysis</li> <li>• Criminal activity analysis</li> <li>• Target analysis</li> </ul> </li> <li>• Learn about various structured analytic techniques and tools, including:                             <ul style="list-style-type: none"> <li>• Collection plans</li> <li>• Frameworks and issue definition</li> <li>• Data visualization</li> <li>• Idea generation, including techniques such as problem-solving analysis</li> <li>• Indicators and scenarios</li> <li>• Hypothesis generation                                     <ul style="list-style-type: none"> <li>• Hypothesis testing, including Analysis of Competing Hypotheses (ACH)</li> </ul> </li> <li>• Assessing cause and effect</li> <li>• Challenge analysis (such as the Delphi method)</li> <li>• Conflict management (between competing hypotheses and/or recommendations)</li> <li>• Decision support, including techniques such as strengths, weaknesses, opportunities, and threats (SWOT) analysis</li> <li>• Evidence-based scenarios</li> </ul> </li> <li>• Comprehensively integrate and apply available tools (including software) to techniques identified above</li> <li>• Leverage analytic software, tools, and techniques in the development of products<sup>15</sup></li> <li>• Evaluate the quality of the application of analytic techniques</li> <li>• Apply the intelligence and analysis cycle in agency operations</li> <li>• Use of open sources: review available sources, search the Internet, use public and commercial databases, and assess validity and value                             <ul style="list-style-type: none"> <li>• Layering of social media sites and information with conventional information sources</li> </ul> </li> <li>• Anticipate change and seek new insights and innovative solutions through creative use of data and imagination techniques</li> </ul>

## Objective IV—(continued)

<b>Conceptual understanding of threat and risk assessments</b>	<ul style="list-style-type: none"><li>• Define, anticipate, assess, and communicate risks and threats</li><li>• Produce threat, vulnerability, and consequence assessments at a level of generality/complexity commensurate to expectations of an intermediate analyst</li><li>• Make recommendations to mitigate risks</li></ul>
<b>The suspicious activity reporting (SAR) process</b>	<ul style="list-style-type: none"><li>• Collect, vet, and disseminate SARs, as appropriate, according to Information Sharing Environment standards<sup>16</sup></li><li>• Use analytic techniques to identify trends, patterns, or other linkages</li><li>• Utilize SAR information as a source when identifying and monitoring significant trends and patterns</li><li>• Understand how collection plans can support the SAR process</li></ul>



Topics	Standard
<p><b>Analytic products development</b></p>	<ul style="list-style-type: none"> <li>• Ensure that analytic products are relevant to customer needs                             <ul style="list-style-type: none"> <li>• Highlighting relevance to the customer (e.g., single agency, U.S. national security)</li> </ul> </li> <li>• Know the types of analytic products and discern which product is appropriate. Products will range from tactical to operational to strategic and will include commonly used formats, such as, but not limited to:<sup>17</sup> <ul style="list-style-type: none"> <li>• Intelligence, tactical, and crime bulletins</li> <li>• Intelligence reports</li> <li>• Assessments (strategic, intelligence, threat, crime, etc.)</li> <li>• Intelligence briefings</li> <li>• Problem-solving projects</li> </ul> </li> <li>• Produce analytic reports to support investigations or prosecutions</li> <li>• Highlight consistency with or alteration from prior reports or products</li> <li>• Articulate assessments, recommendations, and next steps in reports, other analytic products, and briefings</li> <li>• Develop techniques for conceptualizing papers, answering questions, and producing products when resources and information are limited</li> <li>• Frame critical issues and complex scenarios for resolution and action by decision makers</li> <li>• Identify, interpret, and reference data and data sources (such as law enforcement information versus open source information)<sup>18</sup></li> <li>• Coordinate the product with other appropriate partners                             <ul style="list-style-type: none"> <li>• Joint-seal documents</li> </ul> </li> <li>• Mark and disseminate the product</li> </ul>
<p><b>Communicating analytic observations and judgments</b></p>	<ul style="list-style-type: none"> <li>• Assess the criticality and urgency of new information or identify trends and communicate subsequent analytic findings and recommendations to tactical operators and key strategic decision makers and stakeholders</li> <li>• Transform customer needs into criminal information or intelligence requirements</li> <li>• Write a product                             <ul style="list-style-type: none"> <li>• For external release</li> <li>• For internal agency reporting</li> </ul> </li> <li>• Know and implement the review-and-approval process                             <ul style="list-style-type: none"> <li>• Document the review of the product</li> </ul> </li> <li>• Use presentation and publisher software</li> <li>• Brief the product                             <ul style="list-style-type: none"> <li>• Oral presentations/briefings to peers, command staff, line officers, and prosecution</li> </ul> </li> <li>• Follow up on the product, seek and incorporate feedback, and measure its impact</li> <li>• Learn to craft effective source summary statements</li> </ul>

Topics	Standard
<p><b>Topic area initial subject-matter expertise</b></p>	<ul style="list-style-type: none"> <li>• Learn how to develop and write a collection plan</li> <li>• Analyze local, regional, state, national, and international issues related to threat and risk with a nexus to law enforcement and homeland security, including, but not limited to:               <ul style="list-style-type: none"> <li>• Border protection and infiltration</li> <li>• Critical infrastructure and key resources</li> <li>• Cybersecurity and high-tech/electronic crime</li> <li>• Emergency management</li> <li>• Financial crime</li> <li>• Gangs</li> <li>• Human trafficking</li> <li>• Narcotics and drug trafficking</li> <li>• Public health and safety</li> <li>• Strategic criminal threats</li> <li>• Suspicious activity reports</li> <li>• Terrorism</li> <li>• Threat financing</li> <li>• Transnational crime</li> <li>• Violent criminal activity</li> <li>• Weapons of mass destruction proliferation</li> <li>• Burglary</li> <li>• Robbery</li> <li>• Sex offenders</li> <li>• Homicide</li> <li>• Geographic profiling</li> </ul> </li> <li>• Understand correlations between different types of criminal activity (i.e., precursor crimes and terrorism)</li> </ul>

Topics	Standard
<p><b>Performance measurement</b></p>	<ul style="list-style-type: none"> <li>• Anticipate change and seek new insights and innovative solutions for challenges</li> <li>• Evaluate the quality of analytic performance and management</li> <li>• Share best practices in homeland security and law enforcement criminal information and intelligence output and impact</li> </ul>
<p><b>Project management</b></p>	<ul style="list-style-type: none"> <li>• Independently or collaboratively make recommendations and incorporate research toward the design and content of analytic approaches, collection plans, and priority information sharing needs for homeland security and law enforcement issues that balance short-term response with long-term value</li> <li>• Manage projects, time, and competing priorities</li> <li>• Coordinate and participate in the development, review, and delivery of a product</li> </ul>
<p><b>Leadership</b></p>	<ul style="list-style-type: none"> <li>• Coach analysts to help identify the skills and capabilities they already have and enable them to use those skills and capabilities to the best of their ability</li> <li>• Mentor and help guide less experienced analysts by answering questions, encouraging ongoing learning, and providing support to encourage professional development</li> <li>• Build professional contact networks and promote networking opportunities for analysts</li> <li>• Encourage analysts to obtain professional certification from a recognized professional association</li> <li>• Join and encourage membership in professional associations</li> </ul>

## Appendix A—Endnotes

- 1** In the context of this document, “analyst” may refer to state, local, and tribal crime and intelligence analysts as well as to federal analysts operating in a task force intelligence environment.
- 2** For the purpose of this resource, the intelligence and analysis process refers to the intelligence cycle identified in the *National Criminal Intelligence Sharing Plan*, page 3.
- 3** A glossary of terms, defining many of the terms addressed in this document, is located at the end of the document.
- 4** Based on recommendations from the Criminal intelligence Coordinating Council and the Global Justice Information Sharing Initiative (Global) Advisory Committee (GAC), an *Advanced Analytic Minimum Training Standards* document will be developed, which will build upon the *Minimum Criminal Intelligence Training Standards for Law Enforcement and Other Criminal Justice Agencies in the United States* and the *Minimum Standards for Intermediate-Level Analyst Training Courses* and will incorporate the competencies and behavioral indicators identified in the *Common Competencies for State, Local, and Tribal Intelligence Analysts*.
- 5** 2003 *National Criminal Intelligence Sharing Plan*.
- 6** The *Law Enforcement Analytic Standards* was updated in 2012 and is available at <https://it.ojp.gov/gist/Document/91/Law-Enforcement-Analytic-Standards>.
- 7** Additional information on the International Association of Crime Analysts (IACA) crime analysis skill set and training curricula is available at [www.iaca.net](http://www.iaca.net).
- 8** The *Common Competencies for State, Local, and Tribal Intelligence Analysts* is available at [www.it.ojp.gov](http://www.it.ojp.gov).

**9** As identified in the *Minimum Criminal Intelligence Training Standards for Law Enforcement and Other Criminal Justice Agencies in the United States*.

**10** Additional information on the Intelligence Community is available at <http://www.intelligence.gov/about-the-intelligence-community/>.

**11** Based on discussions and feedback from practitioners and training partners, it was determined that this document will identify neither recommended minimum training hours nor an experience timeline (because of the differences in promotional requirements among and between state, local, and tribal agencies).

**12** Additional information on IALEIA is available at [www.ialeia.org](http://www.ialeia.org).

**13** While privacy, civil rights, and civil liberties protections are addressed throughout the intermediate analytic standards, an objective focusing on these protections is important to all training related to criminal intelligence. This objective is designed to provide an in-depth understanding regarding what these protections are and how they should be applied throughout the intelligence and analytical processes.

**14** See the Intelligence Reform and Terrorism Prevention Act of 2004, specifically Titles I through V. Available online at <http://www.gpo.gov/fdsys/pkg/BILLS-108s2845enr/pdf/BILLS-108s2845enr.pdf>.

**15** Examples of analytic software are identified in the *Analyst Toolbox*, available at <http://www.it.ojp.gov/docdownloader.aspx?ddid=1284>.

**16** Part B of the ISE-SAR Functional Standard identifies the behaviors and indicators associated with SARs that may have terrorism implications. The Functional Standard is available at [http://nsi.ncirc.gov/documents/ISE-FS-200\\_ISE-SAR\\_Functional\\_Standard\\_V1\\_5\\_Issued\\_2009.pdf](http://nsi.ncirc.gov/documents/ISE-FS-200_ISE-SAR_Functional_Standard_V1_5_Issued_2009.pdf).

**17** Additional types of analytic products are identified in *Applications in Criminal Analysis: A Sourcebook*. Other types include activity flowchart, assessments, association chart, association matrix, bar charts, biographical sketches, briefings, charts, chronological table, commodity flowchart, commodity flow matrix, composite table, conclusion, crime bulletin, databases, event flowchart, fact pattern, financial summary, forecast, frequency distribution, graphic flowchart (map), inference development, maps, pie chart, premonitory, probability factor, profile, recommendations, report, summary, table, telephone record chart, telephone record matrix, threat assessment, timeline, trend, VIA chart, vulnerability assessment, and warning.

**18** The term “data sources” refers to the various sources of information analysts may utilize as they develop analytical products, resources, reports, and briefings.



## Appendix B—Glossary of Terms

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

**Analysis of Competing Hypotheses (ACH):** An eight-step procedure to help analysts make judgments on important issues requiring careful weighing of alternative explanations or conclusions. The process leaves an audit trail to show what analysts considered and how they arrived at their judgment.

**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 determine 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/Link Analysis:** Collection and analysis of information that indicates relationships among varied individuals suspected of involvement in criminal activity, provision of insight into the criminal operation, and identification of the most effective investigative strategies.

**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.

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

**Critical Infrastructure/Key Resources:** The assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof.

**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.

**Cybersecurity:** Improving resiliency and reducing threats related to computers or computer networks.

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

**Data Sources:** Various sources of information that analysts may utilize as they develop analytical products, resources, reports, and briefings.

**Delphi Method:** A method developed by the RAND Corporation that entails a group of experts who anonymously reply to questionnaires and subsequently receive feedback in the form of a statistical representation of the "group response," after which the process repeats itself. The goal is to reduce the range of responses and arrive at something closer to expert consensus.

**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.

**Emergency Management:** The coordination and integration of all activities necessary to build, sustain, and improve the capabilities to prepare for, respond to, recover from, or mitigate against threatened or actual disasters or emergencies, regardless of cause.

**Evaluation:** An assessment of the reliability of the source and the 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.

**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.

**Human Trafficking:** The recruitment, transportation, transfer, harboring, or receipt of persons by means of the threat or use of force or other forms of coercion, abduction, of fraud, deception, the abuse of power or a position of vulnerability, or the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation.

**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 not subjected to analysis, often referred to as "knowledge in raw form."

**Intelligence:** Information plus 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.

**Operational Intelligence:** Intelligence that details patterns, modus operandi, and vulnerabilities of criminal organizations but is not tactical in nature.

**Personally Identifiable Information (PII):** Any information that permits the identity of an individual to be directly or indirectly inferred, including any information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, a lawful permanent resident, a visitor to the United States, or an employee or contractor of the government.

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

**Risk Analysis/Assessment:** An evaluation of untoward outcomes from an incident, event, or occurrence. The analysis 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 preventive 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.

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

**Suspicious Activity Reporting (SAR):** Official documentation of observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity.

**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.

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

**Threat Financing:** A term used to encompass various types of financing that support activities harmful to U.S. national security.

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



