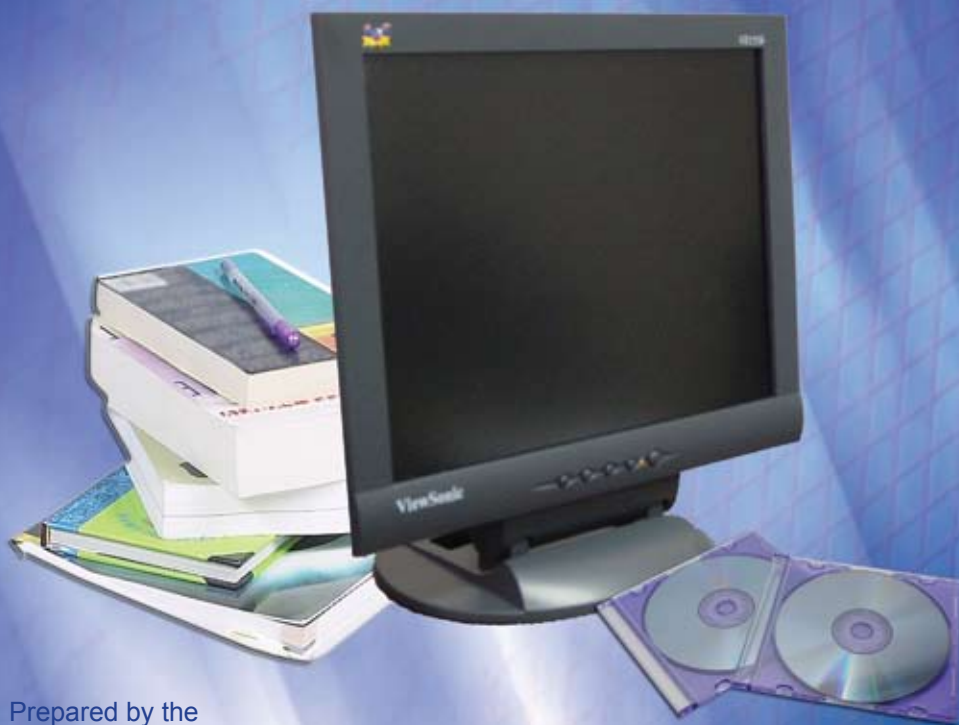




United States
Department of Justice

Analyst Toolbox

A Toolbox for
the Intelligence Analyst



Prepared by the
U.S. Department of Justice's Global Justice Information
Sharing Initiative Intelligence Working Group

About Global

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



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

Introduction and Background



There is a wide range of software available on the market to support intelligence analysis. In order to meet the challenges facing law enforcement today, it is important that intelligence professionals be equipped with the right tools to effectively and efficiently perform their duties and produce meaningful and useful intelligence products. The tools examined in this document represent the basic toolbox that the intelligence analyst will need to provide the vital intelligence service that is expected in today's law enforcement environment.

The *National Criminal Intelligence Sharing Plan* (NCISP)¹—endorsed by the U.S. Department of Justice (DOJ), the U.S. Department of Homeland Security (DHS), and many different law enforcement organizations—contains 28 recommendations for local, state, tribal, and federal law enforcement agencies to implement in order to improve the quality of criminal intelligence in the United States. Two of the recommendations of the NCISP address the need to properly equip those persons involved in intelligence analysis:

- Recommendation 12: The International Association of Law Enforcement Intelligence Analysts (IALEIA) should develop, on behalf of the CICC (Criminal Intelligence Coordinating Council), minimum standards for intelligence analysis to ensure intelligence products are accurate, timely, factual, and relevant and recommend implementing policy and/or action(s). Law enforcement agencies should adopt these standards as soon as developed and approved by the CICC.
- Recommendation 28: The CICC, in conjunction with the Office of Justice Programs (OJP) and the connected sensitive but unclassified systems, shall develop an acquisition mechanism or centralized site that will enable law enforcement agencies to access shared data visualization and analytic tools. The CICC shall identify analytical products that are recommended for use by law enforcement agencies

¹ Available at www.it.ojp.gov/documents/NCISP_Plan.pdf.

in order to maximize resources when performing intelligence functions, as well as a resource list of current users of the products.

Pursuant to Recommendation 12, IALEIA developed the *Law Enforcement Analytic Standards* booklet.² This booklet provides minimum standards for intelligence analysis to ensure that intelligence products are accurate, timely, factual, and relevant. These standards were approved by DOJ's Global Justice Information Sharing Initiative (Global) Advisory Committee in September 2004. Standard 16 of the *Law Enforcement Analytic Standards* states that "Analyses shall utilize the best and most current computerized visualization and analytic tools available to the analyst."

In order to provide law enforcement decision makers with as much information as possible concerning the tools available to the analysis process, the Global Intelligence Working Group (GIWG) tasked the Connectivity/Systems Committee to develop a list of tools to fulfill the needs expressed in NCISP Recommendation 28. To begin the process, a survey was conducted among randomly selected law enforcement analytic practitioners to determine a baseline of needed tools to adequately perform the analyst function.³

Another step in the process of developing tools to aid in the analysis process was the coordination with the Office of National Drug Control Policy to modify its secure Technology Toolbox for police Web-based collaboration programs to accommodate discussion forums for analytical software. This provides a secure mechanism for law enforcement analysts to discuss "how to" issues concerning these tools. Additionally, administrators can compare various intelligence products to gauge the effectiveness of the tools and determine whether they meet the needs of the agency. The Technology Toolbox can be reached via RISSNET™.

The *Analyst Toolbox* list represents the results of extensive Web-based, open source research and the collection of systems currently utilized by local, state, tribal, and federal law enforcement agencies.

² Available at www.it.ojp.gov/documents/law_enforcement_analytic_standards.pdf.

³ The results of the survey are attached as Appendix A.

Analyst Toolbox



Word Processing

Purpose: To produce text documents, including bulletins, fact sheets, investigative summaries, and analytical reports. Analytic products should include a written report of some length and format that can be produced utilizing word processing software. In some instances, the only product of an analysis will be a written report.

Uses: Word processing software includes various formatting tools, such as footnoting, header and footer annotations, mailing labels, and correspondence formatting. This software also enables objects (photographs, graphics, tables, etc.) to be embedded in documents. Word processing software may also include editing and change tracking features for documents being modified by more than one individual.

Spreadsheet

Purpose: To organize numerical data in a column-and-row format for summarization and comparison of data and data charting.

Uses: Spreadsheets are capable of performing calculations and basic statistical computations, searches, defined filtering, and sorting of data. They are ideal for financial data storage and collation. Data can be entered by an operator or imported from files of similar structure. Additional capabilities of this tool should include the ability to generate graphs and tables to visualize data. Drawing toolbars may be used to create rudimentary link charts and flowcharts.

Relational Database

Purpose: To organize data in relation to other data in a format of records and fields arranged into several tables in order to determine commonalities and relationships among data. The relational database tool can also be used for record keeping.

Uses: Relational database software allows the option of records/fields within a database to be related to other fields (e.g., incident name, time, date, gist, and reported by). Records can be associated with other records by any of the fields (a query for records for a particular date will bring up all records associated with that date; e.g., a query for records reported by Officer Jones will retrieve all incidents reported by Jones). Likewise, tables can be related to each other through queries that connect similar fields and reduce data entry and repetition. A relational database also serves as an information management tool. User interface can be via simple forms through which data can be entered and fed directly into the database.

Mapping/Geographic Information System (GIS)

Purpose: To display geographic data using points or shapes corresponding to specific locations or areas on a map to aid in crime mapping and strategic intelligence charting.

Uses: Mapping/GIS software can aid in mapping and in the analysis of data points or areas related to crime or other patterns (dates, times, hot spots of activity, buffer zones). This software can also be used to look at patterns of movement relating to crime to delineate “hunting zones” and reduce the number of leads in predatory crimes.

Public Information Database Resources

Purpose: To provide access to compiled public data sources with one comprehensive search.

Uses: Public information records usually include personal information (address, phone number, date of birth) and asset information (real estate, vehicle, businesses). These types of databases are not considered the primary data source but are a compilation of information from other sources; therefore, the information should be verified at the primary source of the information. Law enforcement agencies may have direct access to these databases, or agencies may access this type of information through the Regional Information Sharing Systems® (RISS), Financial Crimes Enforcement Network (FinCEN), National White Collar Crime Center (NW3C), or High Intensity Drug Trafficking Areas (HIDTA).

Presentation Software

Purpose: To produce professional-looking slide show presentations, with the capability to incorporate text, photographs, graphics, and animation.

Uses: Presentation software provides not only slides but also handouts and presentation outlines that may aid in oral intelligence briefings. This tool can be used to provide a visual summary of pertinent information relating to the investigation or topic being discussed.

Graphics Software

Purpose: To illustrate concepts or conclusions using graphic arts.

Uses: Graphics software allows for cutting and pasting of information into other applications for projects beyond the graphics capability of word processing and spreadsheet software, thereby providing a complete and detailed representation of the applicable data.

PDF File Creation Software

Purpose: To allow the creation of PDF format files. PDF files can be viewed and printed on any operating system (Mac OS X®, Microsoft® Windows®, UNIX®), thereby facilitating the sharing of information.

Uses: PDF files look exactly like original documents and preserve source file information—including text, drawings, 3D, full-color graphics, and photos—regardless of the application used to create them. PDF files can also support full-text searches to locate words and phrases. This software can also be utilized to create electronic documents from paper originals.

Statistical Analysis Software

Purpose: To analyze large amounts of data to identify trends.

Uses: This software enables the user to create descriptive statistics, which in turn allows for the summarization and analysis of qualitative and quantitative data, using calculations such as frequency, percent change, mean, median, mode, and measures of variance (SD and SE). Inferential statistics are used for random sampling of populations (as in a survey) and allow the user to inferentially apply the results to the population from which the sample was drawn.

Publishing Software

Purpose: To produce professional-looking publications, such as newsletters or bulletins.

Uses: Publishing software enables the user to create publications to be distributed on a broad scale. Intelligence that is to be disseminated should be converted into a format similar to PDF to ensure that the quality of the document is not altered.

Communications/Telephone (Toll) Record Software

Purpose: To organize structured information collected from telephone billing systems (including cellular phones), pen registers, and dialed number recorders for analysis.

Uses: Communications/telephone records software aids in the analysis of communication and telephone information, including source or destination of a call; the times of calls; and the dates, frequency, sequence, patterns, and duration of calls to/from one or many telephones. With advancements in communications technologies—such as e-mail, instant messaging (IM), paging, Voice over Internet Protocol (VoIP), and direct connect technologies—software packages should be capable of dealing with nontraditional communications data elements, such as Internet Protocol (IP) addresses, e-mail addresses, direct connect private identification numbers, and IM account numbers and/or screen names.

Timeline/Flowcharting

Purpose: To display chronological events in an easy-to-understand format.

Uses: Timeline/flowcharting can support tactical or strategic planning, as well as investigations. Timeline software tools can visually show the order of events for an identified or suspected crime. Flowcharting can visually demonstrate the flow of goods within a criminal enterprise. Timeline/flowcharting can also serve administrative purposes, such as visual project tracking.

Link Analysis

Purpose: To link associated information from a structured data source and display the links between entities in a graphic display. Also useful for documenting data sources and can help find the links in a large, complex data set. This type of software can also include a timeline or flowcharting capability.

Uses: Link analysis software can visually show relationships, including association analysis and hierarchical relationships (e.g., organized crime hierarchies).

Data Mining/Text Mining

Purpose: To automate the process of determining patterns and relationships in extremely large volumes of information (either statistical or in text) too large for an individual to manage.

Uses: Data mining/text mining tools can assist in complex case management where there may be multiple targets, victims, and pieces of information related to the case. These types of tools aid in efficiently analyzing large amounts of data.

Data Visualization

Purpose: To automatically display information in formats such as graphs and pie charts. This capability can sometimes be part of a larger software application, such as spreadsheet software.

Uses: Data visualization software displays the relationships and findings in an easy-to-read format, such as link charts, flowcharts, or telephone toll-analysis charts.

Investigative Case Management

Purpose: To track investigations and leads and activities conducted in support of investigations in order to preserve a record for investigative and prosecutorial purposes, as well as to manage work flow of investigators and analysts.

Uses: Investigative case management tools provide a central repository for all information relating to a case. Users may query the system to determine whether subjects have previously been identified and current case status. This tool can also provide information and reports regarding strategic planning for law enforcement executives.

Conclusion

Each organization will have to determine the specific vendor to provide the tools listed in this report. It is important when examining these products that interoperability be considered. In order to connect the dots, law enforcement analysts must have a basic set of tools that provide the services they need and can easily communicate with each other.

Appendix A

Results of Analyst Survey to Determine Tools Needed by Analysts

November 2005



I. Hardware

- A. Computer with sufficient processing speed and hard drive capability to run high-end programs and adequate data storage/memory servers
 - 1. CD and DVD Burner capability
 - 2. Backup equipment
 - 3. Video capture capability
 - 4. Laptops if fieldwork is required
- B. Printers
 - 1. Laser for high-speed black and white with capability of printing up to 11" x 17" charts and documents
 - 2. Color printer with capability of printing up to 11" x 17" charts and documents
 - 3. Graphics plotter capable of printing large charts
- C. Document scanner with auto feed and optical character recognition (OCR) software
- D. Digital camera(s) (5-megapixel) for surveillance, target photos, and postseizure analysis
- E. Digital video camera(s)
- F. Facsimile machine
- G. Color copier
- H. Statistical calculator
- I. Projection equipment
- J. Television with cable or satellite access

II. Installed Software

- A. Word processing program
- B. Spreadsheet program
- C. Relational database
- D. Presentation software to include photo manipulation/enhancement
- E. Internet browser
- F. Flowcharting software

- G. Link analysis software
- H. Database reporting/visualization software
- I. Mapping software
- J. Photo enhancement software
- K. E-mail program to include interoffice with ability to calendar/task
- L. Desktop search engine for local and network drives
- M. Telephone analysis software
- N. Portable Document Format (PDF) creation software
- O. Security software
 - 1. Virus blockers
 - 2. Internet restriction
 - 3. Firewall
 - 4. Smart Pass or other encryption software
- P. Publication software
- Q. Statistical analysis software
- R. Data mining/text mining software

III. Access to Systems and Databases

- A. Agency records management system
- B. Agency intelligence system
- C. Direct unfiltered Internet connection
- D. State crime information system
- E. National crime information system
- F. State driver's license database
- G. Commercial databases containing personally identifying information
- H. Regional Information Sharing Systems (RISS)
- I. Law Enforcement Online (LEO)
- J. Homeland Security Information Network (HSIN)
- K. Telephone database
- L. Jail management databases
- M. Financial Crimes Enforcement Network (FinCEN)
- N. Immigration databases
- O. State wage and hour database
- P. State sex offender registries
- Q. Crime-specific listservs
- R. Really Simple Syndication (RSS) readers
- S. Intelligence center databases (state, HIDTA, EPIC, NDIC, etc.)
- T. State corrections/probation databases
- U. Juvenile justice databases
- V. Wireless Internet access
- W. Cellular telephone and PDA

For more information on the U.S. Department of Justice's
Global Initiative and its products, including those
referenced in this document, call (850) 385-0600 or visit

www.it.ojp.gov

November 2006