Networks and Systems

9

CHAPTER NINE

Networks and Systems

Essential to effective intelligence is the ability to access and share information readily. A number of resources and systems are currently available to state, local, and tribal law enforcement (SLTLE) agencies that permit access to federal intelligence products, regional and local intelligence products, current news and events, and secure email. Many resources are available to law enforcement organizations for a minimal, if any, fee. Regardless of the degree of sophistication of any system, it is essential that a law enforcement organization have some form of secure email and access to a Sensitive But Unclassified (SBU) network to receive current advisories to maximize information sharing.

Regional Information Sharing System (RISS)

RISS has been in operation since 1973 providing services supporting the investigative and prosecution efforts of law enforcement and criminal justice agencies. The network was founded in response to trans-jurisdictional crime problems and the need for cooperation and secure information sharing among law enforcement agencies.

Today, RISS is a national network comprising six multistate centers operating regionally.

- Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network (MAGLOCLEN)[158] (Delaware, Indiana, Maryland, Michigan, New Jersey, New York, Ohio, Pennsylvania, and the District of Columbia. The center also has member agencies in England, the Canadian provinces of Ontario and Quebec, and Australia)
  140 Terry Road, Suite 100
  Newton, PA 18940
  Phone: 215.504.4910
  E-mail: info@magloclen.riss.net

158 http://www.iir.com/riss/magloclen

- Mid-States Organized Crime Information Center (MOCIC) (Illinois, Iowa, Kansas, Minnesota, Missouri, Nebraska, North Dakota, South Dakota, and Wisconsin. The center also has member agencies in Canada)
  1610 E. Sunshine Drive, Suite 100
  Springfield, MO 65804
  Phone: 417.883.4383
  Email: info@mocic.riss.net

- New England State Police Information Network (NESPIN) (Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, and Vermont. The center also has member agencies in Canada)
  124 Grove Street, Suite 305
  Franklin, MA 02038
  Phone: 508.528.8200
  Email: info@nespin.riss.net

- Regional Organized Crime Information Center (ROCIC)[159] (Alabama, Arkansas, Florida, Georgia, Kentucky, Louisiana, Mississippi, North Carolina, Oklahoma, South Carolina, Tennessee, Texas, Virginia, and West Virginia, Puerto Rico, and the U.S. Virgin Islands)
  545 Marriott Drive, Suite 850
  Nashville, TN 37214
  Phone: 615.871.0013
  Email: info@rocic.riss.net

- Rocky Mountain Information Network (RMIN)[160] (Arizona, Colorado, Idaho, Montana, Nevada, New Mexico, Utah, and Wyoming. The center also has member agencies in Canada)
  2828 N. Central Avenue, Suite 1000
  Phoenix, AZ 85004
  Phone: 602.351.2320
  Email: info@rmin.riss.net

- Western States Information Network (WSIN) (Alaska, California, Hawaii, Oregon, and Washington. The center also has member agencies in Canada, Australia, and Guam)
  1825 Bell Street, Suite 205
  Sacramento, CA 92403
  Phone: 916.263.1186
  Email: info@wsin.riss.net

The regional approach allows each center to offer support services tailored to the needs of member agencies, though the centers also provide services and products that are national in scope and significance. Typical targets of RISS-member agencies' activities are terrorism, drug trafficking, violent crime, cybercrime, gang activity, and organized crime. While the RISS network is funded by the U.S. Bureau of Justice Assistance, it is controlled by its member agencies. As a result, state and local law enforcement agencies establish priorities as well as decisions related to services, such as secure client email systems.

159 http://www.rocic.com/

160 http://www.iir.com/riss/rmin

Traditional support services provided to law enforcement member agencies from the RISS centers include the following:

- Information-sharing resources
- Analytical services
- Loan of specialized investigative equipment
- Confidential funds
- Training conferences
- Technical assistance

…it is essential that a LAW ENFORCEMENT organization have some form of SECURE EMAIL and ACCESS to a SENSITIVE BUT UNCLASSIFIED (SBU) network, to receive current advisories in order to MAXIMIZE information sharing.

RISS operates a secure intranet, known as RISS.net, to facilitate law enforcement communications and information sharing nationwide. RISS local, state, federal, and tribal law enforcement member agency personnel have online access to share intelligence and coordinate efforts against criminal networks that operate in many locations across jurisdictional lines. In September 2002, the FBI Law Enforcement Online (LEO) system interconnected with RISS. In October 2003, the RISS/LEO interconnection was recommended in the National Criminal Intelligence Sharing Plan (NCISP) as the initial Sensitive But Unclassified (SBU) communications backbone for implementation of a nationwide criminal intelligence-sharing capability. The plan encourages agencies to connect their systems to RISS/LEO.

Anti-Terrorism Information Exchange (ATIX)

In April 2003, RISS expanded its services and implemented the Anti-Terrorism Information Exchange (ATIX) to provide users with access to homeland security, disaster, and terrorist threat information. RISS member

agencies as well as executives and officials from other first-responder agencies and critical infrastructure entities can access the system. ATIX consists of a website and connected services hosted on the RISS network. It is designed for use by officials from government and nongovernment organizations who are responsible for planning and implementing prevention, response, mitigation, and recovery efforts for terrorist attacks and disasters. The ATIX program serves a variety of communities such as state, county, local, and tribal government executives; federal government executives and agencies; regional emergency management; law enforcement and criminal justice organizations; fire departments; agriculture; disaster relief; special rescue units; and telecommunication and transportation.

The website (see Figure 9-1) features secure email and information such as Department of Homeland Security (DHS) bulletins and advisories, terrorist threat-level alerts, advisories from different governmental units such as the Department of Transportation, and areas where users can post and share data specific to their "occupational communities" (e.g., law enforcement, military, emergency services, etc.).

In each individual community section on the website, users can establish collaborative electronic conference services, virtual bulletin boards, and live chat rooms. Member groups also create most of the ATIX site's content and bulletin board posts. Each conference has a live chat feature where users can post conversation threads and discuss topics. An on-screen paging function permits users to notify others if they need to shift a conversation to the telephone or to a face-to-face discussion.

ATIX is informative, user-friendly, and an important resource for law enforcement agencies of any size. The site requires access to the Internet and a Virtual Private Network (VPN) to permit secure communications. To obtain access to ATIX, the potential user must contact the applicable RISS center and request enrollment from the appropriate state coordinator.

Figure 9-1: Anti-Terrorism Information Exchange (ATIX) Welcome Screen

Law Enforcement Online (LEO)[161]

161 The LEO web page is at http://www.fbi.gov/hq/cjisd/leo.htm.

LEO is an online service operated by the FBI for law enforcement, first responders, and criminal justice officials. Approximately 32,500 members have been on LEO since its inception in1995. All that is required for use is Internet access and the FBI VPN.

After logging on to the LEO site, resources that are available include:

- ***Topical Focus Area:*** Custom web-type pages that provide a secure community area for general information related to the law enforcement profession using text, graphics, audio, and video.
- ***Law Enforcement Special Interest Groups:*** Segmented areas with multilevel controlled access for specialized law enforcement groups that have their own members.
- ***Email:*** Provides the capability to send and receive secure Email/messages electronically between LEO users.

- ***News Groups:*** Provides general national and state law enforcement and special interest group bulletin boards for posting timely topical information of interest to law enforcement.
- ***Chat:*** Provides the ability to have a real-time discussion among users (through a keyboard) on three levels; one-to-one, groups, and the Electronic Academy for presentations or question and answer sessions.
- ***Feedback:*** Provides the capability to survey users for input on various topics.
- ***Electronic Calendar:*** Provides national, state, and special-interest calendars for posting upcoming dates of interest for conferences, meetings, training courses, seminars, and other important dates.
- ***Topical Electronic Library:*** Provides an easily accessed repository of a broad range of publications, documents, studies, research, technical bulletins, and reports of interest to the law enforcement community. The library will provide indexed and full-text retrieval capability. Material for this component is expected to come from the entire law enforcement and education communities.
- ***Distance Learning:*** Provides online topical learning modules that can be used any time of the day or night at the user's own pace with instructional feedback

In addition, FBI ***Intelligence Assessments***, FBI ***Intelligence Bulletins***, and FBI ***Intelligence Information Reports*** are available on the LEO website as well as other items of interest related to the FBI intelligence program. To obtain access to LEO, contact the training coordinator at the local FBI Field Office.[162]

162 http://www.fbi.gov/contact/fo/fo.htm

… FBI Intelligence ASSESSMENTS, FBI Intelligence BULLETINS, and FBI Intelligence INFORMATION REPORTS are available on the LEO WEBSITE as well as other items of interest related to the FBI intelligence program.

Law Enforcement Intelligence Unit (LEIU)[163]

Founded in 1956, the purpose of LEIU is to gather, record, and exchange confidential information not available through regular law enforcement channels, concerning organized crime and terrorism. It is an association of state and local police departments, similar in many respects to numerous other associations serving professionals. LEIU has no employees and no capability as an entity to conduct any investigation or law enforcement activity. Each member agency is bound by, and acts pursuant to, local law and its own agency regulations.

The organization is divided geographically into four zones: Eastern, Central, Northwestern, and Southwestern. Each zone elects a chair and vice chair to serve as zone officers. Internationally, LEIU elects a general chair, vice general chair, and designates a secretary-treasurer and a legal advisor who serve as international officers. The International Officers, zone officers, past general chair, and two representatives from the Central Coordinating Agency (i.e., the California Department of Justice which houses LEIU data) make up the executive board. The board is the governing body of LEIU, and, as such, establishes policy and passes on the admission of all members, and is governed by a constitution and bylaws.

163 For more information on LEIU see http://www.leiu-homepage.org/index.html. For contact information concerning LEIU membership, Email leiu@doj.ca.gov. LEIU, California Department of Justice, P.O. Box 163029, Sacramento, CA 95816-3029.

LEIU membership is limited to law enforcement agencies of general jurisdiction having an intelligence function. To become a member, an agency head submits a written application. The applying agencies must be sponsored by an LEIU member. Each member agency head appoints an LEIU representative as the contact for the Law Enforcement Intelligence Unit.

Virtually any type of information that may be lawfully retained in law enforcement intelligence records may be exchanged as long as the recipient meets the need-to-know and right-to-know standards. Importantly, to keep intelligence records consistent with legal standards, LEIU is not a computer system where members can make queries; rather, it is a network where information is exchanged between members, albeit in electronic form.

Information Sharing

To submit an inquiry about a suspected criminal to the LEIU automated system, a member agency enters the subject information through a secure intranet, which is stored on RISS.net. The subject information includes, among other items, the person's identity, criminal activity, and criminal associates. All information submitted to the LEIU Automated File must meet LEIU File Guidelines (Appendix D) and comply with 28 CFR Part 23. The submitting agency must certify that the subject meets established criteria, including criminal predicate. The Central Coordinating Agency manages this automated file.

Joint Regional Information Exchange System (JRIES)

The Joint Regional Information Exchange System (JRIES) is the secure collaborative system used by the Department of Homeland Security (DHS) Homeland Security Operations Center (HSOC) to collect and disseminate information between DHS and federal, state, tribal, and local agencies involved in counterterrorism.

- JRIES is focused on information exchange and real-time collaboration among federal, state, tribal, and local authorities.
- JRIES includes information analysis tools and capabilities to support distributed collaborative analysis and reporting across federal, state, tribal and local law enforcement and intelligence.
- JRIES meets all applicable security requirements and has achieved system accreditation by the Intelligence Community.
- JRIES currently is deployed to more than 100 federal, state, and local entities with many more connecting every month.

This communications capability delivers to states and major urban areas real-time interactive connectivity with the DHS Homeland Security Operations Center. This secure system significantly strengthens the flow of real-time threat information at the Sensitive But Unclassified (SBU) level to all users immediately, and provides the platform for future communications classified as Secret to the state level. This collaborative communications

environment, developed by state and local authorities, will allow all states and major urban areas to collect and disseminate information among federal, state, and local agencies involved in combating terrorism. Already in use in the 24/7/365 DHS Watch of the Homeland Security Operations Center, JRIES is an integrated component of the wider DHS information-sharing and collaboration architecture that will help provide situational awareness, information sharing, and collaboration across the 50 states, U.S. territories, and major urban areas. This program helps fulfill the DHS's charge to enable real-time information sharing of threats to the homeland with a variety of homeland security partners throughout the federal, state, and local levels.

JRIES is not just a communications tool but also an analytical tool for its users. Capacity of the system includes the following:

- Collaboration and analysis
- Secure email
- Interactive collaboration tool (live text or voice)
- Supports requests for information
- Link and temporal analysis
- Daily and periodic reporting
- Suspicious incident/pre-incident indicator data
- Data display on maps (national, state, county, city)
- Critical Infrastructure Protection (CIP) repository
- Strategic analysis on terrorist threats, tactics, and weapons.

Homeland Security Information Network

The next generation of JRIES is the Homeland Security Information Network (HSIN). The HSIN will deliver real-time interactive connectivity among state and local partners and with the DHS HSOC through JRIES. This increased connectivity will result in more effective communications and more efficient responses to deter, detect, prevent, or respond to terrorist actions. Information sharing to reduce vulnerabilities is an essential element of the DHS's mission, and this real-time flow of encrypted information among homeland security partners will allow federal, state, and local agencies to better perform their jobs of protecting America's hometowns.

As a foundation of the Homeland Security Information Network initiative, the broadened JRIES community of users will include the State homeland security advisors, state adjutant generals (National Guard), state emergency operations centers, and local emergency services providers including firefighters, law enforcement, and others. The expanded JRIES network will continue to support the law enforcement and intelligence counterterrorism mission, but will also provide communications, collaboration, and information sharing among DHS and federal, state, local, and tribal agencies and private-sector partners.

As a homeland security program focused on monitoring, information sharing, preventing, and responding to potential terrorist threats, the HSIN will connect to other communications tools used by law enforcement agencies. The RISS.net and LEO programs, for example, sponsored by the Department of Justice, address a much wider spectrum of criminal activity. Within the counterterrorism mission, JRIES, RISS.net, and LEO are complementary programs, and DHS will continue to work closely with law enforcement. The HSIN will post its daily reports and warnings directly to RISS.net via a JRIES interface. Combining JRIES' real-time collaboration capability and state-of-the-art portal technology with RISS.net's legacy databases will enhance the capabilities of DHS law enforcement partners.

Priority capabilities of this expanded information exchange system will include the following:

Communications

- Low-cost, always-on connectivity
- End-to-end encrypted communications.

Collaboration / Analysis

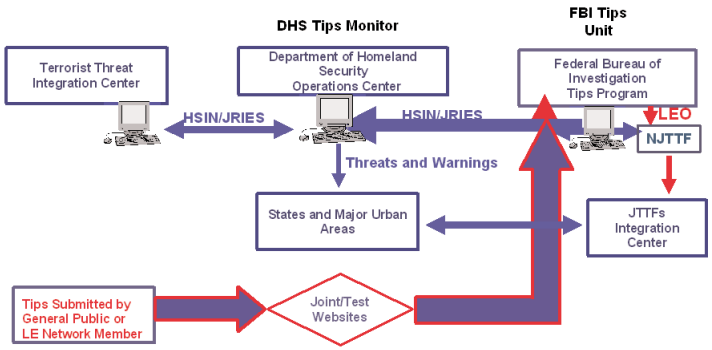
- Secure email
- Interactive collaboration tool (real-time text or voice)
- Supports requests for information, exchange, and cross-reference
- Search and link/timeline analysis, map/imagery displays.

Information

- Daily, periodic, and ongoing report sharing
- Suspicious incident/pre-incident indicator data
- Media studies and analysis
- Mapping and imaging (national, state, county, city)
- Critical Infrastructure Protection (CIP) repository
- Strategic analysis of terrorist threats, tactics, and weapons.

Figures 9-2 illustrates the intelligence interrelationship of the HSIN with other networks as well as the integration of intelligence and operations. A long-term goal of the HSIN is to have seamless connectivity among the different portals that serve the law enforcement and homeland security communities.

Figure 9-2: System Integration–HSIN Operations and Intelligence Integration



Operations – Complaint information can be addressed by FBI/JTTFs/Nationally via LEO.
Intelligence – Information flows to DHS, TTIC and FBI Tips unit simultaneously via HSIN
Universal Tips Report Number will permit tracking through Operations and Intelligence flow routes.

164 For contact information and more details, see http://www.nlets.org/default.asp.

National Law Enforcement Telecommunications System (NLETS)[164]

The National Law Enforcement Telecommunication System (NLETS) was created by state law enforcement agencies nearly 35 years ago as a primary means of integrating data related to traffic enforcement. Since its founding, the NLETS role has evolved from being primarily an interstate telecommunications service for law enforcement to a more broad-based network servicing the justice community at the local, state, and federal

levels. It is now a broad-based interstate law enforcement network for the exchange of law enforcement and related justice information. Its purpose is to provide, within a secure environment, an international criminal justice telecommunications capability that will benefit to the highest degree, the safety, security, and preservation of human life and the protection of property. NLETS will assist those national and international governmental agencies and other organizations with similar missions who enforce or aid in enforcing local, state, federal, or international laws or ordinances.

NLETS is a nonprofit corporation chartered by the states and funded by user fees collected from the membership and managed by a board of directors consisting of state police executives. Primary services include access to key state databases, particularly driver's licenses and motor vehicle records, criminal histories, and sex offender registries. The system also has access to special databases such as Canadian files, hazardous materials archives, U.S. General Services Administration fleet, immigration records, FAA registrations, NDPIX,[165] vehicle impounds, and import/export files. The system also includes terminal-to-terminal messaging and broadcast capabilities (such as an Amber Alert).

Accelerated Information Sharing for Law Enforcement (AISLE)

The next generation of NLETS is Accelerated Information Sharing for Law Enforcement (AISLE). The intent of AISLE is to accelerate information sharing for the entire U.S. law enforcement community by adopting and deploying XML[166] Web Services technology for interstate inquiries and responses. Like the Global Justice Information Sharing Initiative, it also seeks to promote the common XML standard for law enforcement information systems. Essentially, AISLE seeks to move NLETS completely into the most advanced realms of networking to enhance information sharing.

International Criminal Police Organization (INTERPOL)[167]

INTERPOL is the International Criminal Police Organization founded in 1923 to serve as a clearinghouse for information on transnational criminals. It

165 NDPIX is the National Drug Pointer Index, discussed in detail in Chapter 11.

166 Internet web pages are typically written in Hypertext Markup Language (HTML) which aids in formatting and integrating diverse resources. The second generation is XML, Extensible Mark-up Language, which has all the features of HTML and provides significantly increased searching and comparison characteristics.

167 The INTERPOL General Secretariat site is http://www.interpol.int/.

receives, stores, analyzes, and disseminates criminal data in cooperation with its 181 member countries on a 24/7/365 basis in its four official languages (English, French, Spanish, and Arabic). INTERPOL deals only with international crimes. INTERPOL's three core functions are to provide member states with the following:

1. A secure global communications system to provide the timely and effective exchange, storage, and processing of important police information to all member countries and provision of other related services including the issuing of international wanted persons notices and similar alerts.
2. Databases and analytical support, which includes the development of programs and services for police including databases on names, fingerprints, DNA, photographs, identification documents, and notices (see figure 9-3).
3. Operational police support enhancing the role of INTERPOL's National Central Bureaus and further integrating Sub Regional Bureaus into overall INTERPOL activity, including the development of relevant law enforcement initiatives in areas such as terrorism, drugs, organized crime, trafficking in human beings, child abuse images on the Internet, and financial and high-tech crime.

Criminal intelligence analysts at INTERPOL are uniquely placed to recognize and detect patterns and criminal trends from a global perspective, as well as having the resources to assist with specific international crime cases.

In the United States, the contact point for INTERPOL is the U.S. National Central Bureau (USNCB) which operates within the guidelines prescribed by the Department of Justice, in conjunction with the DHS. The mission of the USNCB is to facilitate international law enforcement cooperation as the United States representative to INTERPOL.

When INTERPOL is seeking specific information or seeking a person, it issues a color-coded “notice,” with each color representing a different type of action from the recipient agencies (Figure 9-3). While these notices are rarely encountered by SLTLE officers, it is nonetheless of value to be familiar with them should the issue arise.

Figure 9-3: INTERPOL Notices[168]

Red Notice
Used to seek the arrest with a view to extradition of subjects wanted and based upon an arrest warrant.

Yellow Notice
Used to help locate missing persons, especially minors, or to help identify persons who are not able to identify themselves; for example, a person suffering from amnesia.

Blue Notice
Used to collect additionnal information about person identity or illegal activities related to a criminal matter. This notice is primarily used for tracing and locating offenders when the decision to extradite has not yet been made, and for locating witnesses to crimes.

Black Notice
Used to seek the true identity of unidentified bodies.

Green Notice
Used to provide warnings and criminal intelligence about persons who have committed criminal offences, and are likely to repeat these crimes in other countries.

U.S. law enforcement officers can gain access to INTERPOL reports and make international inquiries by contacting their state point of contact (usually within the state law enforcement or intelligence agency) who will then query the USNCB. For reference, the USNCB address and website are:

U.S. Department of Justice
INTERPOL
United States National Central Bureau
Washington, DC 20530
http://www.usdoj.gov/usncb/index.html

168 http://www.interpol.int/public/ICPO/FactSheets/FS200105.asp

Law Enforcement Information Sharing Program

The U.S. Department of Justice is developing a new initiative called the Law Enforcement Information Sharing Program (LEISP). The initiative is designed not to create a new system, but to integrate systems and relationships that already exist. Too often both systems and initiatives operate independently. The result is that system queries and information dissemination are not comprehensive.

The LEISP plans to implement policies, practices, and technologies to ensure that each component of the Department of Justice share information as a matter of routine across the entire spectrum of the law enforcement community at all levels of government. The intent of the program is to ensure that law enforcement information-sharing practices in the Department of Justice are consistent with the NCISP. Moreover, the program should significantly enhance the amount and quality of intelligence that is shared with SLTLE agencies.

Regional Intelligence Centers[169]

Regional Intelligence Centers (RIC) take many forms throughout the United States. There is currently no one model for what an intelligence center does or how it should be organized. Rather, they have evolved, largely based on local initiatives, as a response to perceived threats related to crime, drug trafficking, and/or terrorism. The intent is to marshal the resources and expertise of multiple agencies within a defined region to deal with cross-jurisdictional crime problems. In some cases, a region is defined as a county (e.g., Rockland County, New York Intelligence Center); as the area surrounding a major city (e.g., Los Angeles Joint Regional Intelligence Center[170]); it may be a portion of a state (e.g., Upstate New York Regional Intelligence Center), or it may encompass an entire state (e.g., Georgia Information Sharing and Analysis Center).

Most RICs were started as the product of counterdrug initiatives starting in the 1980s. Indeed, the High Intensity Drug Trafficking Area (HIDTA) intelligence centers[171] can serve as models for successful structures and initiatives as well as systemic issues that need to be overcome.[172] In the late 1990s, the Bureau of Alcohol, Tobacco and Firearms (ATF) developed a number of programmatic activities to reduce gun violence. Emerging from these initiatives were ATF Regional Crime Gun Centers. The centers, in some cases collocated with the HIDTA RIC, have a number of intelligence-related roles including "…analyzing trace data to identify gun traffickers, disseminate investigative leads, and coordinate with the HIDTA RIC to identify drug traffickers and their sources of guns."[173] In virtually all cases, both the HIDTA and ATF intelligence centers had a great deal of interaction with SLTLE.

169 Regional Intelligence Centers are also sometimes called Fusion Centers. In law enforcement intelligence there is no explicit definition or distinction between the Intelligence Center and Fusion Center.

170 This center is being built and will serve a five-county region, (Los Angeles, Orange, Riverside, San Bernardino, and Ventura) to collect counter terrorism information for the region and analyze that data that allows 24-hour access for law enforcement. http://www.lapdonline.org/press%5Freleases/2004/07/pr04369.htm

171 http://www.whitehousedrugpolicy.gov/hidta/ny-nj-content.html

172 The Counterdrug Intelligence Executive Secretariat (1331 F Street, NW, Suite 700, Washington, DC 20530; Telephone: 202.353.1876/Fax 202.353.1901 has an insightful unpublished report on Metropolitan Area Consolidation/Collocation of Drug Intelligence Elements that describes success and challenges for Regional Intelligence Centers.

173 http://www.atf.gov/field/newyork/rcgc/

Since 9/11, new regional intelligence centers have been created, or are in the process of being developed, to deal with counterterrorism. In several cases, the RIC is funded by the DHS, yet in other cases local and county governments are bearing the costs. While counterterrorism is what stimulated the growth of RICs, as a general rule these are "all crime centers." That is, the centers perform the intelligence function on trans-jurisdictional and organized crime as well as terrorism. To enhance this function, the FBI Field Intelligence Groups are also supporting the RICs.

The structure of intelligence centers also vary widely from being networks (Figure 9-4) to a physical location staffed by multiple agencies (Figure 9-5). There is no right or wrong way to develop a RIC since it must be driven by needs, resources, and geographic characteristics of the region. While the structure may vary widely, there are some best practices that can help guide the RIC operation. At this writing, the Global Intelligence Working Group (GIWG) is developing a set of minimum standards that should be met when an RIC is developed. The reader should monitor the GIWG website[174] where the standards will be posted.

174 http://it.ojp.gov/topic.jsp?topic_id=56

175 http://www.state.ia.us/government/dps/intell/lein/main.htm

Figure 9-4: Law Enforcement Intelligence Network (Iowa)[175]

The Iowa Law Enforcement Intelligence Network (LEIN) is an award-winning program established by the Department of Public Safety in 1984. In August 1994, coordination and administrative responsibilities for LEIN were assigned to the newly created Iowa Department of Public Safety Intelligence Bureau. State, county and local law enforcement agencies from across the state of Iowa provide support to LEIN operations.

LEIN's membership consists of law enforcement officers who have successfully completed a 2-week criminal intelligence course conducted by the Department. LEIN members work together with the department to accomplish two related objectives:

1. To develop and disseminate knowledge about significant criminal conditions that affect the state of Iowa.
2. To use this knowledge to identify, investigate, and remove these criminal conditions.

To achieve the first objective, LEIN serves as a mechanism for the statewide collection and exchange of criminal intelligence information. LEIN members submit information reports to the department's Intelligence Bureau, which in turn, disseminates the information to participating agencies throughout the state.

Figure 9-4: Law Enforcement Intelligence Network (Iowa) (Cont.)

These agencies then use the information to identify and evaluate criminal activity in their area.

LEIN's most effective asset is its members (more than 800 Iowa law enforcement officers and more than 200 agencies) and the trust and personal relationships that are developed to facilitate the sharing of information.

The state is geographically divided into six regions, each of which has a monthly meeting of LEIN members in the region. Information summaries from those meetings are also forwarded to the LEIN Central Coordinating Agency (CCA) for analysis and dissemination.

To further facilitate its mission, LEIN has established relationships with the (MOCIC), Midwest High Intensity Drug Trafficking Area (HIDTA), the LEIU, Iowa Governor's Office of Drug Control Policy (ODCP), U.S. Attorneys' Anti-Terrorism Advisory Councils in both the Northern and Southern Districts of Iowa, and the Iowa Joint Terrorism Task force (JTTF).

Figure 9-5: Georgia Information Sharing and Analysis Center

The Georgia Information Sharing and Analysis Center (GISAC), is responsible for collecting, evaluating, and disseminating intelligence and threat information for Georgia. Its mission is to provide intelligence to law enforcement agencies in Georgia based on the collection, evaluation, and analysis of information that can identify criminal activity. This intelligence can be disseminated the form of either tactical or strategic intelligence.

GISAC is the state's clearinghouse for all terrorism-related intelligence from which it proactively works with the Georgia Bureau of Investigation and other agencies involved in any aspect of counterterrorism.

Multiple state agencies work in the GISAC as outlined in a memorandum of understanding. Federal agencies working in GISAC do so under the provisions of a Participation Agreement between Georgia's Director of Homeland Security and an executive officer for each of the participating federal agencies.

Salary, vehicle, equipment, and supply expenses associated with GISAC personnel are paid for by the employing agency of each GISAC participant. The facilities and furnishings, including computer and communications equipment, are funded by grants and contributions from several of the participating agencies.

CONCLUSION

If effective information sharing is one of the critical goals of contemporary law enforcement intelligence, then networks and systems are the critical tools to reach that goal. As has been seen throughout this chapter, there has been significant growth in the capability for law enforcement agencies to share information. This growth has been a product of new initiatives following 9/11, the availability of new networking technologies that reduce interoperability conflicts, and the commitment of American law enforcement at all levels of government to facilitate information-sharing processes. These factors are in a dynamic state at this writing. Systems and networks will change; therefore, it is incumbent on the intelligence manager to carefully monitor trends to stay current.