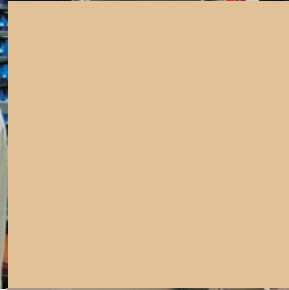


# BJA

Bureau of  
Justice  
Assistance



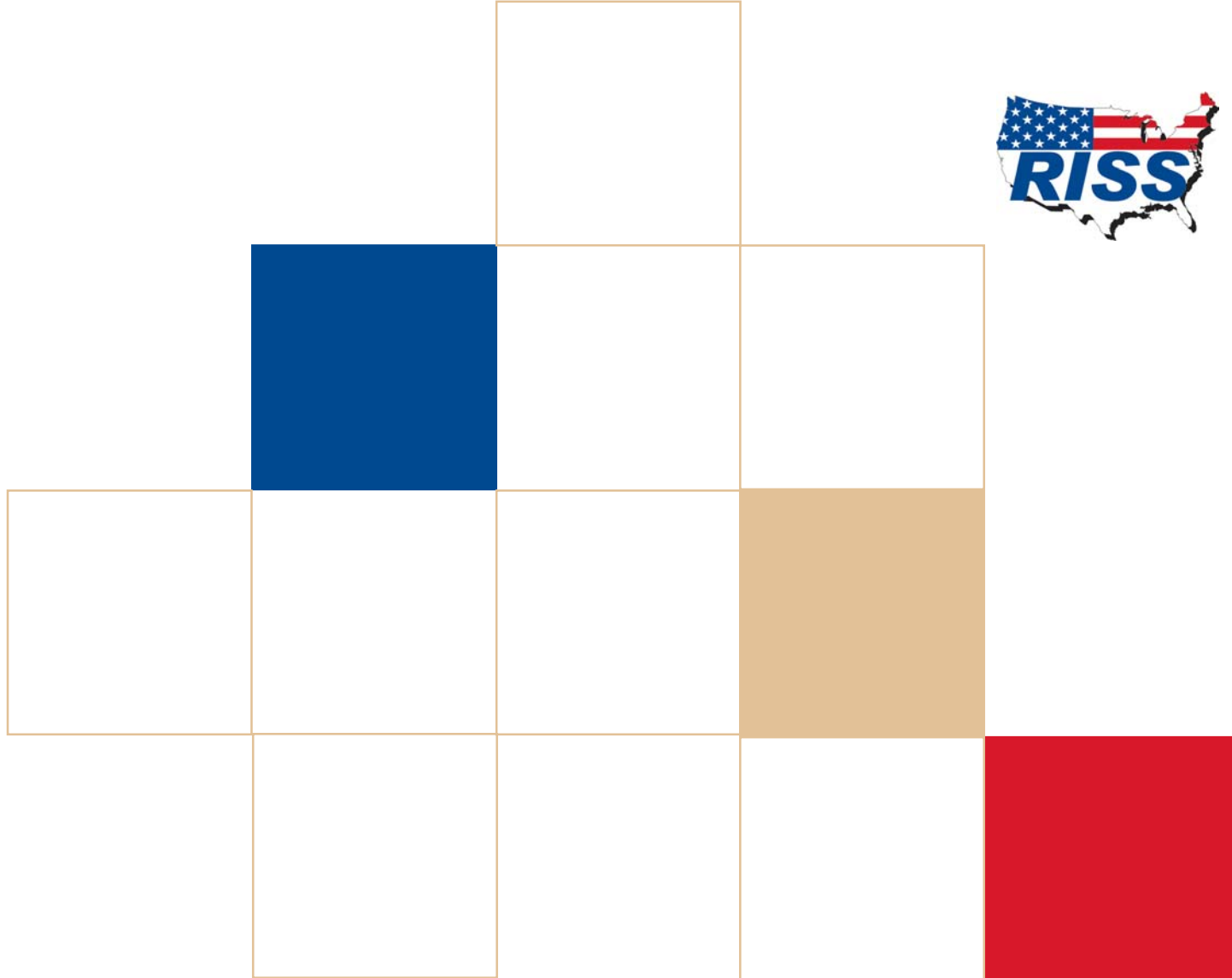
## *The RISS Program: 2002*

*Membership and Service Activity*

Regional Information  
Sharing Systems™  
Program

June 2003





# *The RISS Program: 2002*

*Membership and Service Activity*

Regional Information  
Sharing Systems  
Program

June 2003

# Table of Contents



## **v** Preface

## **1** 2002 Highlights

- 1 RISS/LEO
- 1 RISS ATIX
- 2 RISSearch
- 2 Integrating Other Systems

## **3** riss.net—The RISS Secure Intranet

- 5 Security of riss.net
- 5 Integrating Agency Systems

*This project was supported by Grant Number 2002-RS-CX-0004, awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. 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.*

*The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Bureau of Justice Statistics, and the Office for Victims of Crime.*



## **9 RISS Operations, Membership, and Service Activity**

- 9 RISS Operations
- 10 RISS Membership
- 11 RISS Service Activity
  - 11 Information Sharing
  - 14 Analysis
  - 14 Telecommunications
  - 15 Investigative Equipment
  - 15 Confidential Funds
  - 16 Information Sharing and Training Conferences
  - 16 Other Support

## **17 Results of Member Agency Investigations Supported by RISS Center Services**

- 17 RISS Investigative Leads Bulletin Board (RISSLeads) Support — Example Cases
- 18 Criminal Intelligence Database Support — Example Cases
- 19 Analytical Support — Example Cases
- 20 Confidential Funds Support — Example Cases
- 21 Investigative Equipment Loan Support — Example Cases
- 22 Publications and Training Support — Example Cases

## **23 Conclusion**



# Preface

*Serving over 6,300 member agencies nationwide, RISS continues to foster secure communications and information sharing among all levels of law enforcement.*

The Regional Information Sharing Systems (RISS) Program is a nationwide communications and information sharing network that serves over 6,300 local, state, federal, and tribal law enforcement member agencies in all 50 states, the District of Columbia, U.S. territories, Australia, Canada, and England. The six RISS centers operate in exclusive, multistate geographic regions. This regional orientation allows each center to offer support services that are tailored to the investigative and prosecution needs of member agencies, though the centers also provide services and products that are national in scope and significance.

Traditional RISS communications and information sharing services are designed to help member agencies combat narcotics trafficking, organized crime, violent crime, cybercrime, terrorism, and gang activity. However, RISS is experiencing increased interest in anti-terrorism services, and has responded by expanding the resources available through its secure nationwide law enforcement network. RISS has implemented new services to foster communication among all levels of government and appropriate public entities, as well as meet increased demands by law enforcement member agencies for homeland security information.

The RISS Program is federally funded through the Bureau of Justice Assistance (BJA), Office of Justice Programs (OJP), U.S. Department of Justice (DOJ). BJA provides funding oversight

and program management for the RISS Program. BJA guidelines include required (information sharing, analysis, telecommunications) and optional (equipment loans, confidential funds, training, technical assistance) service components, which all RISS centers provide.

Each RISS center has an oversight group (policy board or executive committee) that determines policy and provides direction regarding center operations and administration. Each center's oversight group is composed of representatives from member agencies in the center's multistate region.

The executive director and policy board chairperson of each center compose the RISS Directors National Policy Group, which has direct control over the policies and operations of the secure nationwide law enforcement communications and information sharing network (riss.net) and related resources. Meetings are held quarterly to address program-wide policy matters and coordination issues for all six centers.

The Institute for Intergovernmental Research (IIR) provides training, research, and analysis services to the RISS Program through the support of grant awards received from BJA. These tasks and activities are usually related to management performance and information systems.



# BJA

The RISS centers, their locations, and geographical regions served are:

**Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network (MAGLOCLN)**, *Newtown, Pennsylvania*, serving Delaware, Indiana, Maryland, Michigan, New Jersey, New York, Ohio, Pennsylvania, and the District of Columbia, as well as Australia, Canada, and England.

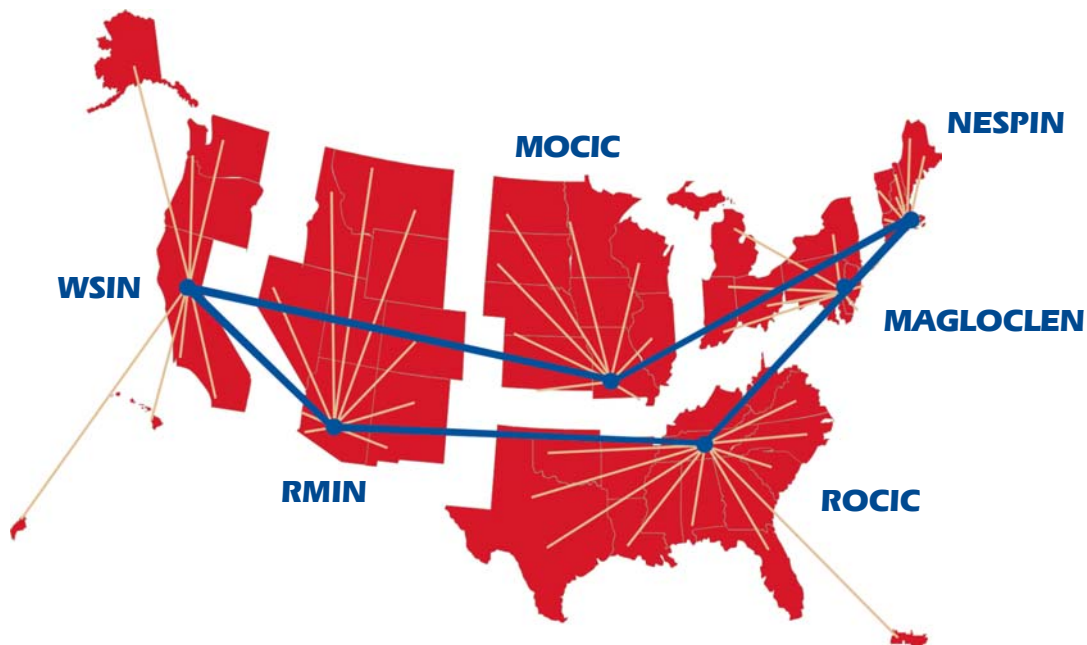
**Mid-States Organized Crime Information Center (MOCIC)**, *Springfield, Missouri*, serving Illinois, Iowa, Kansas, Minnesota, Missouri, Nebraska, North Dakota, South Dakota, and Wisconsin, as well as Canada.

**New England State Police Information Network (NESPIN)**, *Franklin, Massachusetts*, serving Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, and Vermont, as well as Canada.

**Rocky Mountain Information Network (RMIN)**, *Phoenix, Arizona*, serving Arizona, Colorado, Idaho, Montana, Nevada, New Mexico, Utah, and Wyoming, as well as Canada.

**Regional Organized Crime Information Center (ROCIC)**, *Nashville, Tennessee*, serving Alabama, Arkansas, Florida, Georgia, Kentucky, Louisiana, Mississippi, North Carolina, Oklahoma, South Carolina, Tennessee, Texas, Virginia, and West Virginia, as well as Puerto Rico and the U.S. Virgin Islands.

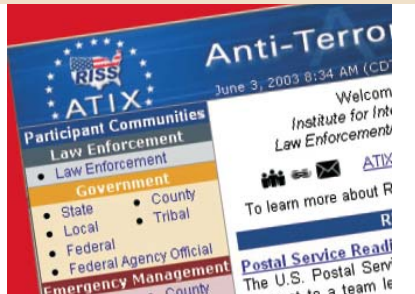
**Western States Information Network (WSIN)**, *Sacramento, California*, serving Alaska, California, Hawaii, Oregon, and Washington, as well as Australia, Canada, and Guam.





# 2002 Highlights

*RISS initiatives are bringing together the law enforcement community and other government and non-government entities responsible for planning and implementing prevention, response, mitigation, and recovery efforts regarding terrorism and disasters.*



During 2002, information sharing has been recognized as the essential element in the fight against terrorism. Traditionally a law enforcement information sharing network, RISS is expanding services to address the changing needs of law enforcement and other public safety officials by leveraging its established technological resource, the RISS secure intranet (riss.net).

## RISS/LEO

On September 1, 2002, the RISS secure intranet and the FBI's Law Enforcement Online (LEO) systems were interconnected to provide for distribution of sensitive but unclassified homeland security information. A seamless secure connection allows riss.net and leo.gov users access to both systems, as authorized, with a single logon. Secure e-mail is also available to users of both systems.

The features of the interconnection are the result of a focus group convened in 2002, comprised of RISS and LEO users, which made recommendations concerning the dissemination and sharing of homeland security information.

LEO will disseminate homeland security information and alerts to users of both systems. RISS continues to maintain the criminal intelligence databases. Expansion of the RISS/LEO interconnection to provide additional capabilities for distributing FBI LEO alerts will occur during 2003.

## RISS ATIX

The RISS Anti-Terrorism Information Exchange (ATIX) was initiated in the latter part of 2002. Through RISS ATIX, RISS is fostering secure communications exchange among the entities responsible for planning and implementing prevention, response, mitigation, and recovery efforts regarding terrorism and disasters.

RISS ATIX is designed to be the secure means to disseminate national security, disaster, and terrorist threat information to law enforcement, other first responders, and key community officials. **RISS ATIX participants will include public service, public safety, emergency management, and utility personnel that have not traditionally been served by RISS.**

RISS ATIX combines three powerful components for use in disseminating information to participants:

1. The electronic RISS ATIX bulletin board, to provide a forum for participant discussion and posting of homeland security information.
2. The RISS ATIX Web site, to house general and community-specific homeland security information and links to restricted and public Web sites and other sources of terrorism, disaster, and homeland security-related information.
3. Secure e-mail accounts, to enhance communication among ATIX participants and allow for delivery of alerts for specific geographic locations.

RISS has these components online via riss.net, and is working to provide materials and training to the ATIX participants in five states initially: Arizona, Colorado, Delaware, Hawaii, and Tennessee. All RISS members have access to the ATIX components.

### RISSSearch

New to riss.net is a search engine that scans and retrieves content from multiple information sources and databases. Members can use the tool to search restricted information sites, sensitive but unclassified sites, and also selected public Internet sites in the same manner as popular Web search engines. The first phase of this service was implemented in August 2002.

### Integrating Other Systems

RISS continues to link state and federal agency systems to riss.net as nodes for secure communications services, including information sharing, use of secure e-mail, and distribution of homeland security information and alerts. During the latter part of 2002, the RISS centers were approached by a coalition of states participating in a pilot project called the **Multistate Anti-Terrorism Information Exchange (MATRIX)**. MATRIX is a pilot project funded by the U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, that uses riss.net as a secure communications backbone to facilitate access and exchange between states regarding anti-terrorism efforts. The state coalition participating in

MATRIX is currently composed of Alabama, Connecticut, Florida, Georgia, Kentucky, Louisiana, Michigan, New York, Ohio, Oregon, Pennsylvania, South Carolina, and Utah. The participants will make their state law enforcement databases available to other participants and RISS member agencies to help law enforcement identify and analyze terrorist and other criminal activity.

A six-month pilot project has been proposed that will connect the **National Law Enforcement Telecommunication System (NLETS)** as a node on riss.net. The agencies of four states—Arizona, Iowa, Maine, and Vermont—will be able to access riss.net resources through their connections to NLETS. The project leverages the extensive infrastructure of NLETS to provide agencies an alternative method of accessing riss.net. The connection will support information sharing between the two systems, expanding the resources available to NLETS users and enhancing access to riss.net.

The **Department of Homeland Security (DHS)** has initiated a pilot project with RISS. The project will employ the RISS Investigative Leads Bulletin Board (RISSLeads) and RISS ATIX resources to post and exchange information among the local, state, and federal agencies from the pilot states: Arizona, California, Florida, Massachusetts, Nebraska, and Pennsylvania.

The project concept uses riss.net to provide DHS the ability to communicate with local and state public safety agencies, elected officials, industries, and the public regarding nuclear power infrastructure information.

# riss.net—The RISS Secure Intranet

*The secure communications backbone allows enrolled RISS member law enforcement agency personnel electronic access to all authorized databases and services located on the intranet for secure exchange of sensitive information.*



The RISS nationwide secure law enforcement network for communications and information sharing by member agencies is known as riss.net. Internet technology is used to provide a secure private intranet that connects the six RISS centers and their participating law enforcement member agencies, as well as member agency systems operating as nodes on the intranet.

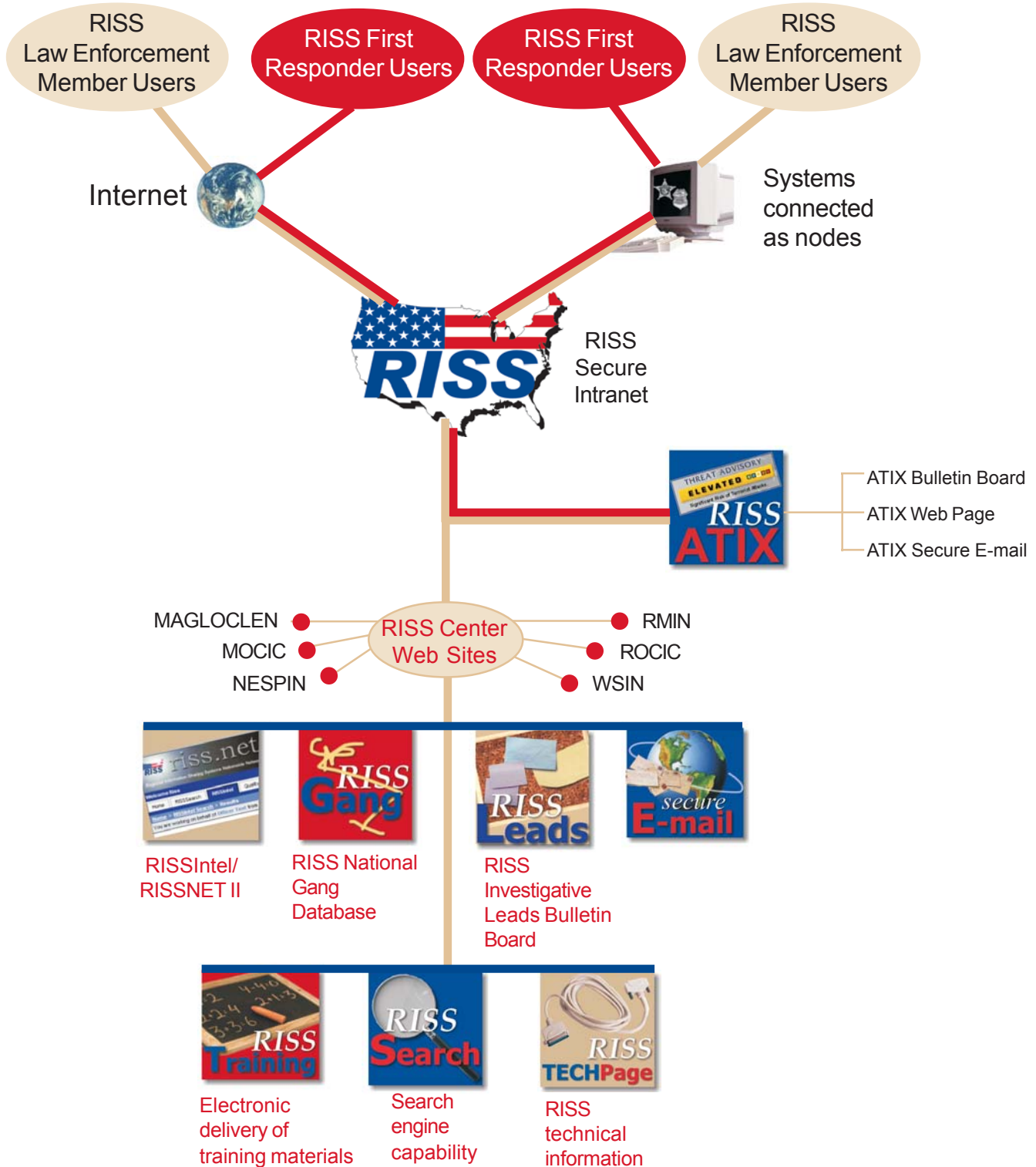
Participants may use either a single computer connection from a member agency or a node connection of an agency network. Node connections expand the availability of riss.net resources and information to law enforcement users of the agency network.

Member agencies may enroll and connect to RISS resources via their agency Internet Service Provider (ISP) or via direct dial-up access without using an ISP. The secure communications backbone allows enrolled RISS member law enforcement agency personnel electronic access to all authorized databases and services located on the intranet for secure exchange of sensitive information.

**riss.net resources**— Services available to member agencies include the RISS Investigative Leads Bulletin Board (RISSLeds), the RISS Criminal Intelligence Databases (RISSIntel/RISSNET II), the RISS National Gang Database (RISSGang), the RISS training Web site (RISSTraining), RISS center Web sites, the RISS technical assistance Web site (TECHPage), and the RISS search engine (RISSSearch). Additional resources are available to RISS member agencies and first responders (public safety, etc.) on the RISS Anti-Terrorism Information Exchange (ATIX). In addition, RISS member agencies and ATIX users have access to secure e-mail via riss.net (see Exhibit 1, page 4).

RISS is committed to increasing electronic collaboration among member agencies in order to promote interagency cooperation on multijurisdictional investigations. As of December 31, 2002, there were 3,432 member agencies electronically connected, which represents 54% of the total RISS membership. The number of officers connected for online access via riss.net increased from 6,377 officers in 2000 to 9,411 officers by the end of 2002.

# Exhibit 1: riss.net Resources



In addition to electronic access, RISS member agency users continue to contact RISS center staff by telephone, fax, or mail to request assistance with database searches and use of other center services.

*In January 2002, the RISS Program received the Second Annual Computer Security and Information Assurance Award.*

## Security of riss.net

RISS has traditionally operated a trusted, proven law enforcement network for the secure exchange of information. The technical capabilities and systems architecture implemented by RISS allow member agencies to interact electronically with one another in a secure environment. The RISS secure intranet (riss.net) protects information transmissions through use of encryption, smart cards, Internet protocol security standards, and firewalls to prevent unauthorized access.

The RISS center provides a security package to member agency users, and access is accomplished by first enrolling each member user. Riss.net uses multiple levels of firewall protection that authenticate the user as an authorized member of the trusted network. Additional firewalls control the traffic to various resources and allow access based on entitlements to those resources.

Penetration testing by a qualified vendor is conducted periodically as required under RISS security policies. RISS security policies and system monitoring procedures are in place at each center.

In January 2002, the RISS Program received the Second Annual Computer Security and Information Assurance Award in the Law Enforcement and Public Service category from the Potomac Forum, LTD. The RISS Program was chosen because it exemplifies government computer security “best practices” by enabling the secure sharing of law enforcement information among thousands of professionals across the United States.

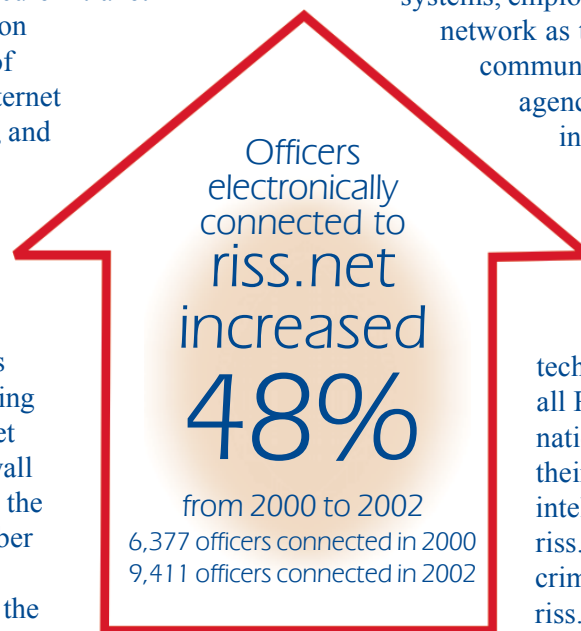
## Integrating Agency Systems

The RISS centers continue to expand electronic connection and integration of law enforcement information systems with the RISS network, as displayed in Exhibit 2 (page 8). The High Intensity Drug Trafficking Areas (HIDTAs) and state agencies, as well as regional and federal systems, employ the RISS nationwide network as their secure means of communication. RISS member agencies are aided in investigations by access to a broader array of agency and database resources.

Several states are working with RISS to develop the necessary technical interface that will allow all RISS member agencies nationwide to directly access their state law enforcement intelligence databases via riss.net. Agencies connecting a criminal intelligence database to riss.net must agree to comply with 28 CFR Part 23 (Criminal Intelligence Systems Operating Policies) and agree to a compliance review by BJA.

Data formats vary greatly between database applications operated by law enforcement agencies. XML (Extensible Markup Language) is a technology that allows for communication between Web-based applications, and is the standard RISS uses. The RISS Data Exchange Specification is promoted to law enforcement agencies connecting to riss.net as nodes to facilitate the ability to share their criminal intelligence information with RISS member agencies.

The systems integrated with riss.net are listed on the following pages. Several pilot, proof-of-concept, projects currently underway are also described.



## Integrating Agency Systems (continued)

### High Intensity Drug Trafficking Areas

RISS is in partnership with the High Intensity Drug Trafficking Areas (HIDTAs), which involves electronic connection of the HIDTAs to riss.net. Agencies participating in the HIDTAs use riss.net as their communications and information sharing backbone.

#### Connected

The HIDTA offices connected as nodes to riss.net as of December 31, 2002, are listed below:

Chicago HIDTA  
 Gulf Coast HIDTA  
 Los Angeles HIDTA  
 Midwest HIDTA  
 Milwaukee HIDTA  
 New York/New Jersey HIDTA  
 Northern California HIDTA  
 Northwest HIDTA  
 Oregon HIDTA  
 Rocky Mountain HIDTA\*  
 South Florida HIDTA  
 South Texas HIDTA\*\*  
 Southern California HIDTA\*\*  
 Southwest Border HIDTA\*\*  
 Washington/Baltimore HIDTA

\* Rocky Mountain HIDTA is composed of Colorado, Utah, and Wyoming.

\*\* Southwest Border HIDTA is made up of five regional partnerships: Arizona, New Mexico, Southern California, South Texas, and West Texas.

#### Connection Pending

HIDTA offices pending connection to riss.net as nodes during 2003 include:

Arizona HIDTA  
 Lake County, Indiana, HIDTA

### State Agency Systems

The following state law enforcement agency systems were electronically connected as nodes to riss.net as of December 31, 2002, and use the riss.net infrastructure for communications and information exchange.

#### Connected

California  
 Colorado<sup>A</sup>  
 Florida<sup>M</sup>  
 Missouri  
 Oregon<sup>M</sup>  
 South Dakota  
 Utah<sup>M</sup>  
 Washington  
 Wyoming

#### Connection Pending

State law enforcement agencies pending connection to riss.net as nodes during 2003 include:

Alabama <sup>M</sup>	Louisiana <sup>M</sup>
Arizona <sup>A</sup>	Michigan <sup>M</sup>
Connecticut <sup>M</sup>	New York <sup>M</sup>
Delaware <sup>A</sup>	Ohio <sup>M</sup>
Georgia <sup>M</sup>	Pennsylvania <sup>M</sup>
Hawaii <sup>A</sup>	South Carolina <sup>M</sup>
Iowa	Tennessee <sup>A</sup>
Kentucky <sup>M</sup>	Vermont

<sup>A</sup> RISS Anti-Terrorism Information Exchange (ATIX)

<sup>M</sup> Multistate Anti-Terrorism Information Exchange (MATRIX)



## Regional and Federal Systems

The following regional and federal systems are available to riss.net users, expanding the resources available to member agencies by providing access to additional intelligence information.

- ◆ Criminal Information Sharing Alliance (CISAnet) (formerly Southwest Border States Anti-Drug Information System, SWBSADIS) – The state systems of Arizona, California, New Mexico, and Texas are connected to each other and to riss.net. Georgia and Idaho are working to connect their state databases as well. The shared databases promote inter-agency information sharing regarding narcotics trafficking.
- ◆ Clandestine Laboratory Seizure System (CLSS) – Operated by the El Paso Intelligence Center (EPIC) for submission and exchange of information regarding methamphetamine lab seizures.
- ◆ Law Enforcement Online (LEO) – Operated by the FBI, the system is interconnected with riss.net to provide RISS members timely access to critical homeland security information.
- ◆ The Law Enforcement Intelligence Unit (LEIU)
- ◆ National Drug Pointer Index (NDPIX)
- ◆ The National Drug Information Center (NDIC)
- ◆ The National White Collar Crime Center (NW3C) – Pending connection to riss.net.
- ◆ Financial Crimes Enforcement Network (FinCEN) – Pending connection to riss.net.
- ◆ The Executive Office for United States Attorneys – As of March 31, 2003, 82 of 94 United States Attorneys' Offices are RISS members. The offices will use the riss.net backbone for communication purposes.



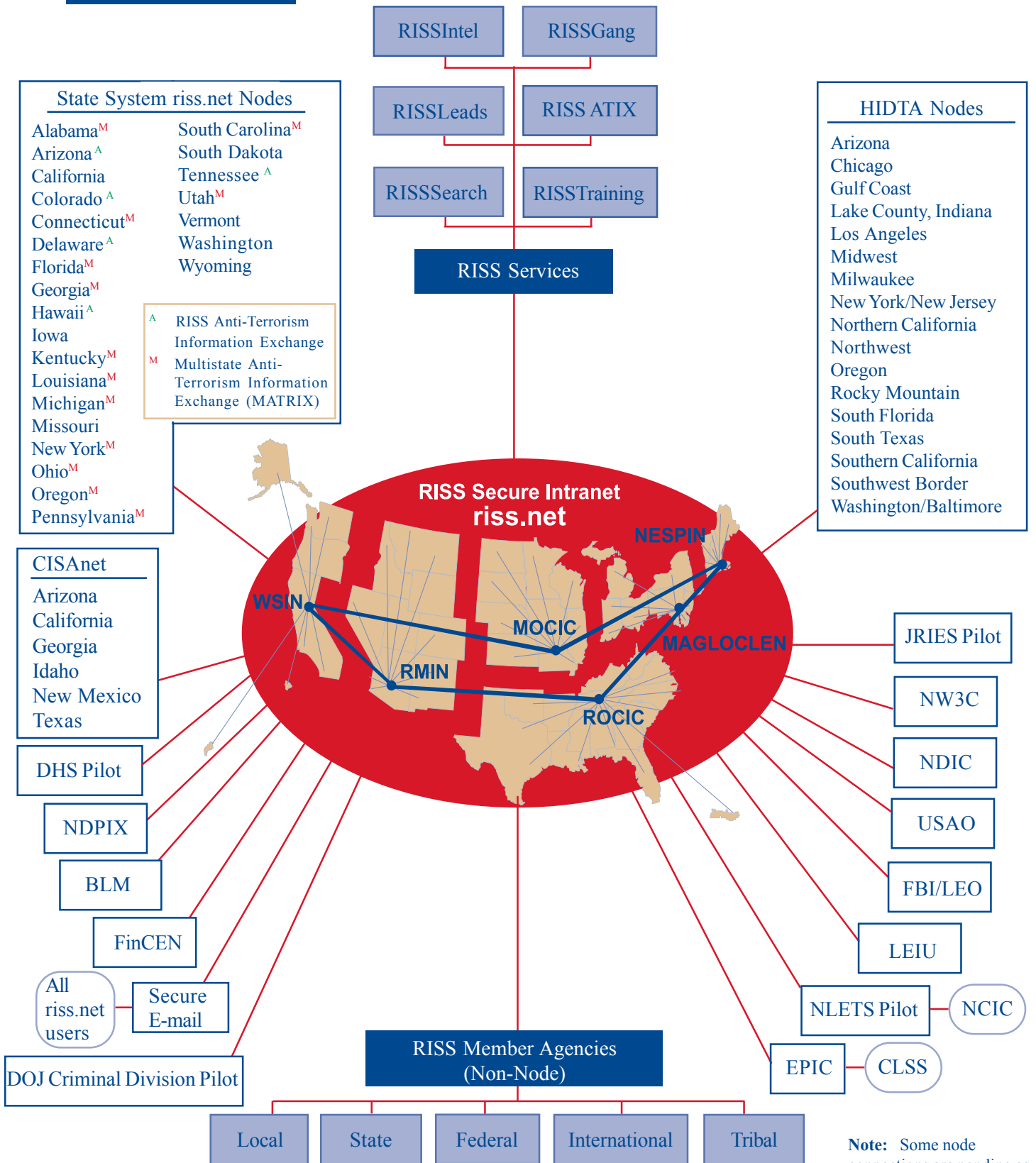
## Pilot Projects

RISS is actively participating in pilot projects that expand information sharing and increase federal agency communication and cooperation with state and local law enforcement entities. The following initiatives are underway and involve connection to riss.net.

- ◆ Department of Homeland Security (DHS) – Through riss.net, DHS will connect with local and state and public safety agencies, elected officials, industries, and the public, allowing the participants to communicate regarding critical infrastructure information.
- ◆ Department of Justice (DOJ), Criminal Division – Fifty DOJ personnel will connect to riss.net for use of secure e-mail.
- ◆ The National Law Enforcement Telecommunication System (NLETS) – The proposed connection of riss.net and NLETS will expand the resources available to NLETS users and enhance access to riss.net. Four states are involved in the pilot project: Arizona, Iowa, Maine, and Vermont.
- ◆ Department of the Interior, Bureau of Land Management (BLM) – The agency is exploring use of the RISS intelligence databases and connection to riss.net for storing and accessing investigative suspect information.
- ◆ The Joint Intelligence Task Force Counter-Terrorism RISS Information Exchange System (JRIES) – Initiated by the Department of Defense, Defense Intelligence Agency, the pilot project provides local, state, and federal law enforcement participants with collection, analysis, collaboration, and warning capabilities for counter-terrorism. The project concept uses riss.net as the communications backbone.

# Exhibit 2: RISS Secure Intranet

## Communication and Information Sharing Partnership with Local, State, and Federal Law Enforcement



**Note:** Some node connections are pending as of June 2003.



# RISS Operations, Membership, and Service Activity

*By staying abreast of technological advances, remaining responsive to the needs of traditional member agencies, and broadening services to include public safety communities, RISS remains a valuable tool for combating multijurisdictional crime and terrorist threats.*



## RISS Operations

The federally funded RISS Program supports member agency investigative and prosecutorial efforts in combating multijurisdictional criminal activities, including terrorism. RISS provides a structured system for the exchange of information among member agencies throughout the United States. The RISS Program Funding and Administration Guidelines prescribed by BJA set out the services and operational guidelines for the six centers.

Under the BJA guideline, each RISS center must implement three required service components: information sharing (databases and conferences), telecommunications (riss.net), and analysis (intelligence analysis of member agency cases, proactive analysis of the center's database, and special criminal activity assessments). Four optional service components may be implemented: investigative support (loan of confidential funds); specialized equipment (pooling of specialized investigative equipment items for loan to member

agencies); training (regional programs and conferences, and electronic delivery of training material on riss.net); and technical assistance (field staff). Each of the RISS centers has implemented all optional components as well as the required components.

While all centers provide the same service components, each center establishes service priorities according to member needs in the region served. However, the six centers coordinate their activities related to national issues and crime problems to generate products of national interest.

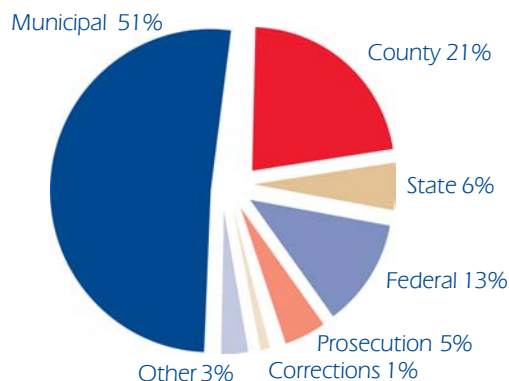
Each of the RISS centers has a policy board selected from the membership in the region. The RISS Directors National Policy Group is made up of the executive director of each center along with the chair of each center's policy board. They meet quarterly and decide on program-wide policy and coordination issues for all six centers. The Office of Justice Programs, Bureau of Justice

Assistance, provides program management and oversight.

In addition, the RISS directors have developed a long-range RISS Strategic Plan that sets out goals, objectives, and strategies for accomplishing the RISS mission in supporting member law enforcement investigative and prosecution efforts, as well as providing support to the homeland security efforts of other public service agencies.

Each of the RISS centers has a professional management staff as well as other service, intelligence, analytical, field, and information technology staff. Center staff are prohibited from direct involvement in law enforcement operations.

The RISS Office of Information Technology (OIT), a centralized information technology staff, provides services, coordination, and support for all six RISS centers. RISS OIT maintains riss.net and develops the common RISS resources provided on the network. The RISS centralized information staff and the technical staff from each of the RISS centers meet twice each year to coordinate technical matters among the centers including security and upgrades to hardware and software, as well as update the center technical staff on the current and future direction of the RISS system and database application development.



### RISS Membership by Type of Agency

To participate in RISS support services and activities, agencies must become members of their in-region RISS center. Each center has established an application and policy board approval process for this purpose.

Combined membership of the six RISS regional intelligence centers increased from 5,603 in calendar year 2000 to 6,345 in 2002. Members include local, state, and federal law enforcement agencies, prosecution agencies, corrections agencies, and others such as tribal police, multijurisdictional task forces, and regulatory agencies with law enforcement or criminal investigative authority.

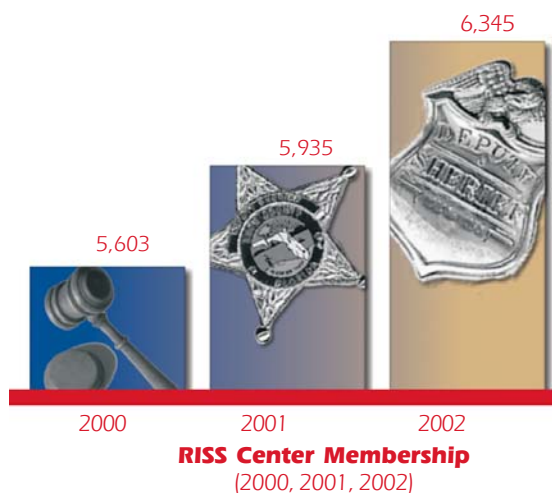
The majority of RISS member agencies are municipal and county law enforcement agencies (72%), but 385 state agencies and 819 federal agencies are also members. The Federal Bureau

## RISS Membership

### RISS Center Membership

Number of agencies as of December 31, 2002

MAGLOCLEN	1,061
MOCIC	1,143
NESPIN	589
RMIN	925
ROCIC	1,509
WSIN	1,118
<b>Total</b>	<b>6,345</b>



of Investigation; U.S. Attorneys' Offices; Immigration and Naturalization Service; Customs; Border Patrol; Drug Enforcement Administration; Internal Revenue Service; Secret Service; Bureau of Alcohol, Tobacco, Firearms and Explosives; and the Bureau of Land Management are among the federal agencies participating in the RISS Program.

As RISS membership grows, the number of law enforcement personnel who benefit from electronic access to RISS resources also increases. A growing number of officers use the RISS secure intranet to communicate with each other through secure e-mail and electronic bulletin boards, and also with the RISS centers for assistance with their investigative needs. From 2000 to 2002, officers with an activated riss.net account increased nearly 50%. The number of law enforcement agencies with riss.net access grew to nearly 3,500 in 2002. These agencies and their personnel enjoy the speed and security of riss.net access to enhanced electronic services, as well as the benefits of traditional RISS resources. RISS services are also available to more than 55,000 RISS member agency access officers by phone, fax, or mail request.

## RISS Service Activity

### Information Sharing

The major goal of the RISS Program is to provide law enforcement member agencies with the necessary tools to share information about known or suspected criminals and criminal activity. The operation of riss.net enhances this goal by expanding the information sharing and communications capabilities of RISS member agencies nationwide. RISS information sharing resources available to member agencies include RISSLeads, RISSIntel/RISSNET II databases, RISSGang, and other specialized databases. These resources and corresponding activity are described on the following pages. RISS member agencies also have access to the newly implemented RISS ATIX resources described on page 2.

In addition, through node connections, there are state, federal, and specialized databases available. These specialized databases currently include the LEIU database and the Clandestine Laboratory Seizure System at EPIC. The California Department of Justice, Bureau of Investigation, intelligence database is accessible to RISS members, and many of the state agencies connected as nodes are working to provide access to their state databases on riss.net. The FBI Inland Regional Terrorism database is restricted to members of the FBI Terrorism Task Force in the Northwest region of the country and is housed at RMIN.

**28 CFR Part 23 Compliance**—All information entered into RISS intelligence databases must comply with the Criminal Intelligence Systems Operating Policies (28 CFR Part 23) issued by the Bureau of Justice Assistance. All intelligence databases connected to riss.net as nodes must also comply with 28 CFR Part 23.

**Deconfliction database**—For officer safety purposes, the ROCIC and WSIN centers each operate a deconfliction database for use by member agencies in their respective regions in determining if other agencies are investigating the same subject.



**Terrorism information is available on RISSLeads through Watch Lists and Special Bulletins.**

## RISSLeads Features and Benefits

- ◆ Bulletin Board – Case information is posted with the intent of generating investigative leads. Member agencies share intelligence by viewing and responding to posted information.
- ◆ Forum and Chat – Geographically disparate law enforcement professionals convene electronically to discuss crime trends or specific cases, and share investigative techniques.
- ◆ Watch Lists and Special Bulletins – RISSLeads is the location of terrorism watch lists and homeland security information available through RISS.



## RISSIntel/RISSNET II Intelligence Database Features and Benefits

- ◆ Criminal Intelligence – Members inquire about criminal subjects, organizations, vehicles, weapons, phone numbers, and addresses. When information is located in the database (a “hit”), members are referred to agencies that have the information. The databases are designed to encourage exchange of information and coordination among member agencies investigating the same individuals or organizations.
- ◆ Web-based – Direct access is provided for member agencies activated on riss.net.
- ◆ Electronically Linked – Users may be selective in which databases to query, or may query all databases and other available systems simultaneously.
- ◆ Batch Upload Option – Member agencies are able to submit large volumes of data for inclusion in the database.

**The RISSGang database includes visual imagery of gang paraphernalia and graffiti.**

## RISSGang Database Features and Benefits

- ◆ Gang-specific – The database contains records of subjects and organizations suspected of involvement in criminal activity.
- ◆ Information and Images – In addition to information on gang members and gangs, the database includes visual imagery of gang paraphernalia and graffiti.

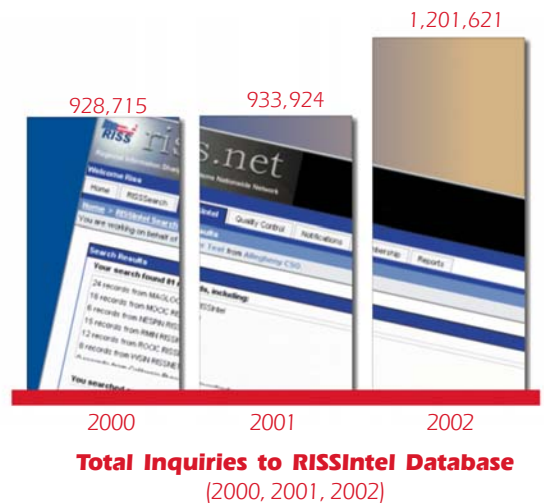
## RISSLeads Usage Data – 2002

- ◆ User connections total 3,629,416. Users are spending more time on the Bulletin Board, and posting more messages.
- ◆ As of December 31, 2002, there were 58 user conferences, or discussion topics, within which users post and view messages. Conferences continue to be added at the request of member agencies and staff.

**Over 3.6 million  
RISSLeads connections  
were made in 2002.**

## RISSIntel/RISSNET II Intelligence Database Usage Data – 2002

- ◆ Data records total 2,791,676. These include individuals, organizations, groups, and associates suspected of involvement in criminal activity, as well as locations, vehicles, weapons, and telephone numbers.
- ◆ Inquiries total 1,201,621. Includes inquiries made and requested by member agencies for all databases combined.
- ◆ Hits total 165,477. Represents number of times information was found in response to member agency inquiries.
- ◆ Agencies notified as a result of a hit total 229,811.



## RISSGang Database Usage Data – 2002

- ◆ Records total 71,647. There are 66,799 records on gang members, and 4,848 records on gangs housed in the database.
- ◆ Inquiries total 20,595.
- ◆ Hits total 10,244.

**The RISSGang database  
contains 71,647 records.**

**Nearly 20,000 analytical products were delivered in 2002.**

## Analysis

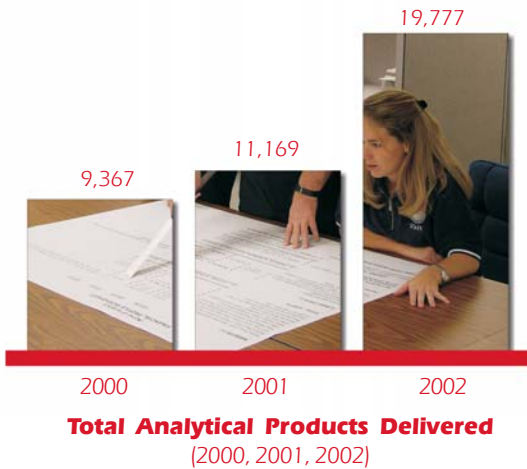
Analytical services are available at each RISS center. Through consultation with the requesting officer, analytical personnel tailor products to member agency needs.

Case-specific support includes compilation and analysis of investigative data to develop flowcharts, link-analysis charts, crime scene diagrams, telephone toll-analysis reports, and financial-analysis reports as requested by the member agency. Prosecutors often request these types of products for use in courtroom testimony.

Analytical staff also prepares crime surveys; criminal activity assessment reports, such as terrorism assessments; and national scope products for distribution to member agencies in the center region.

During 2002, the six RISS centers combined delivered 19,777 analytical products to law enforcement member agencies in response to their requests for support on multijurisdictional investigations and prosecutions.

In addition, RISS personnel provide computer forensics analysis. This service involves data retrieval from computers seized in member investigations.



**Over 37 million connections to riss.net were made in 2002.**

## Telecommunications

The riss.net network is the communications backbone that supports electronic access and exchange of information by RISS users nationwide. Users made over 37 million connections to riss.net during 2002.

In addition, all six RISS centers operate long distance telecommunications, or WATS services, to facilitate contact between RISS member agencies that frequently leads to the agencies working jointly on investigations. The WATS services include the optional service of call patching capabilities for interstate telephone calls. These services are operated at no cost to member agencies and support the operations of the information sharing and analytical components of each center, as well as center-supported investigations and activities. During 2002, 15,962 WATS/Patch calls were made by member agencies.



## Investigative Equipment

Pools of investigative equipment are available for loan to member agencies for use in support of multijurisdictional investigations. Center equipment pools contain various types of specialized photographic, communications, and surveillance equipment. During 2002, the RISS centers made 3,737 investigative equipment loans to member agency personnel.

Inventory controls and procedures ensure proper use of center equipment. Member agencies that request loan of investigative equipment must do so in writing and adhere to loan procedures. The centers require member agencies to report on the use of equipment and the benefit resulting from support of their investigative activity. These reports also provide investigative information on criminal suspects for submission to the center databases.



**Nearly 3,800  
investigative  
equipment loans  
were made in 2002.**

## Confidential Funds

The RISS centers have confidential funds available to member agencies for the purchase of investigative information, contraband, stolen property, and other items of an evidentiary nature, or to provide for other investigative expenses. The net amount of confidential funds provided to member agencies totaled \$282,630 for 2002.

The availability and use of confidential funds are strictly controlled by federal guidelines, and internal policies and procedures are developed by each center. The member agency must demonstrate that funds are not available from other sources.

The centers require member agencies to report on the use of the confidential funds and the benefits resulting from support of the member agency investigative activity. As in the use of investigative equipment, these reports provide investigative information on criminal suspects for submission to center databases.

**Over \$280,000 in  
confidential funds  
were provided  
in 2002.**

## Information Sharing and Training Conferences

Each of the RISS centers sponsors or co-sponsors meetings and conferences that build investigative expertise for member agency personnel in its region. Meeting and conference formats often provide a mixture of training and information sharing activities. Subject areas include anti-terrorism training, crime-specific investigative techniques, surveillance techniques, use of specialized equipment, officer safety information, and analytical techniques. In 2002, 36,043 officers attended RISS-sponsored information sharing conferences and specialized training sessions.

Meetings are held frequently at the local, county, and state levels in each RISS region to exchange information on regional crime problems and criminal activity among law enforcement professionals. In addition, RISS center officials and staff attend national and regional law enforcement association conferences held throughout the country to present information on RISS services.

**Over 36,000 officers attended RISS-sponsored conferences or training in 2002.**



**The RISS centers use their secure Web pages on riss.net to distribute timely information.**

## Other Support

A variety of other information sharing and support services are provided to RISS member agencies. Services may vary to some extent from center to center. A few of the activities and services are described below.

Publications enhance the ability of RISS member agencies to share information on criminal activity in their respective regions. Each center distributes criminal information bulletins, flyers, and other intelligence information publications to member agency personnel. Some publications are distributed on an as-needed basis; others are routinely published.

The RISS centers utilize their secure Web pages on riss.net to post many of their criminal activity publications and bulletins, training calendars, and information on obtaining center services. The center Web pages allow distribution of timely, up-to-date information. Member agencies can access center publications and bulletins, and search for information on criminal activity and crime patterns. This often leads to agency collaboration in solving crimes.

Field staff units at each center provide technical assistance to member agencies. Technical assistance may include explanation of and guidance in requesting services, installment and use of riss.net, and various training activities.





# Results of Member Agency Investigations Supported by RISS Center Services

*The six centers combined assisted their member agencies in making 3,664 arrests by providing information, analytical services, equipment loans, and confidential funds to support their investigations.*

In 2002, member agency investigations that were supported by center services resulted in thousands of arrests, and seizures of narcotics, property, and currency valued in the millions of dollars. A few of the many examples of successful cases in which RISS services were used are summarized in this section.

## RISS Investigative Leads Bulletin Board (RISSLeads) Support – Example Cases



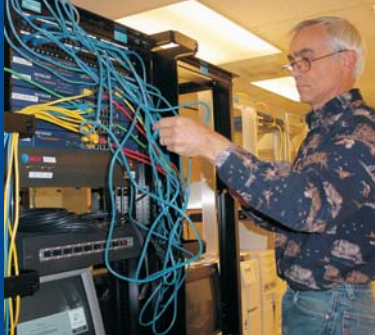
### MOCIC

The MOCIC center staff posted information regarding a sexual assault investigation to RISSLeads that helped the Stevens Point, Wisconsin, Police Department successfully identify and arrest the perpetrator. The posted information indicated that the unknown suspect had left a bottle at the crime scene, and it had been retrieved for fingerprinting. An officer from the Madison, Wisconsin, Police Department, who was investigating a string of sexual assaults, responded to the information posted and asked to intercept the bottle for DNA testing. The Madison officer shared the DNA test results, which led the Stevens Point officer to the suspect. The suspect was charged, and ultimately pled guilty to the case.

### RMIN

Multiple vehicle burglaries prompted the Boulder County, Colorado, Sheriff's Office to request RMIN center services. Credit cards were being stolen from vehicles parked near hiking trails, and used in Las Vegas casinos within hours of the theft. RMIN intelligence technician research staff posted the information on RISSLeads, and also e-mailed the case details to area law enforcement agencies. Shortly after the posting, the Boulder County Sheriff's Office received responses from agencies spanning five states. The information led to the determination that the crime spree most likely involves Russian organized crime groups, and has been recurring for five years. The Boulder County Sheriff's Office plans to share the evidence to assist other jurisdictions in solving similar crimes.

## Criminal Intelligence Database Support – Example Cases



### MAGLOCLLEN

An anti-terrorism investigation led the North Florida Joint Anti-Terrorism Task Force to contact the Tredyffrin Township, Pennsylvania, Police Department to aid in the apprehension of a suspect. The Tredyffrin Township Police Department requested assistance from MAGLOCLLEN intelligence research staff, which provided detectives with the results of intelligence database searches. The suspect was located and later deported to his native country of Jordan for multiple charges of identity fraud and other illegal activity.

### MOCIC

The Mason City, Iowa, Police Department requested the assistance of MOCIC intelligence technician research staff in a music piracy case. A search warrant executed at a store revealed the pirated merchandise, and minimal information about the distributor. Using the available information, the MOCIC staff conducted database records research and was able to locate suspects in Arizona and Florida. Further investigation revealed involvement of businesses in most, if not all, U.S. states. Officers confiscated more than 200,000 CDs valued in excess of \$5 million, as well as drugs and at least one automatic weapon.

### NESPIN

A mid-sized Connecticut police department requested that NESPIN intelligence technician research staff perform an inquiry to the RISSIntel database; hits on eight records were received. The investigators checked each record and recognized one entry, by the Vermont State Police Intelligence Unit, as a person they had arrested in the past for narcotics violations. An informant reported that this person was supplying narcotics and had a connection in Vermont. The investigators contacted the Vermont State Police to discuss and further pursue their case.

### RMIN

The RMIN intelligence technician research staff provided intelligence support to the U.S. Department of Interior, Bureau of Land Management (BLM); the Boise, Idaho, Police Department; and the Ada County, Idaho, Sheriff's Office on a multi-agency investigative task force looking into a series of burglaries to BLM facilities and fire vehicles. Two Boise-area residents were charged with one count of grand theft each. Approximately \$30,000 worth of government property and equipment was recovered during the investigation.

### WSIN

The WSIN center received an inquiry from the San Diego, California, Drug Enforcement Administration regarding a subject and address associated with cocaine. A query of the RISSNET II intelligence database resulted in a hit from information submitted by the Los Angeles, California, Federal Bureau of Investigation office. Appropriate agencies were notified.

### ROIC

ROIC intelligence technician research staff provided database and records checks in support of Louisiana officials in a narcotics investigation. A joint effort between the Union Parish Drug Task Force, Union Parish Sheriff's Office, Metro Narcotics, Montor Police Department Jump Team, and the Federal Bureau of Investigation resulted in an arrest. The individual was in the process of a drug transaction when arrested in Bernice, Louisiana. He had approximately 2 kilograms of cocaine in his possession. He was charged with conspiracy to possess over 400 grams of cocaine and possession of over 400 grams of cocaine. Bond was set at \$1,000,000. He faces up to 30 years in prison and up to a \$600,000 fine.

## Analytical Support – Example Cases



### MAGLOCLEN

The Philadelphia, Pennsylvania, District Attorney’s Office, along with the Philadelphia, Pennsylvania, Police Department, initiated a cocaine trafficking investigation in South Philadelphia, dubbed “Operation Downtown.” MAGLOCLEN analysts were asked to assist by creating analytical charts and searching the RISSIntel databases for additional intelligence on the defendants in question. Analytical charts depicting vehicles, residences, and businesses relating to the defendants were produced, as well as charts using information gleaned from court-authorized wiretaps that illustrated the hierarchy of the defendant organization. “Operation Downtown” resulted in the seizure of 22 kilograms of cocaine, \$439,000 in U.S. currency, \$85,000 in frozen assets, 22 guns, 12 vehicles, and numerous anticipated forfeitures of real estate. Approximately 20 individuals were indicted.

### MOCIC

At the request of the Kansas City, Missouri, Police Department, MOCIC center staff assisted in the successful prosecution of an attorney charged with killing his law partner. The prosecution lacked sufficient motive to charge the suspect with first-degree murder. An MOCIC analyst prepared a financial analysis and charts for use in the courtroom that demonstrated the suspect’s substantial debt. An MOCIC equipment specialist provided still photographs from a surveillance video that supported the financial analysis. The MOCIC analyst testified in the case, and was largely credited with its successful resolution.

### NESPIN

The Massachusetts State Police requested analysis services from the NESPIN center on a larceny investigation involving the Office of the State Treasury of Massachusetts. Seven defendants were indicted in the largest embezzlement case in state history. A total of \$9.4 million was stolen from the unclaimed check fund. Twenty-one sets of telephone toll records were submitted for analysis, and 33,196 telephone records were analyzed. NESPIN provided 123 analytical reports and 12 charts to the agency. Six of the seven defendants pled guilty and were convicted of charges related to the theft. Four of the six received various sentences, and two are awaiting sentencing.

### RMIN

RMIN analytical staff provided case analysis support to the Arizona Attorney General’s Office in the successful prosecution of a suspect wanted for the homicide of a Phoenix police officer that occurred during a shootout with two suspects in a bank robbery. At the time of the initial investigation in 1988, one suspect was arrested and the other suspect fled to Mexico. Mexican authorities recently granted extradition, and Arizona authorities were able to prosecute. RMIN analytical staff provided charts for use by the prosecution, defense, and jury. The suspect was found guilty on nine felony counts.

### ROIC

ROIC analytical staff provided the Bell County, Texas, District Attorney’s Office with more than 20 charts for use in the prosecution of a large-scale embezzlement case. Suspects were charged with defrauding an elderly couple, stealing more than \$249,000 in currency and \$400,000 in property. The charts included trend and pattern analysis, courtroom diagrams, and other flow charts that showed the series of thefts, misappropriations, concealments, diversions, and other felony violations. The defendants were convicted and sentenced to ten years in prison.

### WSIN

The WSIN center was asked to provide analytical assistance for the investigation of a large marijuana trafficking and money laundering organization. The WSIN analyst provided several link and organizational charts, along with telephone toll analysis charts. Fourteen suspects were indicted, ten arrests were made, and eleven properties were seized, along with eight vehicles.

## Confidential Funds Support – Example Cases



### MAGLOCLN

The Erie, Pennsylvania, Bureau of Police Narcotics Unit requested the use of confidential funds from the MAGLOCLN center to further an investigation into a drug distribution conspiracy. The Federal Bureau of Investigation and the Pennsylvania State Police assisted in the investigation. Use of the funds enabled access to the major drug trafficker. Seventeen kilograms of cocaine were seized, and 26 suspects were arrested in Erie, Pennsylvania. Two additional suspects were arrested in Key Largo, Florida. One suspect was arrested for re-entry after deportation. All conspirators will be charged federally.

### MOCIC

The MOCIC center provided confidential funds to the Stateline Area Narcotics Team, which includes MOCIC member Beloit, Wisconsin, Police Department. The funds were used for undercover buys and led to the arrest of two suspects in a major narcotics investigation. The team also confiscated cocaine worth more than \$75,000, marijuana, a vehicle, cellular phones, and a small amount of currency.

### NESPIN

The Rockland, Maine, Police Department requested NESPIN center confidential funds to assist in a large-scale task force narcotics investigation. Officers used the funds to purchase information and drugs, which resulted in the seizure of heroin valued at \$15,000, marijuana valued at \$15,000, prescription pills valued at \$12,000, and cocaine valued at \$3,600. Thirty individuals were arrested in the case. Officers also confiscated \$12,000 in stolen property during the course of the investigation.

### RMIN

The Lovington, New Mexico, Police Department requested RMIN center confidential fund support services concerning a double homicide that was linked to a multijurisdictional criminal investigation. Funds were used to transport investigators and key witnesses to Arizona for coordination with other law enforcement agencies. A federal Grand Jury in New Mexico released a 17-count indictment charging ten defendants with crimes related to drugs and violence, including the Lovington double-murder. This case involved one of the largest racketeering enterprises in New Mexico. Over 15 local, state, and federal agencies in New Mexico, Arizona, and Texas participated in the investigation.

### ROCIC

The R.U.S.H. Drug Task Force, Harrisonburg, Virginia, requested ROCIC center confidential funds to aid an investigation into a major drug distribution ring. The funds enabled the task force to execute a buy/bust involving two leaders of the drug organization. The investigation resulted in 20 arrests, and the seizure of currency and a vehicle.

### WSIN

The WSIN center assisted agents of the Bureau of Narcotic Enforcement, Sacramento, California, Regional Office, by providing confidential funds for use in a methamphetamine investigation. The funds assisted the agents to set up a reverse sting operation. Six individuals were arrested for possession of precursor chemicals with the intent to manufacture methamphetamine. The individuals arrested were part of an organized group of methamphetamine traffickers who wanted to purchase large quantities of pseudoephedrine tablets. Agents also seized \$51,000 in U.S. currency and two vehicles.

## Investigative Equipment Loan Support – Example Cases



### MAGLOCLEN

The MAGLOCLEN center loaned investigative equipment to the Raritan Township, New Jersey, Police Department for use in various investigations over a six-month period. The investigations related to crimes of burglary, theft, and sexual misconduct. The agency credits the success of the investigations to MAGLOCLEN resources.

### NESPIN

The Tewksbury, Massachusetts, Police Department requested the use of a NESPIN center surveillance vehicle in the investigation of a suspected drug trafficker. The suspect was arrested in possession of 135 Oxycontin tablets, an assault rifle, and various other weapons.

### ROCIC

The ROCIC center provided the Summers County, West Virginia, Sheriff's Office with investigative equipment that enabled the surveillance of a suspected narcotics operation. The suspects had been dealing drugs in the area for some time, and the agency did not have the resources or equipment to pursue the investigation. The loaned equipment helped the officers collect enough evidence to arrest seven persons on charges of trafficking crack cocaine, powder cocaine, and heroin. Authorities also seized a vehicle, valued at \$24,000, and \$3,000 in U.S. currency.

## Publications and Training Support – Example Cases



### MAGLOCLLEN

The MAGLOCLLEN center issued a special criminal activity bulletin on an alleged attempted murder suspect, at the request of the Manchester Township, New Jersey, Police Department, that included a photograph and physical description of the suspect. Officers of the Jersey City, New Jersey, Police Department received the bulletin, observed the suspect near a supermarket in Jersey City, and made an arrest when the suspect returned to the supermarket. Jersey City officers then contacted Manchester Township officers to retrieve the suspect. Both agencies stated that the special bulletin directly assisted in the location and apprehension of the alleged attempted murder suspect.

### ROCIC

After attending an Analytical and Investigative Resources class at the ROCIC training center, a captain with the Lawrenceville, Georgia, Police Department used the “timeline analysis method” to organize events, suspects, and other critical information concerning an unsolved double homicide. The use of this method led the officer to the arrest of two men.

### MOCIC

The Mattoon, Illinois, Police Department was investigating a burglary/forgery case in which losses totaled \$27,000. An Illinois officer found details of a similar case in the MOCIC *Criminal Information Digest* submitted by the Brookings, South Dakota, Police Department. Recognizing the suspects’ photographs in the *Digest*, the Illinois officer was able to contact the South Dakota officers and clear the case.

### NESPIN

In hopes of generating leads, the Woonsocket, Rhode Island, Police Department requested that the NESPIN center mail a special bulletin to its members that contained information on a recent bank robbery with the accompanying surveillance photographs. As a result of the bulletin, the investigating officers received information from the Danbury, Connecticut, Police Department regarding a similar bank robbery. The two agencies began working together, in conjunction with the Federal Bureau of Investigation, to identify possible suspects. Officers were able to obtain arrest warrants for two suspects, charging them with first-degree robbery and conspiracy to commit first-degree robbery.

# Conclusion

*The six regional RISS centers continue to provide and enhance traditional support services for their member agencies' investigations, which have resulted in \$29,000,000 in seizures and recoveries.*

As demand for intelligence services and technology increases, RISS continues to respond. The need for sharing terrorism and homeland security information is met by the ability to post information on RISSLeads, the expansion of analytical services regarding terrorism, the distribution of special publications and bulletins on terrorism information, the accessibility of anti-terrorism training material on the RISSTraining Web site, the establishment of the RISS system and LEO system interconnection to disseminate terrorism information and alerts, and the inclusion of essential public safety personnel in the anti-terrorism and emergency information sharing process of RISS ATIX.

Though the need for interagency collaboration and information sharing regarding terrorism is expanding, traditional crime concerns remain. The six regional RISS centers continue to provide and enhance traditional support services for their member agencies.

The combined number of records in the six RISS criminal intelligence databases increased to nearly 3,000,000 by the end of 2002. Member agency inquiries to the databases resulted in 165,477 hits (information found). Gangs and gang member records in the RISSGang database total 71,647, with 10,244 hits received. Fifty-eight conferences have been created on RISSLeads for access by



**In 2002,  
member agency investigations supported  
by RISS center services resulted in:**

Arrests	3,664
Narcotics Seized or Recovered	\$21,000,000
Property Seized or Recovered	\$6,000,000
Currency Seized or Recovered	\$2,000,000

RISS member agencies to post and exchange information on cases and criminal activity, including terrorism activity. Over 36,000 officers attended RISS specialized training and information sharing conferences. The six centers combined assisted their member agencies in making 3,664 arrests by providing information, analytical services, equipment loans, and confidential funds to support their investigations. Seizures or recoveries of over \$21,000,000 in narcotics, nearly \$6,000,000 in property, and nearly \$2,000,000 in currency are attributed to member agency use of the RISS center services.

RISS has placed a high priority on the implementation and operation of information

technology to aid member agency investigations and prosecutions. To best serve member agencies, RISS remains abreast of industry technological advancements. As of December 31, 2002, there were 9,411 officers connected for online access via riss.net. Many state and federal agency systems continue to connect to riss.net as their system of choice for secure communications and information sharing.

The activities and priorities established by the RISS centers reflect the overall objective of the RISS Program to support member agency efforts to combat criminal conspiracies and activities that span jurisdictional boundaries.



*Many state and federal agency systems are connecting to riss.net as their system of choice for secure communications and information sharing.*



## RISS Centers

---

### MAGLOCLN

Middle Atlantic-Great Lakes  
Organized Crime Law Enforcement  
Network

140 Terry Drive, Suite 100  
Newtown, PA 18940  
(800) 345-1322

### MOCIC

Mid-States Organized Crime  
Information Center

1610 East Sunshine Street, Suite 100  
Springfield, MO 65804-1313  
(800) 846-6242

### NESPIN

New England State Police  
Information Network

124 Grove Street, Suite 105  
Franklin, MA 02038  
(800) 343-5682

### RMIN

Rocky Mountain Information  
Network

2828 North Central Avenue  
Suite 1000  
Phoenix, AZ 85004-1027  
(800) 821-0640

### ROCIC

Regional Organized Crime  
Information Center

545 Marriott Drive, Suite 850  
Nashville, TN 37214  
(800) 238-7985

### WSIN

Western States Information Network

Post Office Box 903198  
Sacramento, CA 94203-1980  
(800) 952-5258



**Institute for Intergovernmental Research®**

Post Office Box 12729  
Tallahassee, Florida 32317  
[www.iir.com](http://www.iir.com)