

Testimony Submitted by
The Regional Information Sharing Systems (RISS) Program

Before the
Subcommittee on Technology, Information Policy,
Intergovernmental Relations, and the Census
Of the Government Reform Committee

Submitted by
Gerard P. Lynch, Esq., Executive Director
Middle Atlantic – Great Lakes Organized Crime
Law Enforcement Network (MAGLOCLLEN)
Chairman of the RISS Directors Association

On Behalf of the
Regional Information Sharing Systems (RISS) Program

The events of September 11, 2001, changed much of the historical attitude about sharing data among agencies and across levels of government. Law enforcement and other public safety officials recognize the need for interagency cooperation and coordination in sharing information among local, state, federal, and tribal agencies. The effective coordination and sharing of law enforcement intelligence has proven to be the best method to combat the increasing criminal activity and is paramount to successful counterterrorism and public safety operations.

The Regional Information Sharing Systems (RISS) Program is a nationwide communications and information sharing network that serves nearly 7,000 local, state, federal, and tribal law enforcement member agencies in all 50 states, the District of Columbia, U.S. territories, Australia, Canada, and England. In operation for approximately 25 years through U.S. Department of Justice funding, RISS serves as a force multiplier in fighting increased violent criminal activity by terrorists, drug traffickers, sophisticated cyber criminals, street gangs, and emerging criminal groups that require interagency cooperation. The RISS centers provide support services to facilitate law enforcement investigative and prosecution efforts in combating multijurisdictional criminal activity. The six regional intelligence 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. The RISS centers fill law enforcement's need for rapid but controlled sharing of information and intelligence pertaining to known or suspected terrorists, drug traffickers, and other criminals.

The RISS Program provides secure connectivity and electronic access to law enforcement sensitive but unclassified (SBU) information, encrypted e-mail, electronic collaboration, and databases of criminal intelligence information to more than 75,000 law enforcement and criminal justice professionals from nearly 7,000 member agencies. RISS is operating current state-of-the-art technical capabilities and systems architecture that allow local, state, federal, and tribal law enforcement member agencies to interact electronically with one another in a secure environment. Using a secure Web-based nationwide network known as RISSNET, law enforcement users connect to all RISS criminal intelligence databases and resources 24 hours a day, 7 days a week. RISSNET is a proven, highly effective communications and information sharing system that improves the quality of criminal intelligence information available to law enforcement officers to make key decisions at critical points in their investigation. In addition, the technical architecture adopted by RISS requires proper authorization to access information, but also provides flexibility in the levels of electronic access assigned to individual users based on security and need-to-know issues. This type system and architecture are endorsed by the *National Criminal Intelligence Sharing Plan*.

RISS has expanded its user base by electronically connecting existing state and federal agency information sharing systems to RISSNET to share and expand intelligence capabilities. Currently, 15 state law enforcement systems and 16 High Intensity Drug Trafficking Areas (HIDTA) network systems are electronically connected as nodes to RISSNET. The Executive Office for United States Attorneys has connected staff to RISSNET at each of the 93 U.S. Attorneys' Offices' Anti-Terrorism Task Forces throughout the U.S. Staffs at the U.S. Department of Justice, Criminal Division, have connected to RISSNET. RISS and the El Paso Intelligence Center (EPIC) officials entered into a partnership and have electronically

connected EPIC as a node to RISSNET, to capture clandestine laboratory seizure data from RISS state and local law enforcement member agencies. Other systems connected to RISSNET include the Law Enforcement Intelligence Unit, the National Drug Pointer Index, the National White Collar Crime Center, the National Law Enforcement Telecommunication System, and the Criminal Information Sharing Alliance, formerly the Southwest Border States Anti-Drug Information System. The United States Postal Inspection Service is currently pending connection to RISSNET as a node. The National Drug Intelligence Center uses the RISS network as a communications mechanism for publishing counterdrug intelligence products to federal, state, local, and tribal law enforcement members. RISSNET is in the process of achieving connectivity to the intelligence community's Open Source Information System (100,000 users) and the U.S. Department of Defense Information Systems Agency's ADNET-U system (5,000 users), and anticipates connectivity with the U.S. Department of State's OpenNet Plus system (43,500 users worldwide). Other state systems and HIDTAs are currently in various stages of connection as nodes to RISSNET. The integration of the above-mentioned state, regional, and federal agencies and systems with the RISSNET secure nationwide communications backbone has increased the sharing of criminal intelligence, alerts, and homeland security information within their own agencies and among the other agencies. RISS uses current Extensible Markup Language (XML) technology to assist state law enforcement agencies in electronically connecting their state criminal intelligence databases to RISSNET for access by all RISS member agencies.

The RISS system and the FBI Law Enforcement Online (LEO) system interconnected as a "virtual single system" in 2002 for distribution of SBU homeland security information to authorized users of both LEO and RISS. The value of this interconnection was recognized in 2003 by the *National Criminal Intelligence Sharing Plan*, which is sponsored by the U.S. Department of Justice. The Plan designates the RISS/LEO interconnection as the initial SBU communications backbone for implementation of a nationwide criminal intelligence sharing capability. This nationwide SBU communications backbone supports fully functional, bidirectional information sharing capabilities that leverage existing local, state, tribal, regional, and federal infrastructure investments. The Plan recommends that interoperability of existing systems with the RISS/LEO communications capability proceed immediately to leverage information sharing systems and expand intelligence sharing. The International Association of Chiefs of Police, the U.S. Attorney General, and other federal agency administrators endorse the Plan and have adopted it as a national model for all law enforcement agencies, organizations, and associations. RISS officials are working to implement the Plan recommendations within current budgetary restraints. Due to the interest of many law enforcement agency systems to electronically connect to the RISS/LEO backbone, RISS is testing a security architecture solution to allow users with various types of security credentials to connect and traverse RISSNET to share information and access resources without being required to use the RISS-specific security credentials.

In addition, RISS has recognized that the need for the exchange of information extends beyond law enforcement and the RISS/LEO virtual single system. During 2003, RISS implemented a service available over RISSNET to link law enforcement with the public safety and first responder agencies involved in securing our nation from terrorism. This service is known as the RISS Anti-Terrorism Information Exchange, or RISS ATIX, and includes a secure ATIX Web

site, secure ATIX bulletin board, ATIXLive, and secure e-mail. ATIXLive is an online, real-time, collaborative communications information sharing tool for exchange of information by law enforcement and other first responders. The operation of RISS ATIX provides first responders and critical infrastructure personnel with a secure means via RISSNET to communicate, share information, and receive terrorist threat information, including that provided by the U.S. Department of Homeland Security. Through this capability, users can post timely threat information, view and respond to messages posted by government, police, fire, emergency, and infrastructure security personnel, and collaborate with law enforcement partners. These additional groups of users include public service, public safety, emergency management, utility, and other critical infrastructure personnel that have traditionally not been served by RISS. Currently, more than 47,000 RISS law enforcement members and other public safety participants have access to RISS ATIX services.

Even in its first year of connectivity, ATIX is already proving to be a prized, flexible law enforcement and first responder tool. The team in charge of G8 Summit security and communications this summer, which included the FBI, the U.S. Secret Service, the Georgia Bureau of Investigation, the Georgia Office of Homeland Security, and the Georgia Information Sharing and Analysis Group, selected RISS ATIX as their official system for secure communication and information sharing during the summit. RISS ATIX has also been asked to assist at both the Republican and Democratic national conventions. Amtrak is using the system to request that ATIX participants send reports of suspicious activity around their trains and report to Amtrak and local law enforcement officials. Amtrak has posted accompanying precautions and indicators of suspicious activity on ATIX. Local emergency management services were able to take advantage of the ATIX link to the National Hurricane Center during Hurricane Isabel to track the storm and issue up-to-date warnings and alerts. Water and electric companies have expressed appreciation for the timely, credible information now being shared over ATIX. The Director of Security and Safety of a water utilities company in Newark, Delaware, specifically praised ATIX as a “one-stop shop” for local, regional, and national intelligence data which can be obtained on a daily basis, as well as a source of vital security information that he either could not find previously or which required querying a number of sites.

RISS has also developed and deployed other law enforcement investigative resources available over RISSNET to include RISSLinks, RISSLeads, and RISSLive. RISSLinks is a data visualization tool that instantly creates a link analysis chart of search results from the RISS criminal intelligence databases. Through the click of a button, visual data is provided that instantly displays associations of the suspects that were not previously known and provides the contact information for other agencies that are working the same suspects. This saves valuable law enforcement resources. RISSLeads is a collaborative bulletin board for all types of criminal activity, including terrorism. RISSLive is an online, real-time communications forum which provides RISS law enforcement members the ability to ask questions and receive answers to specific crime topics of interest or for members involved in an operational event requiring an online, real-time communications capability.

The Bureau of Justice Assistance administers the RISS Program and has established guidelines for the provision of services to member agencies. The RISS regional intelligence centers are subject to oversight, monitoring, and auditing by the U.S. Congress; the General Accounting

Office, a federally funded program evaluation office; the U.S. Department of Justice, Bureau of Justice Assistance; and state and local governmental units. The RISS center criminal intelligence databases comply with federal regulation 28 CFR Part 23 (Criminal Intelligence Systems Operating Policies). The 28 CFR Part 23 regulation emphasizes adherence to individual constitutional and privacy rights and places stricter controls on the RISS intelligence sharing function than those placed on most local, state, or federal agencies. RISS supports and has fully operated in compliance with 28 CFR Part 23 since inception. RISS firmly recognizes the need to ensure that individuals' constitutional rights, civil liberties, civil rights, and privacy interests are protected throughout the intelligence process. In this regard, RISS officials recently adopted a RISS Privacy Policy to further strengthen their commitment and support of 28 CFR Part 23 and the protection of individual privacy rights.

RISS continues to provide solutions to the need for enhanced information sharing capabilities between local, state, federal, and tribal law enforcement agencies and homeland security partners. This effort to increase cross-agency and intergovernmental collaboration is demonstrated through the RISS promotion and participation in many initiatives and partnerships to electronically connect additional, existing agency systems as nodes on RISSNET for secure communication and information sharing nationwide. By connecting states and other information sharing systems to the existing RISSNET backbone, rather than funding the build-out of infrastructure for each stand-alone information system, millions of dollars can be saved, and millions of data records can be easily and quickly available to local, state, federal, and tribal law enforcement at little or no cost to the user.

Thank you for this opportunity to provide the subcommittee with this testimony.

THE REGIONAL INFORMATION SHARING SYSTEMS

In addition to RISS technology services, the following are traditional services implemented and maintained by each RISS center to facilitate information sharing and member agency investigation and prosecution efforts:

1. Analysis Services Component: Each center operates an analytical component to assist participating agencies in the compilation, interpretation, and presentation of case investigative and prosecution information provided to the center. This component responds to participating agency requests for analysis of investigative data and data needed for prosecution.
2. Investigative Support Component: Each center operates an investigative support component by providing financial assistance to participating agencies for their conduct of multijurisdictional investigations. Financial resources may include funds for the purchase of information, contraband that may be used as evidence, services, investigative travel and per diem, and overtime compensation. Funds expended and activities conducted under this component must directly support the operation of the information sharing and analytical components.
3. Specialized Equipment Component: Each center maintains a pool of special investigative equipment for loan to participating agencies. The loan of such equipment must directly support the operation of the information sharing and analytical components.
4. Technical Assistance Component: Each center maintains a component to provide technical assistance to member agencies. Through use of center personnel and others in participating agencies, consultation, advice, and information may be made available to member agencies concerning use of specialized equipment; investigative procedures; accounting of center funds, if provided by the center in support of investigations; and information analysis. This component will emphasize use of technical resources among the centers as necessary and available. Technical assistance in the form of active participation by center personnel in member agency investigations is prohibited.
5. Training Component: Each center maintains a training component to upgrade investigative skills of personnel from participating agencies. Such training assistance may consist of financial support to send personnel to training courses, seminars, and conferences or, more commonly, the design and delivery of special training courses by center staff. Training provided under this component must support the center goals and objectives.

To further enhance the coordination and exchange of information among member law enforcement agencies, the centers have initiated additional support service activities, including distribution of criminal activity publications/digests and sponsorship of membership information sharing conferences.

RISSNET RESOURCES

RISS operates the only secure Web-based nationwide network (RISSNET) for communication and exchange of criminal intelligence.

RISSNET gives law enforcement member agencies secure Web browser access to:

- RISS Investigative Leads Bulletin Board (RISSLeads): special emphasis on terrorism information and alerts
- RISS Criminal Intelligence Databases (RISSIntel)
- RISS National Gang Database (RISSGang)
- Secure e-mail
- RISSTraining: emphasis on electronic delivery of anti-terrorism training
- RISSSearch
- RISS criminal activity publications
- RISS training calendars
- Investigative equipment information
- Member contact directories
- State, federal, and regional systems and resources electronically connected
- RISS ATIX: Terrorist threat resources for first responders and law enforcement
- RISSLinks
- RISSLive
- ATIXLive

**THE REGIONAL INFORMATION SHARING SYSTEMS (RISS)
REGIONAL INTELLIGENCE CENTERS**

The Office of Justice Programs' Regional Information Sharing Systems (RISS) Program is a federally funded program comprised of six regional intelligence centers. The six RISS centers provide criminal information exchange and other related operational support services to local, state, federal, and tribal law enforcement agencies located in all 50 states, the District of Columbia, U.S. territories, Canada, Australia, and England. These centers are:

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

Phone: 800-345-1322

E-mail: info@magloclen.riss.net

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

Phone: 800-846-6242

E-mail: info@mocic.riss.net

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

Phone: 800-343-5682

E-mail: info@nespin.riss.net

Regional Organized Crime Information Center (ROCIC) 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

Phone: 800-238-7985

E-mail: info@rocic.riss.net

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

Phone: 800-821-0640

E-mail: info@rmin.riss.net

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

Phone: 800-952-5258

E-mail: info@wsin.riss.net