**Donald F. Kennedy**
**Executive Director**
**New England State Police Information Network**

**Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment**
**United States House of Representatives**

**Regarding a Hearing on:**
**"Homeland Security Information Network: Moving Past the Missteps Toward Better Information Sharing"**

**May 10, 2007**

**Statement of Donald F. Kennedy, Executive Director**
**New England State Police Information Network**
**Before the**
**Committee on Homeland Security, Subcommittee on Intelligence,**
**Information Sharing and Terrorism Risk Assessment**
**United States House of Representatives**
**Regarding a Hearing on:**
**"Homeland Security Information Network:**
**Moving Past the Missteps Toward Better Information Sharing"**
**May 10, 2007**

Chairman Thompson, Ranking Member King, Chairwoman Harman, and Members of the Subcommittee, I sincerely appreciate the opportunity to appear before you today to discuss efforts in the exchange of homeland security information and initiatives currently under way to leverage existing systems available to criminal justice agencies in our country.

I currently serve as the Executive Director of the New England State Police Information Network (NESPIN), one of the six Regional Information Sharing Systems (RISS) centers. Prior to being named Executive Director, I served as NESPIN's Deputy Director of Field Services after retiring as a captain from the Rhode Island State Police, having served in all bureaus and divisions within the state police for 24 years. In my career, I have been afforded the opportunity to actively participate in many aspects of law enforcement, from patrol to policymaker. In those roles, I have come to understand firsthand the importance of information sharing across all levels of government.

Decades before terrorism moved to the forefront, RISS was established to combat crime and enhance public safety. The RISS Program is a congressionally funded, nationwide program supporting local, state, federal, and tribal law enforcement and prosecution efforts, with membership in the 50 states, the District of Columbia, U.S. territories, Australia, Canada, and England. The RISS Program operates on a national basis but provides support regionally through its six regional intelligence centers, which support and serve the unique needs of their individual regions. The six RISS centers and the areas which they serve are:

- **Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network (MAGLOCLEN):** *Delaware, District of Columbia, Indiana, Maryland, Michigan, New Jersey, New York, Ohio, and Pennsylvania, as well as Australia, Canada, and England.*
- **Mid-States Organized Crime Information Center (MOCIC):** *Illinois, Iowa, Kansas, Minnesota, Missouri, Nebraska, North Dakota, South Dakota, and Wisconsin, as well as Canada.*
- **New England State Police Information Network (NESPIN):** *Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, and Vermont, as well as Canada.*
- **Regional Organized Crime Information Center (ROCIC):** *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.*

- **Rocky Mountain Information Network (RMIN):** *Arizona, Colorado, Idaho, Montana, Nevada, New Mexico, Utah, and Wyoming, as well as Canada.*
- **Western States Information Network (WSIN):** *Alaska, California, Hawaii, Oregon, and Washington, as well as Canada and Guam.*

Each RISS center is governed by a policy board or executive committee, composed of representatives from member agencies in the center's multistate region. The RISS National Policy Group is composed of the six Directors of the RISS centers and the chair of each center's policy board. The RISS National Policy Group is responsible for strategic planning, resolution of operational issues, advancement of information sharing, and decision making affecting the six RISS centers, the national organization, service delivery, member agencies, and related partner organizations.

The RISS Program strives to enhance the ability of criminal justice agencies to identify, target, and remove criminal conspiracies and activities spanning multijurisdictional, multistate and, sometimes, international boundaries. RISS facilitates rapid exchange and sharing of information among the agencies pertaining to known suspected criminals or criminal activity and enhances coordination and communication among agencies that are in pursuit of criminal conspiracies determined to be interjurisdictional in nature.

RISS is a force multiplier in fighting increased violent criminal activity by terrorists, drug traffickers, sophisticated cybercriminals, gangs, and emerging criminal groups that require a cooperative effort by local, state, federal, and tribal law enforcement. There is an increasing communications sophistication by the criminal networks, including terrorists, and a rising presence of organized and mobile narcotics crime. Interagency cooperation in sharing information has proven to be the best method to combat this increasing criminal activity. The RISS centers are filling law enforcement's need for rapid, but controlled, sharing of information and intelligence pertaining to known or suspected terrorists and other criminals. Congress funded the RISS Program to address this need, as evidenced by its authorization in the Omnibus Crime Control and Safe Streets Act, Part M.

RISS provides diverse and valuable services and tools directly to detectives and investigative units within local, state, regional, federal, and tribal criminal justice entities, making RISS a comprehensive and universal program. These services and tools include investigative and intelligence analysis, secure national information sharing and communications capabilities, specialized investigative equipment, investigative funds support, criminal activity bulletins and publications, training, and other investigative support and technical services *(Attachment A)*.

The Bureau of Justice Assistance (BJA) administers the RISS Program and has established guidelines for provision of services to member agencies. The RISS centers are subject to oversight, monitoring, and auditing by the U.S. Congress; the U.S. Government Accountability Office, a federally funded program evaluation office; the U.S. Department of Justice (DOJ), BJA; and local and state governmental units. BJA also monitors the RISS centers for 28 Code of Federal Regulations (CFR) Part 23 compliance. 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 its 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 adopted a RISS Privacy Policy to further strengthen their commitment and support of 28 CFR Part 23 and protection of individual privacy rights.

RISS has served as a pioneer, forging the way for today's information sharing age. In 1997, through funding from Congress, RISS implemented and continues to operate the secure Web-based nationwide law enforcement network known as RISSNET. RISSNET offers state-of-the-art technology to address and support law enforcement demands for rapid communication and sharing of information. RISSNET provides the communications backbone and infrastructure for sharing investigative and intelligence information, offers secure sensitive but unclassified electronic communications, and provides controlled access to a variety of sensitive information resources.

Currently, RISS serves over 7,700 law enforcement and criminal justice agencies from all levels of government. Over 75,000 access officers, representing hundreds of thousands of law enforcement officers from all government levels, are able to access the databases of six regional RISS centers and other intelligence systems from a single query—member agencies have bidirectional access to a number of state, regional, federal, and specialized criminal intelligence systems electronically connected to RISSNET. Examples of agencies connected to RISSNET include the Clandestine Laboratory Seizure System at the El Paso Intelligence Center (EPIC); the National Drug Pointer Index (NDPIX); the Law Enforcement Intelligence Unit (LEIU) Database; the National White Collar Crime Center (NW3C); Nlets—The International Justice and Public Safety Information Sharing Network; the California Department of Justice, Bureau of Investigation, Intelligence Database; the Criminal Information Sharing Alliance network (CISAnet); the Oregon State Intelligence Network; the Utah Law Enforcement Information Network; the Wyoming Criminal Justice Information Network; and the Colorado Law Enforcement Intelligence Network. The Executive Office for United States Attorneys has also connected staff to RISSNET, as well as all of the 93 U.S. Attorneys' Offices Anti-Terrorism Task Forces throughout the United States. In addition, staff at DOJ, Criminal Division, have connected to RISSNET.

In this world of rapidly changing technology and with the increased need to provide timely, accurate, and complete information to law enforcement and public safety professionals, the ability to connect critical systems and streamline the ability to house, share, inquire, and disseminate information and intelligence is paramount. Through RISS's trusted system, the ability for law enforcement to target, investigate, and prosecute crime continuously improves. RISS also provides valuable collaboration with others who have experienced similar crime problems or who are investigating the same or similar crime.

RISS has also entered into a partnership with the High Intensity Drug Trafficking Areas (HIDTA) to electronically connect all of the HIDTAs to RISSNET for communications and information sharing. Currently, 18 HIDTAs are electronically connected as nodes to RISSNET.

RISS is working to complete the connection of the remaining HIDTAs. RISS has partnered with the HIDTAs and Nlets to create the National Virtual Pointer System (NVPS). The NVPS, which became operational in June 2004, is an automated system that connects existing deconfliction pointer databases into one virtual pointer system. RISS has also developed an officer safety deconfliction system, RISSafe, to be accessible by member agencies for the purpose of identifying potential conflict in operational cases.

RISS has emerged as one of the nation's most important law enforcement intelligence sharing networks and continues to support efforts to expand and improve information sharing. The partnerships RISS has formed with fellow criminal justice and public safety agencies has allowed for this unprecedented level of information and intelligence to be exchanged through RISSNET. As a result, it is critical to ensure that the information is secure and available only to those with authorized access. RISSNET protects information through use of encryption, smart cards, Internet protocol security standards, and firewalls to prevent unauthorized access. The criminal intelligence information accessed through RISSNET is controlled by its local, state, federal, and tribal law enforcement member agency owners. 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. RISSNET supports secure e-mail and is easily accessible using the Internet. This type system and architecture is referenced and recommended in the *General Counterdrug Intelligence Plan* (GCIP) and is endorsed by the *National Criminal Intelligence Sharing Plan* (NCISP).

The NCISP represents law enforcement's commitment to ensure that the "dots are connected," be it in crime or terrorism. The Plan supports collaboration and fosters an environment in which all levels of law enforcement can work together to improve the safety of the nation. The Plan is the outcome of an unprecedented effort by local, state, federal, and tribal law enforcement officials at all levels, with the strong support of DOJ, to strengthen the nation's security through better intelligence analysis and sharing.

The NCISP provides in Recommendation #21 that RISS and the Federal Bureau of Investigation (FBI) Law Enforcement Online (LEO) systems, which interconnected September 1, 2002, as a virtual single system, shall provide the initial sensitive but unclassified secure communications backbone for implementation of a nationwide criminal intelligence sharing capability. In addition to providing secure communications, the RISS Program has embraced and integrated many of the recommendations contained in the NCISP. For example, RISS is developing 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. This project, known as the Trusted Credential Project, will promote interoperable connectivity among information sharing systems, allow bidirectional sharing, and enhance critical information exchange.

RISS is also embarking on an initiative to streamline the process for RISS users to access RISSNET resources. Known as the RISSNET Portal, it will provide users with one entry point for RISSNET, allowing them to instantly view and access all RISSNET resources from one location. In addition, RISS is moving to an industry standards-based SSL authentication technology. SSL technology is a mature technology for the transmission of encrypted

information and is supported by all major Internet browsers. These three initiatives—the Trusted Credential Project, RISSNET Portal, and SSL—will work in unison and represent the natural next steps for enhancing RISS technology and service to its members.

In the aftermath of 9/11, RISS recognized the critical need for timely exchange of national security and terrorist threat information, not only among law enforcement officials but to all first responders and officials involved in homeland security. As a result, RISS created the Automated Trusted Information Exchange (ATIX). ATIX is a communication system that allows first responders, critical infrastructure personnel, and other public safety personnel—including firefighters and public utility and school personnel and local, state, and federal law enforcement—to share terrorism and homeland security information in a secure, real-time environment. Through ATIX, users access the RISS ATIX Web pages and library, the ATIX bulletin board, ATIXLive, and secure e-mail.

In its first year of connectivity, ATIX was selected as the official system for secure communication and information sharing for the G8 Summit in 2004 by the team in charge of security and communications, 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. In 2005, the ability for ATIX to be successfully utilized in the aftermath of a disaster was demonstrated when it served as a communication tool following Hurricane Katrina. RISS provided logistical support to law enforcement in the damaged areas to receive water, clothing, food, medical supplies, information, and equipment. In addition, RISS prepared intelligence assessments on gang and criminal activity, which aided law enforcement response following the hurricane. In 2006, ATIX demonstrated its communications power during a plane crash incident in Delaware, when a C-5 cargo plane, laden with supplies for U.S. troops in Iraq, crashed after takeoff from Dover Air Force Base. The Delaware Information Analysis Center (DIAC), through its use of ATIX, communicated the incident to appropriate officials and personnel ten minutes prior to media reports of the incident. This allowed law enforcement and first responders to coordinate efforts, assess the situation, and secure the scene. And today, some state homeland security offices, such as DIAC, use ATIX to communicate critical information on a daily basis. In Delaware, more than 100 users across 21 discipline communities involved in their multijurisdictional, multiagency response to all crimes and all hazards utilize ATIX as a primary tool to communicate on a daily basis.

In the months following the creation and deployment of ATIX, RISS reached out to the U.S. Department of Homeland Security (DHS) and other federal agencies to offer the infrastructure support and services available through RISSNET. It was also during this time that DHS was transitioning from the Joint Regional Information Exchange System (JRIES) to the Homeland Security Information Network (HSIN) as a means of expanding to include more communities. In July 2005, at the culmination of numerous briefings and meetings, an executive meeting was held to discuss interoperability and interconnection of the JRIES/HSIN, RISS, and LEO. At that time, a joint decision was made by policymakers from RISS, DOJ, DHS, and FBI to demonstrate interoperability of the systems within a short time frame of 60 days. The parties collaborated to produce a technical white paper describing the information sharing project and a memorandum of understanding. The ultimate goal of this project was to quickly demonstrate the capability to create a seamless connection between systems, permitting users of the individual

systems to access unique tools, resources, and capabilities of all the systems through the current access method.

Although not all the aspects of this initiative came to fruition, RISS and DHS still created an information sharing partnership. During the past two years, RISS has continued to work with DOJ and DHS on what has evolved into the Counterterrorism Collaboration Interoperability Project (CCIP). CCIP is a partnership among RISS, HSIN, LEO, and CISAnet that allows the participating partner systems to publish documents for access by authorized users of the other participating partners' systems via the use of Really Simple Syndication (RSS) feeds. This project has been recognized as a model for all agencies that will share information, as required by Presidential Executive Order 13388, *Strengthening the Sharing of Terrorism Information to Protect Americans*.

While significant strides have been made in the implementation of the CCIP, much work still remains. For example, a disruption in the RSS feeds from HSIN to RISSNET has resulted in a daily search effort by RISS technical staff to access documents posted on the HSIN Law Enforcement and HSIN Emergency Management sites. Through the limited access that RISS has been granted to HSIN, a concerted effort is made to identify and retrieve information available on HSIN, which could be provided automatically through RSS feeds, and post this information on ATIX for access by thousands of users.

In addition to the CCIP, RISS is also involved in other critical initiatives with federal agencies to assist in their efforts to facilitate the exchange of criminal intelligence with local and state law enforcement. As the only nonfederal agency or organization involved in the Law Enforcement Information Sharing Program (LEISP), RISS has the unique opportunity to participate in the this critical initiative with DHS and DOJ to demonstrate applicability of federated identity management as a tool to enhance information sharing. In addition, RISS has been invited to participate in a Secure But Unclassified (SBU) Networks/Systems Collaboration Effort initiative from the Information Sharing Council, tasked to the Program Manager—Information Sharing Environment. This effort is focused on sharing SBU terrorism information and identifying capabilities necessary for a SBU Network/System to be included in the Information Sharing Environment. RISS is pleased to receive these invitations, have the opportunity to assist in the development of national strategies for information sharing, and be recognized for its significant role in advocating for local and state agencies who depend on RISSNET as a system of systems for information sharing.

Local and state law enforcement, which depend on the RISS centers, must be leveraged and included in an information sharing plan. The more than 800,000 law enforcement officers and over 19,000 police agencies in this country are part of the frontline defense in domestic security. Important intelligence/information that may forewarn of a future attack is collected by local and state government personnel through their routine activities. The critical importance of intelligence for frontline police officers cannot be overstated. And without the benefit of intelligence, local and state law enforcement cannot be expected to be active partners in protecting our communities from terrorism. The RISS Program aims to represent these frontline officers in the quest for increased terrorism information sharing in our nation and strives to provide a platform for all areas of homeland security to work together to detect, deter, and

prevent terrorist activities and to improve the safety of our nation. As demand from citizens continues to increase for the country to be ready and prepared and funds continue to tighten, it will be critical to leverage available resources and expertise.

The ultimate goal of RISS is to develop and enhance bidirectional systems access and provide secure real-time information, enabling all participants to share information to enhance the investigative process, in furtherance of recommendations in the *National Criminal Intelligence Sharing Plan*. Having a trusted sharing environment for communicating information and intelligence is a priority issue. There are a number of national systems and networks that local, state, and tribal law enforcement agencies utilize for information sharing efforts, including RISS, LEO, and HSIN. Each of these systems offers unique resources and provides essential information to its primary users. However, the power of these systems linked is exemplary of the whole being greater than the sum of its parts. A true success would be the creation of a "system of systems" that is accessible by hundreds of thousands of criminal justice and homeland security officials, as well as first responders and private sector partners who aid our country in the battle against terrorism.

Currently, users must sign on to multiple systems in order to access information. Rather than develop new systems, it is recommended that the existing networks and systems be modified and augmented based on continuing information needs. The federal government should provide the funding needed to leverage existing information sharing systems and expand intelligence sharing by executing interoperability between operating systems at the local, state, regional, federal, and tribal levels using a federated identification methodology. Local, state, and tribal users should be able to access all pertinent information from disparate systems with a single sign-on, based on the user's classification level and need to know.

In order to succeed, we must bridge the remaining gaps between local, state, and federal intelligence agencies and homeland security information consumers. If we are to continue to successfully deter and prevent attacks, we must work as one united force to combat all crimes.

Over the last few years, RISS has seen increased interest by individuals, agencies, and organizations to use RISSNET as their primary communications system and to partner with RISS on a variety of critical projects and initiatives. RISS is eager to meet this demand and continually partners with law enforcement and criminal justice agencies to fully develop an efficient and effective information sharing environment. However, this demand is draining RISS's resources, and additional funds are needed to ensure that law enforcement and the criminal justice community continue to improve both their information sharing and investigative capabilities in order to most effectively protect public safety.

In Fiscal Year (FY) 2007, RISS was appropriated $39.719 million, the same level appropriated in FY2006. For FY2008, the President's Budget includes $38.5 million, $1.219 million less than the FY2007 appropriation. Based on the needs of local and state law enforcement throughout the country, as well as the demand for increased safeguarding against terrorism, gangs, violent crimes, and other critical crime problems, RISS has requested $53.7 million.

To combat crime, there must be continued funding support to programs like RISS, which have demonstrated decades of success in fighting crime, advancing technology, and enhancing officer safety. Through this strategy, we can maximize available funding, eliminate duplication, and accomplish more with less.

Mr. Chairman, I thank you and your colleagues for giving me the opportunity to speak to you today, and I hope my comments have been of some use to you in your deliberations.

# The Regional Information Sharing Systems

Each RISS center offers basic services to member agencies. Traditional services include information sharing, analysis, telecommunications, equipment loans, confidential funds, training, and technical assistance.

- **Information Sharing**—The operation of RISSNET and its various applications enhances information sharing and communications among RISS members by providing various secure databases and investigative tools. Each RISS center develops and provides access to specialized information sharing systems for use by its member agencies.
- **Analysis**—RISS center personnel create analytical products for investigative and prosecutorial use. RISS develops flowcharts, link-analysis charts, crime scene diagrams, telephone toll analysis reports, and financial analysis reports and provides computer forensics analysis. Staff also provide video and audio enhancement services.
- **Investigative Support**—Each center maintains a staff of intelligence technicians that support member agencies with a variety of investigative assistance. Staff conduct database searches, utilize all RISS applications, and process batch uploads. Intelligence technicians respond to thousands of requests and questions.
- **Field Operations**—Centers maintain field service coordinators who dedicate their time visiting and liaising with RISS member agencies to coordinate delivery of RISS services. This personal interaction with member agencies significantly improves information sharing and ensures that member agencies are provided quality and timely service.
- **Telecommunications**—RISSNET is the communications backbone that supports electronic access and exchange of information by RISS users. The network provides a secure platform for communications, as well as access to various state and federal intelligence systems across the country. RISSNET provides member agencies with a secure, rapid means to access RISS resources. In addition to RISSNET, several RISS centers operate long-distance telecommunications, or WATS services, to facilitate toll-free contact between RISS member agencies working jointly on investigations.
- **Equipment Loans**—Pools of specialized and surveillance equipment are available for loan to member agencies for use in support of multijurisdictional investigations.
- **Confidential Funds**—Member agencies can use funds to purchase information, contraband, stolen property, and other items of an evidentiary nature or to provide for other investigative expenses related to multijurisdictional investigations. The availability and use of confidential funds are strictly controlled by federal guidelines, and internal policies and procedures are developed by each center.
- **Training and Publications**—RISS centers sponsor or cosponsor meetings and conferences that build investigative expertise for member agency personnel. Subject areas include anti-terrorism, crime-specific investigative and surveillance techniques, specialized equipment, officer safety, and analytical techniques. In addition, each center researches, develops, and distributes numerous publications, such as bulletins, flyers, and criminal intelligence publications.

Centers also offer additional services based on regional and member agency needs.